United States Department of State

*Bureau for International Narcotics and Law Enforcement Affairs*

# International Narcotics Control Strategy Report

## Volume II
## Money Laundering and Financial Crimes

March 2007

***Embargoed until***
***March 1, 2007***
***12:30 p.m.***

# Table of Contents
## Volume II

**Legislative Basis for the INCSR** ..... 3
**Introduction** ..... 4
**Bilateral Activities** ..... 9
*Training and Technical Assistance* ..... 9
*Department of State* ..... 9
International Law Enforcement Academies (ILEAs) ..... 10
*Board of Governors of the Federal Reserve System (FRB)* ..... 13
*Drug Enforcement Administration (DEA), Department of Justice* ..... 13
*Federal Bureau of Investigation (FBI), Department of Justice* ..... 14
*Federal Deposit Insurance Corporation (FDIC)* ..... 14
*Financial Crimes Enforcement Network (FinCEN), Department of Treasury* ..... 15
*Immigration and Customs Enforcement, Department of Homeland Security (DHS)* ..... 17
*Internal Revenue Service (IRS), Criminal Investigative Division (CID) Department of Treasury* ..... 17
*Office of the Comptroller of the Currency (OCC), Department of Treasury* ..... 19
*Office of Overseas Prosecutorial Development, Assistance and Training, the Asset Forfeiture and Money Laundering Section, & Counterterrorism Section (OPDAT, AFMLS, and CTS)), Department of Justice* ..... 20
Training and Technical Assistance ..... 20
Money Laundering/Asset Forfeiture ..... 21
Organized Crime ..... 23
Fraud/Anticorruption ..... 24
Terrorism/Terrorist Financing ..... 24
Justice Sector Reform ..... 27
*Office of Technical Assistance (OTA), Treasury Department* ..... 28
Assessing Training and Technical Assistance Needs ..... 28
Anti-Money Laundering and Antiterrorism Financing Training ..... 28
Support for Financial Intelligence Units ..... 29
Casino Gaming ..... 29
Money Services Businesses ..... 30
Insurance ..... 30
Regional and Resident Advisors ..... 30
**Treaties and Agreements** ..... 31
*Treaties* ..... 31
*Agreements* ..... 31
**Multi-Lateral Organizations & Programs** ..... 32
*The Financial Action Task Force (FATF) and FATF-Style Regional Bodies(FSRBs)* ..... 32
*The Egmont Group of Financial Intelligence Units* ..... 33
*The Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Group of Experts to Control Money Laundering* ..... 35
Training and Technical Assistance ..... 35
Other Activities ..... 36

***Pacific Anti-Money Laundering Program (PALP)*** ..... ***36***
***United Nations Global Programme Against Money Laundering*** ..... ***37***
The Mentoring Programme ..... 38
Mentoring & Financial Intelligence Units ..... 39
Computer Based Training ..... 39
Other GPML Initiatives ..... 39
**Major Money Laundering Countries** ..... **40**
***Vulnerability Factors*** ..... ***41***
***Changes in INCSR Priorities for 2006*** ..... ***43***
***Comparative Table*** ..... ***47***
**Country Reports** ..... **56**
Afghanistan ..... 56
Albania ..... 59
Algeria ..... 62
Angola ..... 64
Antigua and Barbuda ..... 65
Argentina ..... 68
Aruba ..... 72
Australia ..... 74
Austria ..... 78
Bahamas ..... 82
Bahrain ..... 84
Bangladesh ..... 87
Barbados ..... 90
Belarus ..... 92
Belgium ..... 96
Belize ..... 101
Bolivia ..... 104
Bosnia and Herzegovina ..... 107
Brazil ..... 110
British Virgin Islands ..... 114
Bulgaria ..... 116
Burma ..... 119
Cambodia ..... 121
Canada ..... 124
Cayman Islands ..... 126
Chile ..... 128
China, People's Republic of ..... 132
Colombia ..... 136
Comoros ..... 141
Cook Islands ..... 143
Costa Rica ..... 146
Côte d'Ivoire ..... 148
Cyprus ..... 151
Czech Republic ..... 158
Dominica ..... 163
Dominican Republic ..... 165
Ecuador ..... 167
Egypt, The Arab Republic of ..... 170
El Salvador ..... 174
France ..... 176
Germany ..... 178
Gibraltar ..... 181

Greece ..... 182
Grenada ..... 187
Guatemala ..... 189
Guernsey ..... 193
Guyana ..... 196
Haiti ..... 198
Honduras ..... 200
Hong Kong ..... 203
Hungary ..... 208
India ..... 212
Indonesia ..... 216
Iran ..... 220
Iraq ..... 222
Ireland ..... 224
Isle of Man ..... 227
Israel ..... 230
Italy ..... 233
Jamaica ..... 237
Japan ..... 239
Jersey ..... 242
Jordan ..... 245
Kenya ..... 246
Korea, Democratic Peoples Republic of ..... 250
Korea, Republic of ..... 250
Kuwait ..... 254
Laos ..... 257
Latvia ..... 259
Lebanon ..... 263
Libya ..... 267
Liechtenstein ..... 269
Luxembourg ..... 272
Macau ..... 277
Malaysia ..... 281
Mexico ..... 285
Moldova ..... 289
Monaco ..... 291
Montenegro ..... 293
Morocco ..... 295
The Netherlands ..... 297
Netherlands Antilles ..... 302
Nicaragua ..... 305
Nigeria ..... 308
Pakistan ..... 312
Palau ..... 315
Panama ..... 317
Paraguay ..... 320
Peru ..... 325
Philippines ..... 329
Poland ..... 333
Portugal ..... 337
Qatar ..... 340
Romania ..... 342
Russia ..... 346
Samoa ..... 352
Saudi Arabia ..... 354
Senegal ..... 357

Serbia ..... 358
Seychelles ..... 362
Sierra Leone ..... 364
Singapore ..... 365
Slovak Republic ..... 370
South Africa ..... 375
Spain ..... 377
St. Kitts and Nevis ..... 382
St. Lucia ..... 384
St. Vincent and the Grenadines ..... 387
Switzerland ..... 389
Syria ..... 394
Taiwan ..... 397
Tanzania ..... 401
Thailand ..... 403
Turkey ..... 408
Turks and Caicos ..... 411
Ukraine ..... 413
United Arab Emirates ..... 417
United Kingdom ..... 423
Uruguay ..... 426
Uzbekistan ..... 429
Vanuatu ..... 434
Venezuela ..... 437
Vietnam ..... 440
Yemen ..... 442
Zimbabwe ..... 444

# Common Abbreviations

| | |
|---|---|
| AML | Anti-Money Laundering |
| APG | Asia/Pacific Group on Money Laundering |
| ARS | Alternative Remittance System |
| CFATF | Caribbean Financial Action Task Force |
| CTF | Counter-Terrorist Financing |
| CTR | Currency Transaction Report |
| DEA | Drug Enforcement Administration |
| DHS | Department of Homeland Security |
| DOJ | Department of Justice |
| DOS | Department of State |
| EAG | Eurasian Group to Combat Money Laundering and Terrorist Financing |
| ESAAMLG | Eastern and Southern Africa Anti-Money Laundering Group |
| EU | European Union |
| FATF | Financial Action Task Force |
| FBI | Federal Bureau of Investigation |
| FinCEN | Financial Crimes Enforcement Network |
| FIU | Financial Intelligence Unit |
| GAFISUD | Financial Action Task Force Against Money Laundering In South America |
| GIABA | Inter-Governmental Action Group against Money Laundering |
| IBC | International Business Company |
| IFI | International Financial Institution |
| IMF | International Monetary Fund |
| INCSR | International Narcotics Control Strategy Report |
| INL | Bureau for International Narcotics and Law Enforcement Affairs |
| IRS | Internal Revenue Service |
| IRS-CID | Internal Revenue Service, Criminal Investigative Division |
| MENAFATF | Middle Eastern and Northern African Financial Action Task Force |
| MLAT | Mutual Legal Assistance Treaty |
| MOU | Memorandum of Understanding |
| NCCT | Non-Cooperative Countries or Territories |
| OAS | Organization of American States |
| OAS/CICAD | OAS Inter-American Drug Abuse Control Commission |
| OFC | Offshore Financial Center |
| PIF | Pacific Islands Forum |
| SAR | Suspicious Activity Report |
| STR | Suspicious Transaction Report |
| UN Drug Convention | 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances |
| UNGPML | United Nations Global Programme against Money Laundering |
| UNODC | United Nations Office for Drug Control and Crime Prevention |
| UNSCR | United Nations Security Council Resolution |
| USAID | Agency for International Development |
| USG | United States Government |

# MONEY LAUNDERING AND FINANCIAL CRIMES

# Legislative Basis for the INCSR

The Money Laundering and Financial Crimes section of the Department of State's International Narcotics Control Strategy Report (INCSR) has been prepared in accordance with section 489 of the Foreign Assistance Act of 1961, as amended (the "FAA," 22 U.S.C. § 2291). The 2007 INCSR is the 24th annual report prepared pursuant to the FAA.

The FAA requires a report on the extent to which each country or entity that received assistance under chapter 8 of Part I of the Foreign Assistance Act in the past two fiscal years has "met the goals and objectives of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances" (the "1988 UN Drug Convention"). FAA § 489(a)(1)(A).

Although the Convention does not contain a list of goals and objectives, it does set forth a number of obligations that the parties agree to undertake. Generally speaking, it requires the parties to take legal measures to outlaw and punish all forms of illicit drug production, trafficking, and drug money laundering, to control chemicals that can be used to process illicit drugs, and to cooperate in international efforts to these ends. The statute lists action by foreign countries on the following issues as relevant to evaluating performance under the 1988 UN Drug Convention: illicit cultivation, production, distribution, sale, transport and financing, and money laundering, asset seizure, extradition, mutual legal assistance, law enforcement and transit cooperation, precursor chemical control, and demand reduction.

In attempting to evaluate whether countries and certain entities are meeting the goals and objectives of the 1988 UN Drug Convention, the Department has used the best information it has available. The 2007 INCSR covers countries that range from major drug producing and drug-transit countries, where drug control is a critical element of national policy, to small countries or entities where drug issues or the capacity to deal with them are minimal. In addition to identifying countries as major sources of precursor chemicals used in the production of illicit narcotics, the INCSR is mandated to identify major money laundering countries (FAA §489(a)(3)(C)). The INCSR is also required to report findings on each country's adoption of laws and regulations to prevent narcotics-related money laundering (FAA §489(a)(7)(C)). This report is that section of the INCSR that reports on money laundering and financial crimes.

A major money laundering country is defined by statute as one "whose financial institutions engage in currency transactions involving significant amounts of proceeds from international narcotics trafficking" (FAA § 481(e)(7)). However, the complex nature of money laundering transactions today makes it difficult in many cases to distinguish the proceeds of narcotics trafficking from the proceeds of other serious crime. Moreover, financial institutions engaging in transactions involving significant

---

The 2007 report on Money Laundering and Financial Crimes is a legislatively mandated section of the U.S. Department of State's annual International Narcotics Control Strategy Report. This 2007 report on Money Laundering and Financial Crimes is based upon the contributions of numerous U.S. Government agencies and international sources. A principal contributor is the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), which, as a member of the international Egmont Group of Financial Intelligence Units, has unique strategic and tactical perspective on international anti-money laundering developments. FinCEN is the primary contributor to the individual country reports. Another key contributor is the U.S. Department of Justice's Asset Forfeiture and Money Laundering Section (AFMLS) of Justice's Criminal Division, which plays a central role in constructing the Money Laundering and Financial Crimes Comparative Table and provides international training. Many other agencies also provided information on international training as well as technical and other assistance, including the following: Department of Homeland Security's Bureau of Immigration and Customs Enforcement; Department of Justice's Drug Enforcement Administration, Federal Bureau of Investigation, and Office for Overseas Prosecutorial Development Assistance; and Treasury's Internal Revenue Service, the Office of the Comptroller of the Currency, and the Office of Technical Assistance. Also providing information on training and technical assistance are the independent regulatory agencies, Federal Deposit Insurance Corporation, and the Federal Reserve Board.

amounts of proceeds of other serious crime are vulnerable to narcotics-related money laundering. This year's list of major money laundering countries recognizes this relationship by including all countries and other jurisdictions, whose financial institutions engage in transactions involving significant amounts of proceeds from all serious crime. The following countries/jurisdictions have been identified this year in this category:

**Major Money Laundering Countries in 2006**

**Afghanistan, Antigua and Barbuda, Australia, Austria, Bahamas, Belize, Bosnia and Herzegovina, Brazil, Burma, Cambodia, Canada, Cayman Islands, China, Colombia, Costa Rica, Cyprus, Dominican Republic, France, Germany, Greece, Guatemala, Guernsey, Haiti, Hong Kong, India, Indonesia, Iran, Isle of Man, Israel, Italy, Japan, Jersey, Kenya, Latvia, Lebanon, Liechtenstein, Luxembourg, Macau, Mexico, Netherlands, Nigeria, Pakistan, Panama, Paraguay, Philippines, Russia, Singapore, Spain, St. Kitts and Nevis, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States, Uruguay, and Venezuela.**

The Money Laundering and Financial Crimes section provides further information on these countries/entities and United States money laundering policies, as required by section 489 of the FAA.

# Introduction

The January 2007 seizure of a staggering $80 million worth of drug trafficking cash and gold in one law enforcement operation in Colombia points to much of what remains dangerous about the global drug and crime trades as well as improving international efforts to combat them. In an age where much of the world's anti-money laundering effort has understandably become focused on countering the terrorist financing threat, this seizure underscores the enormity of funds and profits wrapped up in transnational crime and the potential power that crime syndicates have with this money to inflict substantial political, economic, and social damage on governments and societies around the world. This $80 million seems to be the product of an extraordinarily complex international criminal enterprise. Now that the money and gold are in the hands of the Government of Colombia, it also shows how vulnerable crime syndicates are becoming to global anti-money laundering measures, improved international cooperation, and better law enforcement operations. This success is due in significant part to years of training, technical assistance, and experience.

This case—like any criminal money laundering or terrorist financing seizure—should not, however, stop with the confiscation. Indeed, the confiscation itself should provide valuable intelligence and clues for identifying the individuals most responsible for this trade and enhancing the wherewithal of authorities to find, prosecute, convict, and incarcerate them. Establishing international anti-money laundering and counterterrorist financing norms and standards do much to impede these crimes, but making the masterminds of these operations pay with their freedom is a powerful deterrent for stopping them. The seizure of the money also takes away the primary motivation of these criminal groups—greed.

The Colombian National Police, in this instance, are believed to have made the largest cash seizure ever from a narcotics case. The seizure consisted of U.S. currency, euros, and gold. The money belonged to one criminal organization and was seized at five different locations during one enforcement operation. The Colombian National Police carried out the raids with intelligence and some operational planning assistance from the U.S. Drug Enforcement Administration. Reportedly, no suspects were apprehended at the time of the raids, but several were known ahead of time, and several more have been identified as a result of intelligence gleaned from the seizure.

An $80 million seizure attracts serious attention. In the hands of the Colombian traffickers, it represents the proceeds of criminal operations on a massive scale. It could reflect the wholesale proceeds of exporting more than five metric tons of cocaine to the United States or Europe. This much money in the hands of Asian or Latin America traffickers could also represent the profits from smuggling approximately 1,600 Chinese into the United States or 32,000 illegal aliens from Mexico or Central America across our southwestern border. The circulation of massive amounts of drug money on this scale can create huge, adverse distortions in a weak or small economy.

There is no social or economic "Robin Hood" effect when criminals are in possession of such sums. Their investments tend to be conspicuous, not productive. Moreover, dirty money crowds out legitimate economic activity, creates unfair competition for legitimate businesses, erodes good business practices and ethics, and interferes with the development of sound economic policies. It is almost a bottomless reservoir for corruption that can impede enforcement efforts from front line police officers, to swaying legislators, judges, regulators, or senior executives charged with writing, enforcing, and upholding laws in a rule of law society. $80 million dollars in the hands of terrorists could have funded countless attacks in the United States and around the world. The 9/11 Commission reported that al-Qaida likely spent some $400,000-$500,000 to carry out its 2001 attacks on the United States. While the Colombian seizure is a record amount, it may not be uncharacteristic of similarly large amounts of crime profits lying about in criminal safe havens in the Middle East, Africa, South or Southeast Asia, or Europe.

Dollars, euros, and gold-the three instruments seized in this raid-constitute the face of modern day crime transactions and further highlight the complexity of the money laundering challenge. It suggests large-scale criminal proceeds in the U.S. and European markets, as well as nearly anywhere else in the world. In this respect, the seizure epitomizes the transnational nature of the trade and the dark side of globalization, where national boundaries are no barrier to criminal enterprises, and where most instruments to blur these boundaries-such as rapid and far reaching cyber communications or internationally-recognized currencies-work as much to the benefit of crime syndicates, by easing associations and transfers and providing rapid movement, as they do for legitimate enterprises. The seized gold is especially telling. Historically, the largest value money laundering investigations have involved gold. Gold is both a commodity and a de facto bearer instrument. The form of gold can be readily altered. There is a large cultural demand for gold in Colombian society and elsewhere around the world. Moreover, gold is immune from traditional financial transparency reporting requirements.

The seizure also underscores a likely growing worldwide reluctance of syndicates to place their money in banks where it is increasingly likely to be detected—owing to the steadily improving scrutiny and tracking abilities of the formal financial system. Authorities discovered the dollars, euros, and gold in private residences and businesses, buried in the ground, stashed in private safes, or hidden elsewhere. For any law-abiding entity, this would be an extraordinarily risky way to safeguard and account for such sums. But this example shows how formal financial institutions have become such a significant threat to the operations of crime syndicates and terrorist financiers—that they are willing to take high risks to avoid them.

Since the G-7 created the Financial Action Task Force (FATF) nearly two decades ago in 1989, the international community has been working determinedly to develop the procedures and practices necessary to expose criminal proceeds and take them out of the hands of the syndicates. Since its original seven-country membership (the U.S., Canada, the UK, France, Germany, Italy, and Japan), FATF has grown to include 31 countries and two multilateral organizations (the European Commission and the Gulf Cooperation Council). Its "40 recommendations" to guard against money laundering and nine additional "special recommendations" on terrorist financing contain several provisions aimed specifically at identifying "suspicious transactions," the true owner of such transactions or abnormally large deposits, and tracking them through the system of banks and nonbank financial institutions—such as brokerage houses, money exchangers, or money service businesses. The

provisions include "whistle-blower" type protection for tellers, bankers, and others who are on the front lines of receiving and detecting such deposits to help guard against corruption, intimidation, or retaliation.

FATF "recommendations" carry significant international clout. Both the 2001 UN Convention against Transnational Organized Crime and the 2005 UN Convention against Corruption contain extensive anti-money laundering provisions that are drawn from the FATF recommendations. In addition, recent UN Security Council Resolutions, which member states must abide by, have incorporated the FATF recommendations by direct reference. For instance, in July 2005, UN Security Resolution 1617 "strongly urges all Member States to implement the comprehensive international standards enacted in the FATF Forty recommendations and the Nine Special Recommendations on terrorist financing." This resolution further reinforces the commitment of the 169 members of FATF and the nine FATF-style regional bodies (FSRBs) to criminalize the financing of terrorism and enumerates actions that all UN Member States are legally bound to undertake by virtue of being a party to the UN International Convention for the Suppression of the Financing of Terrorism. It is against this background of growing international acceptance of these norms and standards, and hard work and investment by financial institutions and their compliance officers, that criminals and terrorist financiers, much like these Colombian traffickers, increasingly realize the growing risks they run of having their large or suspicious transactions recorded by banks, shared with the police, and their criminal activities exposed.

A willingness to codify the FATF recommendations into laws and regulations means little if a country is unable, through lack of resources or skill, or unwilling, through lack of political commitment, to implement them. FATF has backed or imposed a wide-ranging set of measures to assist and motivate countries to adopt the "40+9" recommendations. This has included conducting mutual evaluations among its own members to assess their compliance with the recommendations and suggest actions to remedy identified shortfalls. FATF, with bilateral assistance from the U.S. and other donors, has fostered the creation of FATF-style regional bodies around the world so jurisdictions that do not belong to FATF can join and form regionally-tailored organizations to accomplish FATF's objectives. Currently, 138 countries and territories belong to nine such organizations around the world. FATF—and the cooperating donors—have sponsored seminars and provided training and technical experts to help start and sustain these FSRBs. They too have a major responsibility to conduct mutual evaluations among their members.

FATF has also acted in a united, multilateral front to deal with the most incorrigible states, and ones whose weak anti-money laundering regimes or lack of international cooperation pose the most serious risk to anti-money laundering efforts. FATF works internally to identify those countries and will approach them to elicit improvements and better cooperation. If quiet diplomacy fails, FATF can—and has in 23 cases—"named and shamed" noncooperating jurisdictions to focus international attention on them. When FATF identifies problematic countries, it expects its members to respond by invoking any number of countermeasures ranging from issuing advisories that warn their financial institutions about the risks associated with dealing with such jurisdictions, to more drastic measures, such as those taken under Section 311 of the USA PATRIOT Act, to prohibit financial transactions with banks in these countries—or even with the countries themselves.

Many countries come into compliance with global norms and standards and avoid the risk of countermeasures by passing the laws and writing the regulations called for in the FATF recommendations. The laws and regulations, however, need credible enforcement to be dissuasive and effective. This is a tough assignment for many countries, often requiring them to seek and/or accept training and technical assistance from foreign donors. U.S.-provided assistance in this regard can be valuable as the performance by the Colombian National Police in this $80 million seizure attests. The U.S. has provided substantial anti-money laundering assistance to Colombia over the years, making our program there a model for what we are achieving in strategic countries elsewhere. With regard to

the $80 million seizure, the Colombian National Police, who have directly benefited from U.S. assistance, performed with initiative and professionalism. Indeed, aspects of the Colombia program are so strong that today Colombian anti-money laundering experts and officials are sought to provide advice, training, and assistance elsewhere in the region.

The State Department's anti-money laundering/counterterrorist financing training and technical assistance goal is to strengthen regional anti-money laundering organizations and build comprehensive anti-money laundering regimes, with no weak links, in strategic countries. We seek to maximize the institution-building benefits of our assistance by delivering it in both sequential and parallel steps. The steps, while tailored to each country's unique needs as determined by needs and threat assessments, include help in the following areas:

- Drafting and enacting comprehensive anti-money laundering and terrorist financing laws that have measures to enable states to freeze and seize assets as well as comply with the FATF's "40+9" recommendations on money laundering and terrorist financing;
- Establishing a regulatory regime to oversee the financial sector, including to guard against corruption and intimidation;
- Training law enforcement agencies, prosecutors, and judges so that they have the skills to successfully investigate and prosecute financial crimes; and
- Creating and equipping financial intelligence units (FIUs) so that they can collect, analyze, and disseminate suspicious transactions reports and other forms of financial intelligence to both help develop cases domestically and share information internationally through FIUs in other countries as part of transnational investigations.

The crowning achievements in money laundering cases, however, reach beyond the asset seizures and forfeitures. Authorities can, and must, glean from pre-and post-raid intelligence strong evidence to indict the financial and operational masterminds and foot soldiers behind these operations. The international community is underachieving on this front. Despite now nearly unanimous compliance with the FATF recommendation to criminalize money laundering, and acceptance of various UN conventions and Security Council resolutions that make this mandatory, few criminals are being prosecuted or convicted for money laundering. The United Arab Emirates, where the threats of money laundering and terrorist finance are particularly acute, is one example of many strategic countries that are on the right track, but still need to get over this hurdle. The UAE has worked hard, particularly since 9/11, to establish anti-money laundering and counterterrorist finance regimes and countermeasures that adhere to current world standards, yet it is still working to achieve its first money laundering or terrorist financing conviction. The UAE is not alone in this regard as a review of this year's INCSR country reports reveals a similar, unfortunate lack of implementation and enforcement around the world, including even in a number of the most advanced and developed economies on six continents.

The Colombia seizure highlights other key anti-money laundering challenges ahead: the use of cash couriers and trade based money laundering. The cash courier threat is also linked with the misuse of charities to finance terrorism. FATF, for instance, has issued special recommendations and published associated interpretive notes and best practices to address the misuse of charities for terrorist financing. Some charities have been designated under various UN Security Council Resolutions for their roles in financing terrorism resulting in having their assets frozen and/or financial transactions with them prohibited. As this terrorist financing avenue has become more constricted and risky, terrorists have had to rely increasingly on cash couriers for their funds. FATF has a special recommendation, interpretive notes, and best practices papers to help countries address this threat also. Meanwhile, the United States has developed a course focused specifically on cash couriers, including

how to find and stop them at borders, and inserted it as a feature in our anti-money laundering/counterterrorist training and technical assistance program.

The Department of State, in collaboration with the Departments of Homeland Security (DHS) and Treasury, began making combating trade based money laundering a key part of its anti-money laundering effort several years ago. Since then, others have picked up on this urgency, including FATF which last year issued a special paper on trade-based money laundering. Trade is the common denominator in many entrenched underground or alternative remittance systems such as hawala, the black market peso exchange, the misuse of the international gold and gem trades, and other value transfer systems. To help address these vulnerabilities, the State Department's Bureau of International Narcotics and Law Enforcement Affairs (INL) began providing funding to the Department of Homeland Security in 2005 to establish prototype Trade Transparency Units (TTUs) in the Triborder Area countries of Argentina, Paraguay, and Brazil.

TTUs examine anomalies in trade data that could be indicative of customs fraud and trade-based money laundering. As a result of the 2005 INL/DHS initiative, DHS Immigration and Customs Enforcement (ICE) agents teamed with Brazilian authorities in 2006 to target a scheme involving the under-valuation of U.S. exports to Brazil to evade more than $200 million in Brazilian customs duties over the past five years. The scheme involved tax evasion, document fraud, public corruption and other illegal activities in Brazil and the United States. In an excellent example of the long reach of law enforcement, more than 128 arrest warrants and numerous search warrants were simultaneously served in 238 locations in Brazil.

The State Department is working with DHS to expand the TTU concept to Southeast Asia An international TTU network may eventually develop that will promote trade-transparency, combat customs fraud, and be the back door to entrenched informal underground value transfer systems.

Despite the increased awareness and significant progress that has been made on several fronts, much remains to be done in the global effort to combat money laundering. It will remain important to sustain and strengthen these gains because focusing on money laundering is one of the most valuable tools law enforcement has to combat international crime. A focus on money laundering can accomplish what many other law enforcement tools cannot: it can be applied equally effectively to a wide variety of crimes, to any crime that must be financed or is committed for profit. Once in place, anti-money laundering measures can be used without any special tailoring to attack such threats as narcotics trafficking, alien smuggling, intellectual property theft, corruption, terrorism, and more.

Money laundering investigations also take advantage of one of the most important vulnerabilities of sophisticated criminal or terrorist organizations: their risk of exposure. Terrorism and much of organized crime thrive because they take place in the shadows of open society. As long as criminality remains in the underground of aliases, coded messages, false documents, bearer instruments, and clandestine operations, it is often undetectable to even seasoned investigators. When criminal activity breaches this underground, it often provides leads and evidence authorities can use to unravel these cases. The challenge of coping with especially large amounts of money inevitably generates pressure on criminal organizations to take placement, layering, and integration actions involving record keeping, meetings, or other events that eventually surface and expose them for identification and tracking. Full exploitation of these vital breakthroughs can lead investigators, armed with incriminating financial intelligence and evidence, to the financiers and managers of these organizations—to the heart of the syndicates. This is happening in Colombia, as the $80 million seizure demonstrates. But getting to this desirable outcome in many countries around the world still requires a great deal of training, equipping, and political will.

# Bilateral Activities

## *Training and Technical Assistance*

During 2006, a number of U.S. law enforcement and regulatory agencies provided training and technical assistance on money laundering countermeasures and financial investigations to their counterparts around the globe. These courses have been designed to give financial investigators, bank regulators, and prosecutors the necessary tools to recognize, investigate, and prosecute money laundering, financial crimes, terrorist financing, and related criminal activity. Courses have been provided in the United States as well as in the jurisdictions where the programs are targeted.

## *Department of State*

The Department of State's Bureau for International Narcotics and Law Enforcement Affairs (INL) and the Department's Office of the Coordinator for Counter-Terrorism (SCT) co-chair the interagency Terrorist Finance Working Group, and together are implementing a multi-million dollar training and technical assistance program designed to develop or enhance the capacity of a selected group of more than two dozen countries whose financial sectors have been used or are vulnerable to being used to finance terrorism. As is the case with the more than 100 other countries to which INL-funded training was delivered in 2006, the capacity to thwart the funding of terrorism is dependent on the development of a robust anti-money laundering regime. Supported by and in coordination with the State Department, the Department of Justice, Department of Homeland Security, Treasury Department, the Federal Deposit Insurance Corporation, and various nongovernmental organizations offered law enforcement, regulatory and criminal justice programs worldwide. This integrated approach includes assistance with the drafting of legislation and regulations that comport with international standards, the training of law enforcement, the judiciary and bank regulators, as well as the development of financial intelligence units capable of collecting, analyzing and disseminating financial information to foreign analogs.

Nearly every federal law enforcement agency assisted in this effort by providing basic and advanced training courses in all aspects of financial criminal investigation. Likewise, bank regulatory agencies participated in providing advanced anti-money laundering/counterterrorist financing training to supervisory entities. In addition, INL made funds available for the intermittent or full-time posting of legal and financial advisors at selected overseas locations. These advisors work directly with host governments to assist in the creation, implementation, and enforcement of anti-money laundering and financial crime legislation. INL also provided several federal agencies funding to conduct multi-agency financial crime training assessments and develop specialized training in specific jurisdictions to combat money laundering.

The success of the Brazilian Trade Transparency Unit (TTU) less than nine months after being established in late 2005 augurs well for the nascent TTUs of Argentina and Paraguay. In 2006, INL obligated funds to DHS to establish a TTU in Southeast Asia and will continue to provide funding to DHS for the development of TTUs globally. Similar to the Egmont Group of Financial Intelligence Units that examines and exchanges information gathered through financial transparency reporting requirements, an international network of TTUs would foster the sharing of disparities in trade data between countries and be a potent weapon in combating customs fraud and trade-based money laundering. Trade is the common denominator in most of the world's alternative remittance systems and underground banking systems. Trade-based value transfer systems have also been used in terrorist finance.

The success of the now-concluded Caribbean Anti-Money Laundering Programme (CALP) convinced INL that a similar type of program for small Pacific island jurisdictions had the potential of developing viable anti-money laundering/counterterrorist regimes. Accordingly, INL contributed $1.5 million to the Pacific Islands Forum to develop the Pacific Island Anti-Money Laundering Program (PALP). The objectives of the PALP are to reduce the laundering of the proceeds of all serious crime and the financing of terrorist financing by facilitating the prevention, investigation, and prosecution of money laundering. The PALP's staff of resident mentors provides regional and bilateral mentoring, training; and technical assistance to the Pacific Islands Forum's fourteen non-FATF member states for the purpose of developing viable regimes that comport with international standards.

In 2005, INL reserved $900,000 for the United Nations Global Programme against Money Laundering (GPML). In addition to sponsoring money laundering conferences and providing short-term training courses, the GPML instituted a unique longer-term technical assistance initiative through its mentoring program. The mentoring program provides advisors on a yearlong basis to specific countries or regions. GPML mentors provided assistance to the Secretariat of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and to the Horn of Africa countries targeted by the President's East Africa Counterterrorism Initiative. GPML resident mentors provided country-specific assistance to the Philippine FIU and asset forfeiture assistance to Namibia. Regional assistance to Central and Southeast Asia and the Pacific was also provided by other GPML mentors.

INL continues to provide significant financial support for many of the anti-money laundering bodies around the globe. During 2006, INL supported FATF, the international standard setting organization. INL continued to be the sole U.S. Government financial supporter of the FATF-style regional bodies, including the Asia/Pacific Group on Money Laundering (APG), the Council of Europe's MONEYVAL, the Caribbean Financial Action Task Force (CFATF), the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and the South American Financial Action Task Force, Grupo de Accion Financiera de Sudamerica Contra el Lavado de Activos (GAFISUD). INL also financially supported the Pacific Islands Forum and the Organization of American States (OAS) Inter-American Drug Abuse Control Commission (CICAD) Experts Group to Control Money Laundering and the OAS Counter-Terrorism Committee.

As in previous years, INL training programs continue to focus on an interagency approach and on bringing together, where possible, foreign law enforcement, judicial and Central Bank authorities. This allows for an extensive dialogue and exchange of information. This approach has been used successfully in Asia, Central and South America, Russia, the Newly Independent States (NIS) of the former Soviet Union, and Central Europe. INL also provides funding for many of the regional training and technical assistance programs offered by the various law enforcement agencies, including assistance to the International Law Enforcement Academies.

## International Law Enforcement Academies (ILEAs)

The mission of the regional ILEAs has been to support emerging democracies, help protect U.S. interests through international cooperation, and promote social, political and economic stability by combating crime. To achieve these goals, the ILEA program has provided high-quality training and technical assistance, supported institution building and enforcement capabilities, and fostered relationships of American law enforcement agencies with their counterparts in each region. ILEAs have also encouraged strong partnerships among regional countries to address common problems associated with criminal activity.

The ILEA concept and philosophy is a united effort by all the participants-government agencies and ministries, trainers, managers, and students alike to achieve the common foreign policy goal of international law enforcement. The goal is to train professionals that will craft the future for the rule of law, human dignity, personal safety and global security.

The ILEAs are a progressive concept in the area of international assistance programs. The regional ILEAs offer three different types of programs. The core program, a series of specialized training courses and regional seminars tailored to region-specific needs and emerging global threats, typically includes 50 participants, normally from three or more countries. The specialized courses, comprised of about 30 participants, are normally one or two weeks long and often run simultaneously with the Core program. Topics of the regional seminars include transnational crimes, financial crimes, and counterterrorism.

The ILEAs help develop an extensive network of alumni that exchange information with their U.S. counterparts and assist in transnational investigations. These graduates are also expected to become the leaders and decision-makers in their respective societies. The Department of State works with the Departments of Justice (DOJ), Homeland Security (DHS) and Treasury, and with foreign governments to implement the ILEA programs. To date, the combined ILEAs have trained over 18,000 officials from over 75 countries in Africa, Asia, Europe and Latin America. The ILEA budget averages approximately $16-18 million annually.

**Africa**. ILEA Gaborone (Botswana) opened in 2001. The main feature of the ILEA is a six-week intensive personal and professional development program, called the Law Enforcement Executive Development Program (LEEDP), for law enforcement mid-level managers. The LEEDP brings together approximately 45 participants from several nations for training on topics such as combating transnational criminal activity, supporting democracy by stressing the rule of law in international and domestic police operations, and by raising the professionalism of officers involved in the fight against crime. ILEA Gaborone also offers specialized courses for police and other criminal justice officials to enhance their capacity to work with U.S. and regional officials to combat international criminal activities. These courses concentrate on specific methods and techniques in a variety of subjects, such as counterterrorism, anticorruption, financial crimes, border security, drug enforcement, firearms and many others.

Instruction is provided to participants from Angola, Botswana, Cameroon, Comoros, Congo, the Democratic Republic of Congo, Djibouti, Ethiopia, Gabon, Kenya, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Nigeria, Seychelles, South Africa, Swaziland, Tanzania, Uganda, and Zambia.

United States and Botswana trainers provide instruction. ILEA Gaborone has offered specialized courses on money laundering/terrorist financing-related topics such as Criminal Investigation (presented by FBI) and International Banking & Money Laundering Program (presented by the DHS Federal Law Enforcement Training Center). ILEA Gaborone trains approximately 500 students annually.

**Asia.** ILEA Bangkok (Thailand) opened in March 1999. The ILEA focuses on enhancing the effectiveness of regional cooperation against the principal transnational crime threats in Southeast Asia—illicit drug-trafficking, financial crimes, and alien smuggling. The ILEA provides a core course (the Supervisory Criminal Investigator Course or SCIC) of management and technical instruction for supervisory criminal investigators and other criminal justice managers. In addition, this ILEA presents one Senior Executive program and approximately 18 specialized courses—lasting one to two weeks—in a variety of criminal justice topics. The principal objectives of the ILEA are the development of effective law enforcement cooperation within the member countries of the Association of Southeast Asian Nations (ASEAN), East Timor and China (including Hong Kong and Macau), and the strengthening of each country's criminal justice institutions to increase their abilities to cooperate in the suppression of transnational crime.

Instruction is provided to participants from Brunei, Cambodia, China, East Timor, Hong Kong, Indonesia, Laos, Macau, Malaysia, Philippines, Singapore, Thailand and Vietnam. Subject matter experts from the United States, Hong Kong, Japan, Netherlands, Philippines, and Thailand provide

instruction. ILEA Bangkok has offered specialized courses on money laundering/terrorist financing-related topics such as Computer Crime Investigations (presented by FBI and DHS/Bureau of Customs and Border Protection (BCBP) and Complex Financial Investigations (presented by IRS, DHS/BCBP, FBI and DEA). Approximately 600 students participate annually.

**Europe.** ILEA Budapest (Hungary) opened in 1995. Its mission has been to support the region's emerging democracies by combating an increase in criminal activity that emerged against the backdrop of economic and political restructuring following the collapse of the Soviet Union. ILEA Budapest offers three different types of programs: an eight-week Core course, Regional Seminars and Specialized courses in a variety of criminal justice topics. Instruction is provided to participants from Albania, Armenia, Azerbaijan, Bulgaria, Croatia, Czech Republic, Estonia, Georgia, Hungary, Kazakhstan, Kyrgyz Republic, Latvia, Lithuania, Macedonia, Moldova, Montenegro, Poland, Romania, Russia, Serbia, Slovakia, Slovenia, Tajikistan, Turkmenistan, Ukraine and Uzbekistan.

Trainers from 17 federal agencies and local jurisdictions from the United States and also from Hungary, Canada, Germany, United Kingdom, Netherlands, Ireland, Italy, Russia, Interpol and the Council of Europe provide instruction. ILEA Budapest offered specialized courses on money laundering/terrorist financing-related topics such as Investigating/Prosecuting Organized Crime and Transnational Money Laundering (both presented by DOJ/OPDAT). ILEA Budapest trains approximately 950 students annually.

**Global.** ILEA Roswell (New Mexico) opened in September 2001. This ILEA offers a curriculum comprised of courses similar to those provided at a typical Criminal Justice university/college. These three-week courses have been designed and are taught by academicians for foreign law enforcement officials. This Academy is unique in its format and composition with a strictly academic focus and a worldwide student body. The participants are mid-to-senior level law enforcement and criminal justice officials from Eastern Europe; Russia;, the Newly Independent States (NIS); Association of Southeast Asian Nations (ASEAN) member countries; and the People's Republic of China (including the Special Autonomous Regions of Hong Kong and Macau); and member countries of the Southern African Development Community (SADC) plus other East and West African countries; the Caribbean, Central and South American countries. The students are drawn from pools of ILEA graduates from the Academies in Bangkok, Budapest, Gaborone and San Salvador. ILEA Roswell trains approximately 450 students annually.

**Latin America.** ILEA San Salvador was established in 2005. The training program for the newest ILEA is similar to the ILEAs in Bangkok, Budapest and Gaborone and will offer a six-week Law Enforcement Management Development Program (LEMDP) for law enforcement and criminal justice officials as well as specialized courses for police, prosecutors, and judicial officials. In 2007, ILEA San Salvador will deliver three LEMDP sessions and about 10 Specialized courses that will concentrate on attacking international terrorism, illegal trafficking in drugs, alien smuggling, terrorist financing, financial crimes, culture of lawfulness and accountability in government. Components of the six-week LEMDP training session will focus on terrorist financing (presented by the FBI), international money laundering (presented by DHS/ICE) and financial evidence/money laundering application (presented by DHS/FLETC and IRS). The Specialized course schedule will include courses on financial crimes investigations (presented by DHS/ICE) and anti-money laundering training (presented by IRS). Instruction is provided to participants from: Argentina, Barbados, Bahamas, Belize, Bolivia, Brazil, Chile, Colombia, Costa Rica, Dominican Republic, El Salvador, Guatemala, Honduras, Jamaica, Nicaragua, Panama, Paraguay, Peru, Trinidad and Tobago, Uruguay and Venezuela.

The ILEA Regional Training Center located in Peru will officially open in 2007. The center will augment the delivery of region-specific training for Latin America and will concentrate on specialized courses on critical topics for countries in the Southern Cone and Andean Regions.

## *Board of Governors of the Federal Reserve System (FRB)*

An important component in the United States' efforts to combat and deter money laundering and terrorism financing is to verify that supervised organizations comply with the Bank Secrecy Act and have programs in place to comply with Office of Foreign Assets Control (OFAC) sanctions. The FRB, working with the other bank regulatory agencies, examines banking organizations under its supervision for compliance with these statutes. This task was advanced in 2005 with the issuance of the Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money Laundering Examination Manual, which was revised in 2006.

Internationally, the FRB conducted training and provided technical assistance to bank supervisors and law enforcement officials in anti-money laundering and counterterrorism financing tactics in partnership with regional supervisory groups or multilateral institutions. In 2006, the FRB provided training and/or technical assistance to regulators and bankers in Argentina and Mexico. In addition, the FRB hosted an Anti-Money Laundering Examination Seminar in Washington D.C. for bank supervisors from sixteen countries. Due to the importance that the FRB places on international standards, the FRB anti-money laundering experts participated regularly in the U.S. delegation to the Financial Action Task Force and the Basel Committee's cross-border banking groups. The experts also meet with industry groups to support industry best practices in this area.

The FRB also presented training courses on International Money Movements to domestic law enforcement agencies including the Internal Revenue Service, the Federal Bureau of Investigation, the U.S. Postal Inspection Service, the Department of Homeland Security's Bureau for Immigration and Customs Enforcement, and the Drug Enforcement Administration, as well as at the Federal Law Enforcement Training Center.

## *Drug Enforcement Administration (DEA), Department of Justice*

The International Training Section of the DEA conducts its International Asset Forfeiture and Money Laundering courses in concert with the Department of Justice (DOJ). In 2006, more than two hundred participants from The Netherlands, Brazil, South Korea, Spain, People's Republic of China, Singapore, and Russia received this training.

A wide range of DEA international courses contain training elements related to countering money laundering and other financial crimes. The basic course curriculum, which was conducted in Brazil, South Korea, China, and Russia addresses money laundering and its relation to asset identification, seizure and forfeiture techniques, financial investigations, the role of intelligence in financial investigations, document exploitation, and case studies with a practical exercise. The curriculum also includes overviews of U.S. asset forfeiture law, country specific forfeiture and customs law, and prosecutorial perspectives. The advanced course, conducted in The Netherlands, Spain, and Singapore included tracing the origin of financial assets, internet/cyber banking, terrorist financing, reverse undercover operations, electronic evidence and data exploitation, role of intelligence in money laundering investigations, and case studies. Additionally, a legal overview of U.S. methods of administrative, civil, and criminal forfeiture, along with asset sharing, liability, and ethical issues was presented.

The DEA training division also delivers training at the International Law Enforcement Academies in Bangkok, Budapest, Gaborone, and San Salvador. In addition, DEA presented a three-week International Narcotics Enforcement Management Seminar for officials from China, Laos, Philippines, New Zealand, Thailand, Indonesia, Fiji, South Korea, Vietnam, Malaysia, Singapore, Japan, Cambodia, Macau, Hong Kong, and Australia. The DEA Chief of Financial Operations presented a

block of training related to the Office of Financial Operations Mission; the stages of drug money flow; the role of U.S. based Financial Investigative Teams; and financial investigative initiatives.

In addition to the financial training described above, the DEA Office of Financial Operations provided anti-money laundering and/or asset forfeiture training in 2006 to officials from Ecuador, the People's Republic of China, Costa Rica, Spain, Mexico, Nicaragua, Latvia, and Canada.

## *Federal Bureau of Investigation (FBI), Department of Justice*

During 2006, with the assistance of State Department funding, Special Agents and other subject matter experts of the FBI continued their extensive international training in terrorist financing, money laundering, financial fraud, racketeering enterprise investigations, and complex financial crimes. The unit of the FBI responsible for international training, the International Training and Assistance Unit (ITAU), is located at the FBI Academy in Quantico, Virginia. ITAU coordinates with the Terrorist Financing and Operations Section of the FBI's Counterterrorism Division, as well as other divisions within FBI Headquarters and in the field, to provide instructors for these international initiatives. FBI instructors, who are most often intelligence analysts, operational Special Agents or supervisory special agents from headquarters or the field, rely on their experience to relate to the international law enforcement students as peers and partners in the training courses.

The FBI regularly conducts training through International Law Enforcement Academies (ILEA) in Bangkok, Thailand; Budapest, Hungary; Gaborone, Botswana; and San Salvador, El Salvador. In 2006, the FBI delivered training in white collar crime investigations to 240 students from 15 countries at ILEA Budapest. At the ILEA in Bangkok, for the Supervisory Criminal Investigators Course, the FBI trained 45 students from Thailand. Similarly, at the ILEA San Salvador, the FBI provided terrorist financing training to 40 students from El Salvador, Panama, Costa Rica, and Ecuador.

The FBI also provided training to officials in the Bahamas, Thailand, Nigeria, Moldova, Suriname, Bulgaria, Tanzania, Indonesia, Jordan, Chile, Egypt, Czech Republic, Philippines, Pakistan, Malaysia, Bangladesh, Kuwait, and the United Arab Emirates. This training includes FBI participation in financial investigation and organized crime seminars that DOJ's Office of Overseas Prosecutorial Development delivered to 59 students in Suriname and Bulgaria. The FBI also delivered one-week terrorist financing and money laundering training initiatives that the FBI regularly conducts with the assistance of the Internal Revenue Service Criminal Investigative Division,. This training was provided to 326 international students in 2006. For the first time, the FBI participated in IRS sponsored Financial Investigations Techniques/Money Laundering courses in Malaysia, Philippines, Bangladesh and Kuwait to 138 participants.

In other FBI training programs, the FBI included blocks of instruction on terrorist financing and/or money laundering for 38 students from 18 Latin American countries participating in the Latin American Law Enforcement Executive Development Seminar and for 24 students from 11 Middle Eastern and Northern African countries participating in the first Arabic Language Law Enforcement Executive Development Seminar. Both seminars were conducted at the FBI Academy. Terrorist Financing instruction was also included in the FBI's Pacific Training Initiative, which served 50 participants from 10 countries, to include Australia, Cambodia, China, Japan, Korea, Micronesia, Pakistan, Philippines, Singapore, and Thailand.

## *Federal Deposit Insurance Corporation (FDIC)*

In 2006, the FDIC continued to work in partnership with several agencies to combat money laundering and the global flow of terrorist funds. Additionally, the agency planned and conducted missions to

assess vulnerabilities to terrorist financing activity worldwide, and developed and implemented plans to assist foreign governments in their efforts in this regard. To accomplish that objective, the FDIC has 37 individuals available to participate in foreign missions. Periodically, FDIC management and staff meet with supervisory and law enforcement representatives from various countries to discuss anti-money laundering (AML) issues, including examination policies and procedures, the USA PATRIOT Act and its requirements, the FDIC's asset forfeiture programs, suspicious activity reporting requirements, and interagency information sharing mechanisms. In 2006, the FDIC gave such presentations to representatives from Malaysia, Australia, Armenia and India.

In September 2006, in partnership with the Department of State, the FDIC hosted 20 individuals from Iraq, Afghanistan, Yemen, Kenya, and South Africa. The session focused on AML and counter terrorist financing, including the examination process, customer due diligence, and foreign correspondent banking. In December 2006, the FDIC participated in an interagency Financial Systems Assessment Team (FSAT) to Bosnia. The group reviewed the country's AML law and provided information in the areas of customer identification programs, financial intelligence units and the monitoring of nonbank financial institutions.

In December 2006, the FDIC partnered with the Financial Services Volunteer Corp to provide technical assistance to the government of Russia by reviewing its AML legislation and delivering a presentation on the U. S. AML regime from a financial regulatory perspective. FDIC staff reviewed and advised the Russian central bank, financial intelligence unit, and legislature regarding amendments to their AML law. FDIC staff also delivered a presentation at the Eurasian Group seminar in Moscow, Russia in 2006. During 2006, the FDIC also assisted in an interagency assessment of identifying AML/CFT vulnerabilities in South Africa's financial, legal, and law enforcement systems. Additionally FDIC reviewed draft AML legislation for Paraguay in 2006.

## *Financial Crimes Enforcement Network (FinCEN), Department of Treasury*

FinCEN, the U.S. Financial Intelligence Unit (FIU), a bureau of the U.S. Department of the Treasury, coordinates and provides training and technical assistance to foreign nations seeking to improve their capabilities to combat money laundering, terrorist financing, and other financial crimes. FinCEN's particular focus is the creation and strengthening of FIUs—a valuable component of a country's anti-money laundering/counterterrorism financing (AML/CTF) regime. FinCEN's international training program has two primary focuses: (1) instruction and presentations to a broad range of government officials, financial regulators, law enforcement officers, and others on the subjects of money laundering, terrorist financing, financial crime, and FinCEN's mission and operation; and (2) specific training to FIU counterparts regarding FIU operations and analysis training via personnel exchanges and FIU development seminars. Much of FinCEN's work involves strengthening existing FIUs and the channels of communication used to share information to support anti-money laundering investigations. Participation in personnel exchanges (from the foreign FIU to FinCEN and vice versa), delegation visits to foreign FIUs, and regional and operational workshops are just a few examples of FinCEN activities designed to assist and support FIUs.

In 2006, FinCEN hosted representatives from approximately 60 countries. These visits, typically lasting one to two days, focused on topics such as money laundering trends and patterns, the Bank Secrecy Act, USA PATRIOT Act, communications systems and databases, case processing, and the goals and mission of FinCEN. Representatives from foreign financial and law enforcement sectors generally spend one to two days at FinCEN learning about money laundering, the U.S. AML regime and reporting requirements, the national and international roles of a financial intelligence unit, and various other topics.

Regarding assistance to nascent FIUs that are not yet members of Egmont, FinCEN hosts FIU-orientation visits and provides training and mentoring on FIU development. In 2006, at the invitation of FinCEN's Director, a delegation from India's nascent Financial Intelligence Unit (FIU-IND) and representatives from Jordan's Central Bank were hosted by FinCEN for week-long seminars that included an overview of FinCEN's operations and programs and briefings from various other U.S. agencies brought in by FinCEN (OFAC, IRS-CI, FDIC, Secret Service, and FBI) to discuss the U.S. AML/CFT regime.

For those FIUs that are fully operational, FinCEN's goal is to assist the unit in increasing effectiveness, improving information sharing capabilities, and better understanding the phenomena of money laundering and terrorist financing. As a member of the Egmont Group of FIUs, FinCEN works closely with other member FIUs to provide training and technical assistance to countries and jurisdictions interested in establishing their own FIUs and having those units become candidates for membership in the Egmont Group Additionally, FinCEN works multilaterally through its representative on the Egmont Technical Assistance Working Group to design, implement, and co-teach Egmont-sponsored regional training programs to both Egmont-FIUs and Egmont candidates.

In addition to hosting delegations for training on FinCEN premises, FinCEN conducts training courses and seminars abroad, both independently and in conjunction with other domestic and foreign agencies, counterpart FIUs, and international organizations. Occasionally, FinCEN's training and technical assistance programming is developed jointly with these other agencies in order to address specific needs of the jurisdiction/country receiving assistance. Topics such as FIU primary and secondary functions; regulatory issues; international case processing procedures; technology infrastructure and security; and terrorist financing and money laundering trends and typologies provide trainees with broader knowledge and a better understanding of the topics of money laundering and terrorism financing. By way of example, as a follow-up to Romania's visit to FinCEN in 2005, FinCEN at the invitation of U.S. Embassy in Bucharest participated in a financial investigations seminar co-sponsored by the Romanian FIU and the Romanian National Anti-Corruption Department. FinCEN also prepared and delivered a training module on money laundering, FIUs and international cooperation in Spanish which was given at the ILEA in San Salvador., involving participants from Ecuador, Costa Rica, El Salvador and Panama.

Core analytical training to counterpart FIUs is conducted both on FinCEN premises and abroad, often in conjunction with other U.S. agencies. FinCEN's analytical training program, typically delivered over the course of one to two weeks, provides foreign analysts with basic skills in critical thinking and analysis; data collection; database research; suspicious transactions analysis; the intelligence cycle; charting; data mining; and case presentation. As Nigeria's sponsor for Egmont membership, FinCEN devoted three analysts to provide two weeks of analytical training to the newly formed FIU in Abuja in August 2006. The training, which consisted of basic analysis theory and charting techniques, was delivered to the FIU as well as other agencies, from intelligence to regulatory to enforcement.

Over the last twelve months, in an effort to reinforce the sharing of information among established Egmont-member FIUs, FinCEN conducted personnel exchanges with a number of Egmont Group members: Albania, Canada, and Chile. These exchanges offer the opportunity for FIU personnel to see first-hand how another FIU operates; develop joint analytical projects and other strategic initiatives; and also to work jointly on on-going financial crimes cases. The participants in these exchanges share ideas, innovations, and insights that lead to improvements in such areas as analysis, information flow, and information security at their home FIUs, in addition to deeper and more sustained operational collaboration.

## *Immigration and Customs Enforcement, Department of Homeland Security (DHS)*

During 2006, U.S. Immigration and Customs Enforcement (ICE), Financial Investigations Division and the Office of International Affairs delivered money laundering/terrorist financing, and financial investigations training to law enforcement, regulatory, banking and trade officials from more than 100 foreign countries. The training was conducted in both multilateral and bilateral engagements. ICE money laundering and financial investigations training is based on the broad experience achieved while conducting international money laundering and traditional financial investigations techniques as part of the U.S. Customs Service (USCS) legacy.

Using State Department INL funding, ICE provided bilateral training and technical assistance on the interdiction and investigation of bulk cash smuggling, for more than 200 officials in the Philippines, Paraguay, Pakistan, Tanzania, Malaysia, and Indonesia. The training was conducted in furtherance of the Financial Action Task Force (FATF) on Money Laundering, Special Recommendation IX on Cash Couriers.

ICE conducted financial investigation/money laundering training programs for more than 300 participants at the State Department sponsored International Law Enforcement Academy (ILEA) locations in El Salvador, Thailand, and Botswana. The specialized training was given three times each at the ILEAs in El Salvador and Botswana, and once in Thailand.

ICE also provided training to foreign police, judicial, banking and public sector officials at seminars and conferences sponsored by the FATF, the Caribbean Financial Action Task Force and the Asia/Pacific Group on Money Laundering Under the auspices of these multinational organizations, ICE delivered training on money laundering, financial investigations, bulk cash smuggling, and trade based money laundering to officials from more than 100 countries.

With INL funding, ICE worked to expand the network of foreign Trade Transparency Units (TTU) beyond Colombia. With ICE established TTU's in the Tri-border area countries of Brazil and Argentina. ICE also exchanged trade data with the Government of Paraguay and ICE is in the process of establishing a TTU for that nation.

ICE updated the technical capabilities of Colombia's TTU and trained new TTU personnel, to include members of the Financial Intelligence Unit (FIU). Additionally, ICE strengthened its relationship with the Colombian TTU by deploying temporary duty personnel to work onsite and provide training. This action had an immediate, positive impact on information sharing between the U.S. and Colombia and resulted in ongoing joint criminal investigations.

TTUs identify anomalies related to cross-border trade that are indicative of international trade-based money laundering. TTUs generate, initiate and support investigations and prosecutions related to trade-based money laundering, the illegal movement of criminal proceeds across international borders, alternative money remittance systems, and other financial crimes. By sharing trade data, ICE and participating foreign governments are able to see both sides of import and export transactions for commodities entering or exiting their countries. This makes trade transparent and assists in the investigation of international money launderers and money laundering organizations.

## *Internal Revenue Service (IRS), Criminal Investigative Division (CID) Department of Treasury*

In 2006, the IRS Criminal Investigative Division (IRS-CID) continued its involvement in international training and technical assistance efforts designed to assist international law enforcement officers in

detecting criminal tax, money laundering and terrorism financing. With funding provided by the Department of State, IRS-CID delivered training through agency and multi-agency technical assistance programs to international law enforcement agencies. Training consisted of basic and advanced financial investigative techniques as needed. IRS-CID provided instructor and course delivery support to the International Law Enforcement Academies (ILEAs) in Bangkok, Thailand; Budapest, Hungary; Gaborone, Botswana; and San Salvador, El Salvador.

At ILEA Bangkok, IRS-CID participated in one Supervisory Criminal Investigator Course (SCIC) and was the coordinating agency of the Complex Financial Investigations (CFI) course. CFI is provided to senior, mid-level, and first-line law enforcement supervisors and officers from the countries of Cambodia, Hong Kong, Indonesia, Macau, Malaysia, Republic of China, Philippines, Singapore, Thailand, Timore-Leste, and Vietnam.

At ILEA Budapest, IRS-CID participated in six sessions, ILEA 53-58. For ILEA 58 IRS-CID provided a class coordinator to coordinate and supervise the daily duties and activities of the participants. The countries that participated in these classes are Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Georgia, Hungary, Kazakhstan, Kyrgyzstan, Macedonia, Montenegro, Moldova, Romania, Russia, Serbia, Tajikistan, and Ukraine.

IRS-CID participated in five Law Enforcement Executive Development (LEED) programs LEED 17-21 at ILEA Gaborone. Countries that participated in these classes are Angola, Botswana, Lesotho, Malawi, Mauritius, Mozambique, Namibia, South Africa, Swaziland, Tanzania, Zambia, Djibouti, Ethiopia, Kenya, Seychelles, Uganda, Nigeria, Cameroon, Comoros, Republic of the Congo, Democratic Republic of Congo (DRC), Gabon, and Madagascar. IRS-CID participated in two Latin America's Law Enforcement Development (LEMDP) programs, LEMDP 002 and 003 at ILEA San Salvador. LEMDP stresses the importance of conducting a financial investigation to further develop a large scale, criminal investigation.

IRS-CID conducted Financial Investigative Techniques (FIT) courses in Malaysia, Peru, and Philippines. These programs focused on Financial Investigative Techniques while investigating criminal tax, money laundering and terrorism financing investigations. The twenty-four participants that attended the week long course in included members of the Royal Malaysian Police, Inland Revenue Board, members of the Intelligence and Special Investigative Unit, Central Bank of Malaysia, Ministry of Finance, and Customs. Two one-week classes were presented in Lima, Peru, to forty (40) law enforcement officials, prosecutors and judges from Peru and Brazil. The curriculum was designed to parallel the progress of a simulated case exercise. The week-long course in Manila, Philippines attended by forty-three (43) participants from twenty-five (25) different organizations completed FIT training. The curriculum consisted of techniques focusing on money laundering with attention called to the unlawful activities of drug trafficking, public corruption, terrorism financing and kidnapping for ransom.

In Kuwait, IRS-CID presented a one-week conference with a total of forty seven participants from seventeen different federal agencies and banks. In Dhaka, Bangladesh IRS-CID conducted both a one-week basic and a one-week advanced course, which provided a more in-depth, and comprehensive look at financial investigations. In accordance with the International Criminal Investigative Training Assistance Program (ICITAP) IRS-CID conducted six advanced money laundering classes in Bogotá, Colombia. This training provided along with the Federal Law Enforcement Training Center (FLETC), was the first multi-agency joint effort to develop, coordinate and instruct an advanced money laundering course based on the new accusatory judicial system in Colombia. Along with the participation of the Attaché in Bogotá, approximately 144 judges, magistrates, government attorneys, and law enforcement officers received instruction on financial investigative techniques focusing on working a case from start to completion.

IRS-CID continued to assist the FBI in delivering multiple one-week courses on anti-money laundering and antiterrorism financing. During 2006, the course was successfully delivered to participants in Tanzania, Indonesia, United Arab Emirates, Jordan, Egypt, Philippines, and Pakistan. In conjunction with the Office of Overseas Prosecutorial Development Assistance and Training (OPDAT), IRS-CID presented an Asset Forfeiture Unit course. Participants included 140 participants composed of advocates, investigators and administrative personnel of the National Prosecuting Authority of South Africa.

The National Criminal Investigation Training Academy (NCITA) hosted a delegation of four investigators from Her Majesty's Revenue & Customs (HMRC) of the United Kingdom for a week long Money Laundering Investigations Workshop. The delegates received presentations on money laundering investigative methods. The HMRC delegation also visited the Savannah CID Field Office and met with prosecutors at the U.S. Attorneys Office in Savannah (Southern Judicial District of Georgia).

The IRS-CID Mexico Attaché assisted with the coordination and served as a liaison between Treasury Office of Technical Assistance Representatives and the Mexican Government Attorney Generals Office's (PGR) Money Laundering Unit Director during an Advanced Money Laundering training session for various Mexican Officials, to include prosecutors, judges, attorneys and investigators. In addition, the IRS-CID Mexico Attaché participated in a Money Laundering/Terrorist Financing Awareness Conference sponsored by the Panama Financial Investigative Unit before an audience of approximately 230 law enforcement officials from that country. This conference was sponsored by the Narcotics Affairs Section (NAS) of the U.S. Embassy and the Drug Enforcement Agency (DEA) Office in Panama. IRS-CID Hong Kong Attaché coordinated and supported a Financial Investigative Techniques/Anti-Money Laundering course in Macau in 2006. It was a week long course for approximately 45 law enforcement and regulatory participants from Macau, China.

## *Office of the Comptroller of the Currency (OCC), Department of Treasury*

The Office of the Comptroller of the Currency charters, regulates and supervises all national banks and federal branches and agencies of foreign banks. The OCC's nationwide staff of examiners conducts on-site reviews of national banks and provides sustained supervision of bank operations. They review, among other things, the bank's internal controls, internal and external audit and compliance with law, including Bank Secrecy Act (BSA) and anti-money laundering (AML) compliance.

The OCC offers three internal courses for examiners that have significant BSA/AML components; these are the Basic Consumer Compliance School, Bank Supervision School and FinCEN Database Training. The OCC also periodically develops and provides other BSA/AML training to examiners as needed, such as the Federal Financial Institutions Examination Council BSA/AML Examination Manual.

In addition to hosting BSA/AML Schools for OCC examiners, the OCC offers its AML School to foreign bank supervisors. The OCC conducted and sponsored a number of anti-money laundering (AML) training initiatives for foreign banking supervisors during 2006. In August 2006, the OCC sponsored an Anti-Money Laundering/Anti Terrorist Financing School in Washington, D.C. The school was designed specifically for foreign banking supervisors to increase their knowledge of money laundering and terrorist financing activities and of how these acts are perpetrated. The course provided a basic overview of AML examination techniques, tools, and case studies. Twenty-two banking supervisors from the following countries were in attendance: Argentina, Bahrain, Canada, Cayman Islands, Croatia, Czech Republic, Mexico, Netherlands, Nigeria, Panama, Philippines, Singapore, Slovenia, Turkey, and United Kingdom.

In October 2006, the OCC provided an instructor to the IMF sponsored Anti-Money Laundering/Combating Terrorist Financing Workshop for the Eastern Caribbean Central Bank in St. Kitts, W.I. The workshop was designed specifically for foreign banking supervisors to increase their knowledge of money laundering and terrorist financing activities and how these acts are perpetrated. The course provided a basic overview of AML examination techniques, tools and case studies. Twenty-one banking supervisors from the Eastern Caribbean Central Bank and off-shore bank regulators attended the workshop. The ECCB is the monetary authority for a group of eight islands—Anguilla, Antigua and Barbuda, Commonwealth of Dominica, Grenada, Montserrat, St Kitts and Nevis, St Lucia, and St Vincent and the Grenadines.

OCC officials participated in numerous international conferences on combating money laundering. For example, in February and March of 2006, OCC officials were part of a body of U.S. regulators presenting to the international audiences at the Florida International Bankers Association and the Money Laundering Alert's International Conference on Combating Money Laundering. In addition, the OCC's senior compliance official was a guest speaker at the Inaugural Conference on Combating Money Laundering and Terrorist Financing by the U.S.-Middle East/North Africa Private Sector Dialogue group that was held in Cairo Egypt with over 300 participants from 23 countries.

# *Office of Overseas Prosecutorial Development, Assistance and Training, the Asset Forfeiture and Money Laundering Section, & Counterterrorism Section (OPDAT, AFMLS, and CTS)), Department of Justice*

## Training and Technical Assistance

The Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT) section is the office within the Justice Department that assesses, designs and implements training and technical assistance programs for our criminal justice sector counterparts overseas. OPDAT draws upon components within the Department, such as the Asset Forfeiture and Money Laundering Section (AFMLS) and the Counterterrorism Section (CTS), to provide programmatic expertise and to develop good partners abroad. Much of the training provided by OPDAT and AFMLS is provided with the assistance of the Department of State's funding.

In 2006, OPDAT provided technical assistance in the areas outlined below. In addition to programs that are targeted to each country's specific needs, OPDAT also provides long term, in-country assistance through Resident Legal Advisors (RLAs). RLAs are federal prosecutors who provide in-country technical assistance to improve the skills, efficiency and professionalism of foreign criminal justice systems. RLAs normally live in a country for one or two years to work with counterparts such as ministries of justice, prosecutors and the courts. To promote reforms in the criminal justice system, RLAs provide assistance in legislative drafting, modernizing institutional policies and practices, and training criminal justice sector components. For all programs, OPDAT draws on the expertise of the Department of Justice's Criminal Division, National Security Division, and other components as needed. OPDAT works closely with AFMLS, the lead Justice section that provides countries with technical assistance in the drafting of money laundering and asset forfeiture statutes compliant with international standards.

## Money Laundering/Asset Forfeiture

During 2006, the Justice Department's OPDAT and AFMLS continued to provide training to foreign prosecutors, judges and law enforcement, and assistance in drafting anti-money laundering statutes compliant with international standards. The assistance provided by OPDAT and AFMLS enhances the ability of participating countries to prevent, detect, investigate, and prosecute money laundering, and to make appropriate and effective use of asset forfeiture. The content of individual technical assistance varies depending on the specific needs of the participants, but topics addressed in 2006 included developments in money laundering legislation and investigations, complying with international standards for anti-money laundering/counterterrorist financing regimes, illustrations of the methods and techniques to effectively investigate and prosecute money laundering, inter-agency cooperation and communication, criminal and civil forfeiture systems, the importance of international cooperation, and the role of prosecutors.

AFMLS provides technical assistance directly in connection with legislative drafting on all matters involving money laundering, asset forfeiture and the financing of terrorism. During 2006, AFMLS provided such assistance to 16 countries and actively participated in the drafting of the forfeiture provisions for the OAS/CICAD Model Regulations. AFMLS continues to participate in the UN Working Group to draft a model nonconviction based asset forfeiture law and the G-8 working groups on corruption and asset sharing and the CARIN Group on asset recovery.

AFMLS provided training to government officials concerned with money laundering and asset forfeiture issues in Azerbaijan, Andorra; Bangladesh, Brazil; Bulgaria; Estonia; Kosovo, Macedonia, Peru, the Republic of Korea, Sri Lanka, and Turkey. These officials attended in-depth sessions on money laundering and international asset forfeiture. Additionally, in 2006, AFMLS provided technical assistance to Afghanistan, Albania, Bangladesh, Brazil, Bulgaria, Pakistan, Indonesia, Iraq, Kenya, Kosovo, Malawi; Sri Lanka, the Republic of Korea, Tanzania, Thailand, and Turkey.

In an effort to improve international cooperation, AFMLS, in conjunction with the Italian Ministry of Justice, co-hosted a conference in Rome, Italy, April 4-6, 2006, on International Forfeiture Cooperation for prosecutors and investigators to discuss "What Works? What doesn't and Why?" Practitioners and other experienced government officials from Austria, Brazil, Canada, Denmark, Estonia, France, Guernsey, Hong Kong, Isle of Man, Ireland, Israel, Luxembourg, the Netherlands, South Africa, Sweden, United Kingdom and the United States participated. This conference brought practitioners and international experts, including representatives from Egmont, Eurojust and the private sector, together to share experiences and ideas to provide practical tools to further international cooperation in forfeiture.

With the assistance of Department of State funding, in 2006 OPDAT provided training to government officials on money laundering and financial crime related issues in more than eleven countries, including Romania, Slovenia, Nigeria, South Africa, Suriname, Malawi, Azerbaijan, and Albania. OPDAT RLAs in these countries organized in-country seminars on money laundering, asset forfeiture, terrorist financing and financial crime investigations and prosecutions.

In February 2006, OPDAT conducted a three-day conference on financial crimes, asset forfeiture and money laundering in Abuja, Nigeria, for approximately 50 Nigerian prosecutors and police. Topics included money laundering, asset forfeiture, financial investigations, prosecuting complex financial cases, and offshore banking and electronic funds transfer systems.

In February and March 2006, OPDAT organized a series of three anti-money laundering/counter terrorist financing workshops conducted by AFMLS in Ankara, Antalya, and Istanbul, Turkey, for approximately 100 Turkish prosecutors and investigators. The workshops focused on providing an interactive platform for participants to examine the tools (legislative, investigative, prosecutorial) available in financial crime cases.

In April 2006, OPDAT RLA to Bosnia and Herzegovina organized two financial crimes training seminars in Sarajevo, Bosnia and Herzegovina. Each of the two-day sessions included an in depth examination of current issues regarding financial and transnational crimes. The seminars explored various investigative techniques (money laundering detection, asset forfeiture) and the roles of different agencies (prosecutors, finance police, financial intelligence units, bank regulators).

In May 2006, OPDAT conducted an intensive three-day workshop in Paramaribo, Suriname, on best practices for financial investigations and prosecutions. The OPDAT training team, consisting of a U.S. federal prosecutor and an FBI special agent, presented the course to an audience of Surinamese prosecutors, investigators, and a legislative expert.

In July 2006, OPDAT deployed its new RLA to Azerbaijan. The RLA placed renewed emphasis on establishing a legal framework in Azerbaijan to investigate and prosecute money laundering, terrorist financing and financial crimes, including pushing for the passage of the draft AML/CFT law and the creation of a financial intelligence unit (FIU). Passage of a comprehensive AML/CFT (Anti-Money Laundering/Counter-Financing Terrorism) law and the development of an FIU that complies with international standards are significant USG priorities for Azerbaijan. OPDAT and AFMLS have provided detailed technical assistance on the draft AML/CFT law for the last year, but the draft appeared stalled. In late 2006, the RLA identified several specific obstacles to passage of this law and strategies to overcome them, with the goal of seeing the AML/CFT law passed by the end of the first quarter of 2007. These steps included engaging the government of Azerbaijan (GOAJ) at multiple levels, and creating opportunities to substantively assist the GOAJ in areas that were holding up the passage of the law. In furtherance of this strategy, the RLA took a delegation of Azerbaijani officials to an anti-money laundering conference sponsored by the SECI Center held in Moldova in September 2006. This conference impressed the Azerbaijani delegation with the progress being made by many other countries in the region and stressed the need to move forward with their own legislation in a timely manner. The RLA also coordinated with the President's Office and the Council of Europe to organize a comprehensive conference on the creation of a FIU in Azerbaijan—an issue that is significantly delaying the passage of the AML/CFT. In October 2006, the OPDAT RLA, in collaboration with AFMLS, organized the aforementioned FIU conference in Baku, Azerbaijan, for an audience of over 50 participants from a dozen different ministries and agencies, including the National Bank, the Prosecutors Office and the President's Office.

In July 2006, OPDAT RLA to South Africa coordinated a training session with participation by AFMLS for all the members of the South African Asset Forfeiture Unit (AFU). In August 2006, the RLA also arranged for three financial investigators from the AFU to attend a U.S.-based financial investigation training in New York City provided by AFMLS. All reports point to the fact that the training was substantive and very relevant to the work of an AFU investigator. These three talented investigators are now positioned as resources on financial investigation techniques for the rest of the AFU investigators and the core financial investigation competency of the AFU has increased. Of particular note during this period was the OPDAT conference on organized crime (August 28-September 1) that was attended by the National Prosecution Service and the Scorpions. For the first time and at the direction of the OPDAT RLA, attorneys from the AFU helped plan the conference and participated in the program. As a result, the conference educated South African prosecutors on the importance of prosecution components (National Prosecution Service and the Scorpions) calling upon the expertise and involvement of the AFU in the early stages of important investigations. This will help meet the AFU goal of increasing the amount of illicit proceeds that are recovered by the AFU in conjunction with significant criminal prosecutions. According to the Chief of the Pretoria Division of the AFU, the OPDAT program finally made the AFU a full law enforcement partner.

As part of Plan Colombia, in 2006, OPDAT continued to provide assistance to enhance the capability of Colombia's National Asset Forfeiture and Money Laundering Task Force to investigate and prosecute money laundering and other complex financial crimes, and to execute the forfeiture of

profits from illegal narcotics trafficking and other crimes. These efforts are complemented by a comprehensive long-range program to assist the country's judges, prosecutors and investigators in making the transition from the inquisitorial to the accusatory system

In October-November 2006, OPDAT in cooperation with the Federal Bureau of Investigation organized a week-long anti-money laundering U.S.-based study tour in Washington, DC, for a 15-person, senior-level Malaysian delegation headed by the Solicitor General of Malaysia and the Inspector General of the Royal Malaysia Police. The delegation consisted of officials from the Attorney General's Chambers, Royal Malaysia Police, Anti-Corruption Agency, Central Bank of Malaysia, Ministry of Finance, as well as representatives from other law enforcement and legal agencies. The program focused on the legal aspects surrounding money laundering investigations and prosecutions, as well as asset forfeiture and the management and disposal of forfeited properties.

## Organized Crime

During 2006, OPDAT organized a number of programs for foreign officials on transnational or organized crime, which included such topics as corruption, money laundering, implementing complex financial investigations and special investigative techniques within a task force environment, international standards, legislation, mutual legal assistance, and effective investigation techniques.

OPDAT RLAs continued to support Bosnia's Organized Crime Anti-Human Trafficking Strike Force and the Strike Force's working relationship with officials in Albania, Bulgaria, Kosovo, Macedonia, Montenegro, and Serbia—through mentoring and training programs on investigating and developing organized crime case strategies.

In February 2006, OPDAT RLA to Albania organized training for 40 prosecutors on the organized crime amendments to the Albanian Criminal Procedure Code. This training was part of a series of trainings for all 250 prosecutors in the nation, addressing the host of new anti-organized crime laws and Code amendments that were enacted in 2004.

Also in February 2006, OPDAT conducted a three-day conference on investigating and prosecuting terrorism and other organized crimes in Manila, Philippines. The program focused on familiarizing 22 Filipino judges, prosecutors, and investigators with methods of combating transnational organized crime and terrorism offenses, including effective investigative and prosecutorial techniques.

In March 2006, an OPDAT RLA to Macedonia organized a two-week U.S.-based study tour program on combating organized crime for a ten-member delegation from Macedonia, which consisted of seven prosecutors and three judges. The program focused on familiarizing the Macedonians with collecting evidence and building organized crime cases, especially in cases relating to trafficking in persons, corruption, narcotics, financial crime and money laundering, as well as related asset forfeiture.

In June 2006, OPDAT conducted a week-long program on combating prosecuting organized crime in Hanoi, Vietnam, for an audience of 35 Vietnamese judges, prosecutors and investigators. The program focused on the methods of combating transnational organized crime, including effective investigative and prosecutorial techniques.

In July 2006, OPDAT's RLA to Serbia organized a three-day seminar for 30 Serbian prosecutors and police officials focused on the task force approach to combating organized crime and corruption.

In September 2006, OPDAT deployed an Intermittent Legal Advisor (ILA) to Pretoria, South Africa, for a three-month assignment that focuses on assisting the South African prosecution authority in its efforts to combat organized crime. The same ILA has already completed several previous three to six-month tours of duty in South Africa. Throughout these tours of duty, the ILA developed and began implementing several iterations of a training program for prosecutors on combating organized crime and racketeering. The ILA has already trained nearly 500 prosecutors at several sessions all over the

country. In addition, the ILA is meeting with prosecutors and investigators throughout the country and conducting case audits. During this process the potential use of the South African racketeering statute is discussed. The statute is the South African equivalent of the U.S. RICO statute that has been so effective in combating organized crime in the U.S. As a result of these consultations the prosecutorial use of the racketeering statute in charging crimes has increased dramatically. Much of this increase can be attributed directly to the ILA's work in South Africa.

## Fraud/Anticorruption

In 2005, OPDAT placed two RLAs overseas in Indonesia and Nicaragua to provide technical assistance on a long-term basis specifically on corruption cases. In 2006, both RLAs continued to provide technical assistance on anticorruption matters for prosecutors and investigators to improve their investigative and prosecutorial abilities to combat public corruption. In Nicaragua, OPDAT RLA supported the creation of a vetted Anti-Corruption and Money Laundering Unit ("Task Force") that consists of members of the Nicaraguan National Police and the Attorney General's Office who are tasked with investigating money laundering and other corruption-related crimes. The RLA is helping train the Nicaraguan anticorruption specialists, making the Task Force a cornerstone in the U.S.-Nicaragua cooperation in the fight against corruption. The RLA is providing technical assistance and training to the Task Force and serves as a conduit of information between the unit and U.S. law enforcement agencies.

In May 2006, OPDAT in collaboration with AFMLS and the General Secretariat of the Organization of American States (OAS), held a seminar on the recovery of the proceeds of the acts of corruption in Miami, Florida. The workshop was in line with the G-8 and Summit of the Americas commitments to deny safe haven and assets to those who are corrupt and to those who corrupt them.

Also in May 2006, the OPDAT RLA to Indonesia organized a one-day workshop on investigating and prosecuting corruption cases in Bogor, Indonesia. The assembled 59 participants included police investigators, prosecutors, and auditors from the state auditing agency. The one-day workshop focused on familiarizing the participants with investigative and prosecutorial strategies for public corruption cases, which are not commonly used in Indonesia.

In May-June 2006, the OPDAT RLA to Bosnia and Herzegovina sponsored a three-day seminar on tax fraud cases for prosecutors and tax administrators in Sarajevo, Bosnia & Herzegovina. The 60 participants in the program included prosecutors and tax administrators from the various districts and regions of the country. The seminar taught the participants the basics of investigating and prosecuting tax fraud cases. In addition, it promoted cooperation and communication between the two groups.

## Terrorism/Terrorist Financing

Since 2001 OPDAT, the DOJ's Counterterrorism Section (CTS), and AFMLS have intensified their efforts to assist countries in developing their legal infrastructure to combat terrorism and terrorist financing. OPDAT, CTS, and AFMLS, with the assistance of other Department of Justice (DOJ) components, play a central role in providing technical assistance to foreign counterparts both to attack the financial underpinnings of terrorism and to build legal infrastructures to combat it. In this effort, OPDAT, CTS, and AFMLS work as integral parts of the U.S. Interagency Terrorist Financing Working Group (TFWG) in partnership with the Departments of State, Treasury, Homeland Security's ICE, and several other DOJ components.

OPDAT currently has seven RLAs assigned overseas who are supported by the interagency Terrorist Financing Working Group (TFWG), co-chaired by State INL and S/CT. The RLAs are located in Bangladesh, Indonesia, Kenya, Pakistan, Paraguay, Turkey, and the United Arab Emirates. Working in countries where governments are vulnerable to or may even be complicit in terrorist financing, these

RLAs focus on money laundering and financial crimes and developing counterterrorism legislation that criminalizes terrorist acts, terrorist financing, and the provision of material support or resources to terrorist organizations. The RLAs also develop technical assistance programs for prosecutors, judges and, in collaboration with DOJ's International Criminal Investigative Training Assistance Program (ICITAP), police investigators, to assist in the implementation of new anti-money laundering and counterterrorist financing procedures.

In August 2003, OPDAT dispatched its first counterterrorism RLA to Asuncion, Paraguay, part of the Tri-Border area (with Brazil and Argentina) where the rather porous borders facilitate money laundering and bulk cash smuggling. The second counterterrorism RLA arrived in Nairobi, Kenya, in December 2004, to assist with terrorism legislation, training in complex financial crimes and, in general, to bolster the capacity of the prosecutor's office. Both RLAs have conducted significant legislative reform and/or training programs during their tenure. The Paraguay RLA in 2006 continued his focus on needed reforms to the Paraguayan Criminal Procedure Code, providing counsel and technical assistance to the legislative commission assigned with the task of reform.

In January 2006, OPDAT organized a trial advocacy course in Nairobi, Kenya, following the successful trial advocacy training provided by the OPDAT RLA in August 2005. In addition to U.S. prosecutors, U.S. judges and FBI agents, presenters included two prosecutorial trainers from the U.K. Crown Prosecution Service who provided a British perspective on Kenyan legal practice. After the first OPDAT RLA to Kenya departed Nairobi in November 2005, OPDAT sent out its second RLA to Kenya in May 2006. During his first few months in country, the RLA met with all the regional offices of the Department of Public Prosecutions, setting the stage for a country-wide prosecutorial training program. The RLA also monitored the progress of the pending Kenyan counterterrorism legislation, offering DOJ expertise in guiding the development of the counterterrorism strategy for Kenya and the region as needed.

In July 2006, OPDAT sent a new counterterrorism RLA to the United Arab Emirates (UAE) to work on financial crimes, terrorist financing, and money laundering issues. The RLA immediately engaged local officials responsible for money laundering and terror finance issues. The RLA held meetings with the Anti-Money Laundering and Financial Crimes Unit (AMLFCU) of the Dubai Police Department, Criminal Investigation Division, to discuss future training and collaboration. OPDAT expanded the UAE RLA portfolio to include assistance to other states in the Gulf Region in combating money laundering and terrorist financing. In September 2006, the RLA traveled to Kuwait and Jordan to meet with the key players in the Anti-Money Laundering/Terrorist Financing (AML/TF) field in the Kuwaiti and Jordanian governments. In November 2006, the RLA again traveled to Kuwait to discuss the possibility of providing training that would strengthen the Kuwaiti FIU and the capacity of Kuwaiti prosecutors and judges to combat financial crimes. As a result, the RLA is currently in the process of planning AML/CTF trainings in both Kuwait and Jordan, set to take place in early 2007.

In December 2006, OPDAT's RLA to the UAE also engaged with Saudi Arabian officials. The RLA was a member of the U.S. delegation to the U.S.-Saudi Arabia Strategic Dialogue Working Group sessions that took place December 3-5, 2006, in Riyadh. These consultations were focused on a bilateral exchange of ideas regarding possible future technical assistance programs involving the Saudi justice sector. The results were positive and future programs in Saudi Arabia on money laundering/counter terrorism financing (including perhaps charities regulation) are anticipated.

In March 2005, OPDAT placed its first RLA in South Asia at Embassy Dhaka with the goal of assisting the Government of Bangladesh in strengthening its anti-money laundering/terrorist financing regime, and improving the capability of Bangladeshi law enforcement to investigate and prosecute complex financial and organized crimes. During 2006, the RLA continued to provide assistance to Bangladeshi officials in their efforts to establish an effective anti-money laundering and terrorist financing regime. Specifically, the RLA continued her work on forming a financial crimes task force

and a Financial Intelligence Unit (FIU) to be housed in the central bank. The RLA achieved a major step forward on task force development when she facilitated the signing, by five relevant government agencies, of an inter-agency agreement promoting the creation of a task force for money laundering and terrorist financing cases. The signing came at the end of a two day retreat organized in September for just this purpose, bringing together the key figures at each relevant agency. The group consisted of the Bank of Bangladesh (the central bank), the Attorney General's Office, the Finance Ministry (the tax authority), Criminal Investigation Division CID), and the Home Affairs Ministry. The agreement sets forth the process by which anti-money laundering cases initiated by the central bank will be investigated and prepared for trial. Among the critically important agreed upon provisos: CID will designate 6 officers to work anti-money laundering/terrorist financing (AML/TF) cases and will also work with prosecutors throughout the investigation. The September retreat represented the culmination of six months of work by the RLA.

In October 2006, the Bangladeshi Law Minister (the country's lead prosecutor) designated four attorneys to handle money laundering and terrorist financing cases on the task force. The first money laundering investigations by the task force commenced in November, based on Bank of Bangladesh referrals to the CID of suspicious transaction reports. Training for the task force members continued throughout the quarter and into the second quarter of FY2007. In November, the RLA worked with a team from the IRS to provide two weeks of interactive training for officials from four agencies on accounting methods used to detect money laundering. In December, the prosecutors dedicated to the task force participated in a workshop with DOJ Asset Forfeiture and Money Laundering Section (AFMLS) Deputy Chief Linda Samuel; particular emphasis was given to working with these prosecutors on how to anticipate defense arguments in pre-trial and trial proceedings and prepare counter arguments.

OPDAT placed its first RLA in Indonesia in June 2005. In 2006, the RLA continued his work in providing assistance to the Indonesian Counter Terrorism Task Force (CTTF) to augment their advanced criminal procedures, criminal laws, and prosecutor skills to prepare and try complex terrorism and other organized crime cases. He also assisted the general prosecutors with skill-building and integrity development to ultimately enlarge the cadre of counterterrorism prosecutors. The RLA provided legislative drafting assistance and skills development seminars, and invited experts from other components of DOJ to demonstrate techniques for effective mutual legal assistance. Upon the departure of the first RLA in June 2006, OPDAT deployed its second Indonesia RLA to Jakarta in July 2006. The new RLA helped establish the Attorney General's Terrorism and Transnational Crime Task Force as an operational unit. He negotiated and arranged for the procurement and delivery approximately $80,000 in office supplies and computers to the Task Force. As a result, the Task Force is now actively supervising cases against 21 defendants. The RLA also spoke at a regional counterterrorism conference in Makassar, Indonesia, on police/prosecutor cooperation—a major obstacle in Indonesia.

In September 2006, OPDAT deployed its first-ever RLA to Ankara, Turkey, with the goal of assisting Turkey to amend and implement effective money laundering legislation, and other related and potentially affected criminal statutes, codes, laws and regulations. In the same month, OPDAT also deployed its first ever RLA to Pakistan. The RLA spent his first month in country appraising the capacity of Pakistan's criminal justice system to function effectively. Since then, the Ambassador asked the RLA to place a heavy emphasis on laying the foundation with Pakistani prosecutors and investigators for future trainings on financial crimes.

In addition to the programs organized by the seven counterterrorism RLAs, in 2006 OPDAT conducted both bilateral and regional counterterrorism training programs. In June-July 2006, OPDAT RLA to Bosnia and Herzegovina conducted a nine-day study tour to the United States for thirteen members of the Counter-Terrorism Task Force (CTTF) of Bosnia and Herzegovina. The program introduced the delegation to the working procedures of U.S. inter-agency task forces, thereby

promoting cooperation and information sharing between and among Bosnian prosecutors and police agencies.

In April 2006, OPDAT conducted a South Asia regional seminar in Colombo, Sri Lanka, on safeguarding charities from abuse. Law enforcement officers, prosecutors, and financial sector officials from Sri Lanka, Afghanistan, Bangladesh, the Maldives, and Pakistan participated in the event. The conference stressed the importance of mutual cooperation in preventing the ability of terrorists to generate and disperse terrorist funds.

## Justice Sector Reform

In 2006 DOJ's Justice Sector Reform Program in Colombia focused on four specific areas: (1) continued assistance in implementation of accusatory system, (2) assistance in specialized areas of criminal law, (3) implementation of justice and peace law, and (4) security and protection programs. In 2006, DOJ trained over 1,000 prosecutors; 6,000 police; 300 judges; and 100 forensic scientists in the accusatory system and implementation of the new Colombian Criminal Procedure Code, most of who will be implementing the new Code in their respective judicial districts in 2007 as part of the gradual, region by region implementation of the new law. This training involved intensive, practical training in the concepts and legal underpinnings of an accusatory system and the new Code, as well as the technical skills and practical application necessary for implementation—crime scene management, forensic development and presentation of forensic evidence, witness interview, trial preparation, chain of custody and presentation of evidence at trial, trial techniques, investigation and prosecution strategy, police/prosecutor cooperation. DOJ also provided equipment to facilitate the implementation of the new Code. DOJ's assistance in specialized areas of criminal law included training for prosecutors, investigators, and forensic scientists in money laundering, antikidnapping, sex crimes, anticorruption, forensic anthropology, intellectual property, and human rights. DOJ also provided equipment and operational funds to specialized units within the Prosecutor General's Office. DOJ initiated training and technical assistance as well as providing equipment, office and court facilities development, and operational funds for the Prosecutor General's Justice and Peace Unit tasked with the investigation, interviewing and prosecution of demobilized paramilitary members under the Justice and Peace law. DOJ also provided similar assistance to the Colombian magistrates who will be involved in the court proceedings under this law. In the area of protection, DOJ continued to provide judicial protection training to Colombian protection details and began a shift in this protection training and assistance to courtroom and courthouse security. Over 200 protection personnel were trained in 2006. In addition, DOJ placed a U.S. Marshals Service (USMS) official in the Embassy in Bogota to assist the Colombian Prosecutor General's Office to develop a viable witness protection program. The goal is to train over 100 protection personnel as well as to enhance the structure for a protection program.

OPDAT currently has eight Resident Legal Advisors (RLAs) in Iraq assisting the Iraqi justice sector in enhancing sustainable institutions built on rule of law principles, with plans to expand the program in the near future. Presently, two RLAs are stationed at the Embassy in Baghdad and six RLAs are deployed as Rule of Law Coordinators to Provincial Reconstruction Teams (PRTs) in Iraqi provinces, one each in Ninewa (Mosul), Tamim (Kirkuk), Babil (Hillah), Salah ad Din (Tikrit), and Baghdad. As members of the interdisciplinary reconstruction effort, OPDAT RLAs work with local police and judges to identify and overcome obstacles to effective, fair prosecutions. The RLAs stationed at the Embassy in Baghdad advise the Multi-National Corps—Iraq, the U.S. Embassy, the Central Criminal Court of Iraq, the Iraq Ministry of Justice, and the Iraqi Higher Juridical Council on criminal justice, rule of law, and judicial capacity building.

# *Office of Technical Assistance (OTA), Treasury Department*

The Treasury Department's Office of Technical Assistance is located within the Office of the Assistant Secretary for International Affairs. OTA has five training and technical assistance programs: tax reform, government debt issuance and management, budget policy and management, financial institution reform, and, more recently, financial enforcement reform related to money laundering, and other financial crimes.

Sixty-three highly experienced intermittent and resident advisors comprise the Financial Enforcement Team. These advisors provide diverse expertise in the development of anti-money laundering/combating terrorist financing (AML/CTF) regimes, and the investigation and prosecution of complex financial crimes. The Financial Enforcement Team is divided into three regional areas: Europe and Asia; Africa and the Middle East; and the Americas. Each region is managed by a full-time regional director.

OTA receives funding from USAID country missions and direct appropriations from the U.S. Congress. OTA has been designated as the recipient of Millennium Challenge Corporation funding to provide assistance to a number of Threshold Countries to enhance their capacity to address corruption and related financial crimes.

## Assessing Training and Technical Assistance Needs

The goal of OTA's Financial Enforcement program is to build the capacity of host countries to prevent, detect, investigate, and prosecute complex international financial crimes by providing technical assistance in three primary areas: money laundering, terrorist financing, and other financial crimes; organized crime and corruption; and capacity building for financial law enforcement entities.

Before initiating any training or technical assistance to a host government, the OTA Enforcement team conducts a comprehensive assessment to identify needs and to formulate a responsive assistance program. These needs assessments address the legislative, regulatory, law enforcement, and judicial components of the various regimes, and include the development of technical assistance work plans to enhance a country's efforts to fight money laundering, terrorist financing, organized crime, and corruption. In 2006, such assessments were carried out in Ethiopia, Nigeria, Namibia, Mauritius, Seychelles, Kuwait, and Maldives.

## Anti-Money Laundering and Antiterrorism Financing Training

OTA specialists delivered anti-money laundering and antiterrorism financing courses to government and private sector stakeholders in a number of countries. These course components, included an overview of money laundering and financial crimes investigations; identifying and developing local and international sources of information; how banks and nonbank financial institutions operate, how they are regulated, and what records they keep and in what form; investigative techniques, including electronic surveillance and undercover operations; forensic evidence, including fingerprints, and ink and paper analysis; computer assistance; interviewing; case development, planning, and organization; report writing; and, with the assistance of local legal experts, rules of evidence, search, and seizure, as well as asset seizure and forfeiture procedures. OTA delivered such courses in several African countries, including Ethiopia, Lesotho, Malawi, Namibia, Senegal and Zambia. In Asia, OTA conducted financial investigative techniques training in Macau. OTA has also conducted several training sessions for Philippine border control agencies on bulk cash smuggling.

In Europe, OTA teams delivered a variety of technical assistance products, including financial investigation training programs in Bulgaria; anti-money laundering and antifraud training for the insurance and gaming industries in Romania; a "train-the-trainer" program on auditing techniques for

concerned officials in Armenia; assistance to develop the criminal tax enforcement capability of Croatia; investigative training for the financial police in Georgia; and anti-money laundering seminars for investigative agencies in Montenegro.

In the Caribbean, OTA delivered Phases II and III of a train-the-trainers initiative, begun in 2005 and centered on the Financial Investigative Techniques (FIT) course. Advisors presented the Phase I two-week course, comprising state-of-the-art techniques, to financial crimes investigators from Antigua and Barbuda, Bahamas, Barbados, Bermuda, Cayman Islands, Grenada, Guyana, Jamaica, St. Kitts & Nevis, St. Lucia, St. Vincent and the Grenadines, Trinidad and Tobago, and Turks and Caicos. Brazil also attended this first phase training course at the REDTRAC training facility in New Kingston, Jamaica. In 2006, OTA met again with students it trained at REDTRAC in 2005, and provided them with Basic Instructor Training (BIT) to prepare them to teach the FIT course on their own. Following this training, OTA advisors mentored REDTRAC trainers as they delivered the FIT course to students drawn from Caribbean law enforcement agencies charged with the investigation and prosecution of financial crimes. To ensure continued sustainability of this training effort, OTA will meet periodically with REDTRAC trainers to provide them with updates to FIT materials, thus ensuring REDTRAC's continued ability to provide the latest FIT training to Caribbean law enforcement authorities.

## Support for Financial Intelligence Units

In Afghanistan, OTA assisted in the establishment and development of a FIU as a semi-autonomous unit within Da Afghanistan Bank. In Sri Lanka, OTA's resident advisor helped to stand up an operational FIU. Resident advisors in Albania, Bulgaria, Montenegro, and Serbia continued efforts to streamline and enhance host governments' FIU's. In Senegal, OTA continued to assist the FIU in achieving operational status and begin receiving suspicious transaction reports and training its staff. In Namibia and Jordan, advisors were engaged to the respective Central Banks. In Malawi, OTA assigned a resident advisor under the Millennium Challenge Corporation Threshold Program to assist in the passage of AML/CFT laws, establish an FIU, and work to improve the capacity of the government to combat financial crimes.

## Casino Gaming

In the Casino Gaming Group, OTA combines experts from its Tax and Financial Enforcement Teams and has been providing technical assistance to the international community in the areas of Gaming Industry Regulation since 2000. The program provides assistance in the drafting of gaming legislation, and in drafting the regulations required to implement the laws. The program also includes the provision of technical training to gaming industry regulators, including FIU personnel, to provide the capacity for auditing and inspecting casino operations and all games of chance. In addition, advanced technical workshops have been conducted in Las Vegas involving regulators from participating countries. The program has been well received by host country officials who see it as both a valuable revenue-producing project and an anticorruption measure. They also view the assistance as very beneficial in fostering the host country's compliance efforts with the FATF 40 Recommendations as they relate to casinos. In 2006, the OTA Casino Gaming Group conducted an assessment in the Philippines, a follow-up assessment in Panama, and conducted technical assistance and training as described above in Antigua and Barbuda, El Salvador, Panama, Nicaragua, Chile, Montenegro and Romania. Also during 2006, the Casino Gaming Group participated in conferences in Macau and Argentina to highlight the FATF 40 Recommendations for casinos, and their obligations pursuant to the specific FATF Recommendations.

## Money Services Businesses

Money services businesses (MSB's) offer several types of services (check cashing, money transmissions, currency exchange, etc.). Because of the high volume of their cash transactions, and because account relationships with related customer identification procedures are absent, resulting in an uncertain audit trail, MSB's are vulnerable to abuse for the purpose of money laundering and terrorist financing. FATF Recommendations call upon governments to regulate MSB's.

OTA collaborated with the Caribbean Group and the Central American Council of Bank Supervisors in the organization and presentation of two workshops for the oversight, regulation, and examination of MSB's. The first, in June 2006, was a workshop hosted by the Bank of Jamaica and was presented to regulators from fifteen of its English speaking member countries. The second workshop, presented in October, was hosted by the Superintendent of Banks, Santo Domingo, Dominican Republic, in collaboration with the Central American Council of Bank Supervisors for regulators from its seven member countries.

## Insurance

In May 2006, OTA began its program to provide technical assistance relating to insurance enforcement. Compromise of an insurance system weakens an economy and provides avenues for money laundering. Since inception of the program, insurance assistance has been provided in all three OTA geographic regions. In Paraguay, OTA completed an assessment for AML assistance to establish regulation, inspection procedures, and manuals and training. In Jordan, assessment for fraud and AML purposes has been completed to establish an antifraud investigation unit; amend legislation; and establish electronic reporting and case management systems, public awareness campaigns, training and other related activities. Internal company fraud inspection procedures have been prepared for Romania. Participation in training covering both AML and fraud subjects was provided for a number of countries including Romania, Ukraine, Jordan, Jamaica, Turks and Caicos, and Anguilla. OTA also gave assistance to the National Association of Insurance Commissioners relative to international AML programs for its training efforts.

## Regional and Resident Advisors

OTA resident advisors continued international support in the areas of money laundering and terrorist financing. In April 2006, OTA placed a regional advisor in Pretoria, South Africa with regional responsibilities for Africa and the Middle East. In September 2006, OTA posted an advisor to the Africa Development Bank in Tunis, Tunisia to provide assistance in the development and implementation of an anticorruption strategy for the Bank and its member countries.

As noted, the resident advisors in Albania, Bulgaria, Montenegro, and Serbia continued efforts to streamline and enhance host governments' FIU's. Supporting national efforts against financial crimes was the focus of the resident advisors in Albania and Zambia. Resident advisors for the Caribbean focused on national efforts against financial crimes as well as on bank regulatory compliance. OTA resident advisors in Armenia and Albania provided technical assistance on internal audit. OTA continued to work with the Secretariat of the Eurasian Group to Combat Money Laundering and Terrorist Financing. OTA placed a resident advisor in Kabul, Afghanistan, in March 2006, and assisted in the establishment and development of a FIU as a semi-autonomous unit within Da Afghanistan Bank. OTA also placed a resident advisor in Colombo, Sri Lanka in August 2006. This advisor has been assisting in the development of an effective anti-money laundering and counterterrorism financing regime, to include the establishment of an FIU that meets international standards. An OTA resident advisor posted to the Asian Development Bank (ADB) at its Manila headquarters provided guidance and operational support to the financial and governance sector

operations of ADB Regional Departments relative to anti-money laundering and border controls, including the use of wireless value transfers. The advisor also provided assistance to the Philippines' Anti-Money Laundering Council that resulted in charges being filed in several high-profile money laundering cases.

Under the auspices of the Millennium Challenge Corporation Threshold Program established for Paraguay, OTA placed a resident advisor there to continue work begun in 2003 that culminated in the establishment, by Presidential Decrees, of an internal affairs unit within the Ministry of Finance, and criminal investigation units in the Customs and Tax Administrations. OTA worked with counterparts in the Ministry of Finance towards the establishment of these units; the identification, vetting, and training of personnel; and the provision of workplaces. Each of these units has made significant progress in identifying and investigating matters under its jurisdiction.

# Treaties and Agreements

## *Treaties*

Mutual Legal Assistance Treaties (MLATs) allow generally for the exchange of evidence and information in criminal and ancillary matters. In money laundering cases, they can be extremely useful as a means of obtaining banking and other financial records from our treaty partners. MLATs, which are negotiated by the Department of State in cooperation with the Department of Justice to facilitate cooperation in criminal matters, including money laundering and asset forfeiture, are in force with the following countries: Antigua and Barbuda, Argentina, Australia, Austria, the Bahamas, Barbados, Belgium, Belize, Brazil, Canada, Cyprus, Czech Republic, Dominica, Egypt, Estonia, France, Grenada, Greece, Hong Kong (SAR), Hungary, India, Israel, Italy, Jamaica, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Mexico, Morocco, the Netherlands, the Netherlands with respect to its Caribbean overseas territories (Aruba and the Netherlands Antilles), Nigeria, Panama, the Philippines, Poland, Romania, Russia, South Africa, South Korea, Spain, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Switzerland, Thailand, Trinidad and Tobago, Turkey, Ukraine, the United Kingdom, the United Kingdom with respect to its Caribbean overseas territories (Anguilla, the British Virgin Islands, the Cayman Islands, Montserrat, and the Turks and Caicos Islands) and Uruguay. MLATs have been signed by the United States but not yet brought into force with the European Union and the following countries: Colombia, Germany, Ireland, Japan, Sweden and Venezuela. The United States has also signed and ratified the Inter-American Convention on Mutual Legal Assistance of the Organization of American States. The United States is actively engaged in negotiating additional MLATs with countries around the world. The United States has also signed executive agreements for cooperation in criminal matters with the Peoples Republic of China (PRC) and Nigeria. In addition, the United States recently ratified the United Nations Convention against Corruption (UNCAC).

## *Agreements*

In addition, the United States has entered into executive agreements on forfeiture cooperation, including: (1) an agreement with the United Kingdom providing for forfeiture assistance and asset sharing in narcotics cases; (2) a forfeiture cooperation and asset sharing agreement with the Kingdom of the Netherlands; and (3) a drug forfeiture agreement with Singapore. The United States has asset sharing agreements with Canada, the Cayman Islands (which was extended to Anguilla, British Virgin Islands, Montserrat, and the Turks and Caicos Islands), Colombia, Ecuador, Jamaica, Mexico and the United Kingdom.

Treasury's Financial Crimes Enforcement Network (FinCEN) has a Memorandum of Understanding (MOU) or an exchange of letters in place with other FIUs to facilitate the exchange of information between FinCEN and the respective country's FIU. FinCEN has an MOU or an exchange of letters with the FIUs in Argentina, Australia, Belgium, Canada, Cayman Islands, France, Guatemala, Italy, Japan, Netherlands, Netherlands Antilles, Panama, Poland, Russia, Singapore, Slovenia, South Korea, Spain, and the United Kingdom.

## *Asset Sharing*

Pursuant to the provisions of U.S. law, including 18 U.S.C. § 981(i), 21 U.S.C. § 881(e)(1)(E), and 31 U.S.C. § 9703(h)(2), the Departments of Justice, State and Treasury have aggressively sought to encourage foreign governments to cooperate in joint investigations of narcotics trafficking and money laundering, offering the possibility of sharing in forfeited assets. A parallel goal has been to encourage spending of these assets to improve narcotics-related law enforcement. The long-term goal has been to encourage governments to improve asset forfeiture laws and procedures so they will be able to conduct investigations and prosecutions of narcotics trafficking and money laundering, which include asset forfeiture. The United States and its partners in the G-8 are currently pursuing a program to strengthen asset forfeiture and sharing regimes. To date, Canada, Cayman Islands, Hong Kong, Jersey, Liechtenstein, Luxembourg, Switzerland, and the United Kingdom have shared forfeited assets with the United States.

From 1989 through December 2006, the international asset sharing program, administered by the Department of Justice, shared $228,371,464.04 with foreign governments which cooperated and assisted in the investigations. In 2006, the Department of Justice transferred $26,921.94 to the Dominican Republic. Prior recipients of shared assets include:, Anguilla, Antigua and Barbuda, Argentina, the Bahamas, Barbados, British Virgin Islands, Canada, Cayman Islands, Colombia, Costa Rica, Dominican Republic, Ecuador, Egypt, Greece, Guatemala, Guernsey, Hong Kong (SAR), Hungary, Indonesia, Isle of Man, Israel, Jordan, Liechtenstein, Luxembourg, Netherlands Antilles, Paraguay, Peru, Romania, South Africa, Switzerland, Thailand, Turkey, the United Kingdom, and Venezuela.

From Fiscal Year (FY) 1994 through FY 2006, the international asset-sharing program administered by the Department of Treasury shared $27,493,927.00 with foreign governments which cooperated and assisted in successful forfeiture investigations. In FY 2006, the Department of Treasury transferred $85,895 in forfeited proceeds to Canada ($8,850) and St. Vincent & the Grenadines ($77,045). Prior recipients of shared assets include: Aruba, Australia, the Bahamas, Cayman Islands, Canada, China, Dominican Republic, Egypt, Guernsey, Honduras, Isle of Man, Jersey, Mexico, Netherlands, Nicaragua, Panama, Portugal, Qatar, Switzerland, and the United Kingdom.

# Multi-Lateral Organizations & Programs

## *The Financial Action Task Force (FATF) and FATF-Style Regional Bodies(FSRBs)*

**The Financial Action Task Force (FATF)** is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF was created in 1989 and works to generate legislative and regulatory reforms in these areas. The FATF currently has 33 members, comprising 31 member countries and territories and two regional organizations, as follows: Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, Ireland, Italy, Japan,

Luxembourg, Mexico, Netherlands, New Zealand, Norway, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, the United States, the European Commission and the Gulf Cooperation Council.

There are also a number of FATF-style regional bodies, which, in conjunction with the FATF, constitute an affiliated global network to combat money laundering and the financing of terrorism.

**The Asia Pacific Group (APG)** was officially established in February 1997 at the Fourth (and last) Asia/Pacific Money Laundering Symposium in Bangkok as an autonomous regional anti-money laundering body. The 32 APG members are as follows: Afghanistan, Australia, Bangladesh, Brunei Darussalam, Burma, Cambodia, Canada Chinese Taipei, Cook Islands, Fiji, Hong Kong India, Indonesia, Japan, Macau Malaysia, Marshall Islands, Mongolia, Nepal, New Zealand, Niue, Pakistan, Republic of Korea, Palau, Philippines, Samoa, Singapore, Sri Lanka, Thailand, Tonga, United States, and Vanuatu. Afghanistan, Burma and Canada became members at the APG July 2006 plenary in Manila.

**The Caribbean Financial Action Task Force (CFATF)** was established in 1992. CFATF has thirty members: Anguilla, Antigua & Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda, British Virgin Islands, Cayman Islands, Costa Rica, Dominica, Dominican Republic, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Montserrat, Netherlands Antilles, Nicaragua, Panama, St. Kitts & Nevis, St. Lucia, St. Vincent & the Grenadines, Suriname, Trinidad & Tobago, Turks & Caicos Islands, and Venezuela.

**The Eastern and South African Anti Money Laundering Group (ESAAMLG)** was established in 1999. Fourteen countries comprise its membership: Botswana, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Uganda, Zambia, and Zimbabwe.

**The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)** was established on October 6, 2004 and has seven members: Belarus, China, Kazakhstan, Kyrgyzstan, the Russian Federation, Uzbekistan, and Tajikistan.

**The Financial Action Task Force on Money Laundering in South America (GAFISUD)** was formally established on 8 December 2000 by the nine member states of Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru and Uruguay. Mexico became the tenth member of GAFISUD in July, 2006.

**The Groupe Inter-gouvernemental d'Action contre le Blanchiment en Afrique (GIABA)** consists of 15 countries: Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, Gambia, Ghana, Guinea Bissau, Guinea Conakry, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo.

**The Middle East and North Africa Financial Action Task Force (MENAFATF)** consists of 16 members: Algeria, Bahrain, Egypt, Jordan, Kuwait, Lebanon, Mauritania, Morocco, Oman, Qatar, Saudi Arabia, Sudan, Syria, Tunisia, United Arab Emirates, and Yemen.

## *The Egmont Group of Financial Intelligence Units*

The Egmont Group began in 1995 as a collection of a small handful of entities, today referred to as financial intelligence units (FIUs), seeking to explore ways of cooperation among themselves. The FIU concept has grown over the years and is now an important component of the international community's approach to combating money laundering and terrorist financing. To meet the standards of Egmont membership an FIU must be a centralized unit within a nation or jurisdiction to detect criminal financial activity and ensure adherence to laws against financial crimes, including terrorist financing and money laundering. Since its inception in 1995 the Egmont Group has grown dramatically from 14 units to a recognized membership of 100 FIUs. The Egmont Group now has

passed its first decade, and it is evolving toward a structure of independent units working closely together to strengthen not only their own countries' AML/CFT regime, but to strengthen the global firewall of economic resistance to money launderers and terrorist financiers.

The Egmont Group is an international network designed to improve interaction among FIUs in the areas of communications, information sharing, and training coordination. The goal of the Egmont Group is to provide a forum for FIUs around the world to improve support to their respective governments in the fight against money laundering, terrorist financing and other financial crimes. This support includes expanding and systematizing the exchange of financial intelligence information, improving expertise and capabilities of personnel employed by such organizations, and fostering better and more secure communication among FIUs through the application of technology. The Egmont Group's secure Internet system permits members to communicate with one another via secure e-mail, requesting and sharing case information as well as posting and assessing information regarding trends, analytical tools and technological developments. FinCEN, on behalf of the Egmont Group, maintains the Egmont Secure Web (ESW). Currently, there are 98 FIUs connected to the ESW.

The Egmont Group is organizationally structured to meet the challenges of the volume of membership and its workload. The Egmont Committee, a group of 14 members, is an intermediary group between the 100 Heads of member FIUs and the five Egmont Working Groups. This Committee addresses the administrative and operational issues facing Egmont and is comprised of seven permanent members and seven regional representatives based on continental groupings (i.e., Asia, Europe, the Americas, Africa and Oceania). In addition to the Committee there are five Working Groups: Legal, Operational, Training, Information Technology and Outreach. The Legal Working Group reviews the candidacy of potential members and handles all legal aspects and matters of principle within the Egmont Group. The Training Working Group looks at ways to communicate more effectively, identifies training opportunities for FIU personnel and examines new software applications that might facilitate analytical work. The Outreach Working Group concentrates on expanding and developing the FIU global network by identifying countries that have established or are establishing FIUs. Outreach is responsible for making initial contact with potential candidate FIUs, and conducts assessments to determine if an FIU is ready for Egmont membership. The Operational Working Group is designed to foster increased cooperation among the operational divisions of the member FIUs and coordinate the development of studies and typologies—using data collected by the FIUs—on a variety of subjects useful to law enforcement. The Information Technology (IT) Working Group promotes collaboration and information sharing on IT matters among the Egmont membership, in particular looking to increase the efficiency in the allocation of resources and technical assistance regarding IT systems. The Committee and the Working Groups meet at a minimum three times per year, including the annual plenary session.

To meet an ever-growing demand in terms of volume and complexity, the Egmont Group decided in June 2005 that a change was necessary to allow Egmont to meet its objectives and continue to grow and adapt to emerging trends. Consensual agreement by all Egmont members was reached for the creation of an Egmont Secretariat, the first step for Egmont to sustain, and more importantly enhance, its role in the global fight against money laundering and terrorist financing. With Egmont's input and expertise in increasing demand by other players on the global stage, the creation of the Secretariat will allow for consistent and active collaboration with other international organizations. The new Egmont Secretariat, to be located in Toronto, Canada, will begin setup and staffing by mid-2007, and is expected to be fully operational by 2008.

As of December 2006, the 100 members of the Egmont Group are Albania, Andorra, Anguilla, Antigua and Barbuda, Argentina, Aruba, Australia, Austria, Bahamas, Bahrain, Barbados, Belgium, Belize, Bermuda, Bolivia, Bosnia and Herzegovina, Brazil, British Virgin Islands, Bulgaria, Canada, Cayman Islands, Chile, Colombia, Cook Islands, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominica, Egypt, El Salvador, Estonia, Finland, France, Georgia, Germany, Gibraltar,

Greece, Grenada, Guatemala, Guernsey, Honduras, Hong Kong, Hungary, Iceland, Indonesia, Ireland, Isle of Man, Israel, Italy, Japan, Jersey, Latvia, Lebanon, Liechtenstein, Lithuania, Luxembourg, Macedonia, Malaysia, Malta, Marshall Islands, Mauritius, Mexico, Monaco, Montenegro, Netherlands, Netherlands Antilles, New Zealand, Norway, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Qatar, Romania, Russia, San Marino, Serbia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, St. Kitts & Nevis, St. Vincent & the Grenadines, Sweden, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States, Vanuatu and Venezuela.

## *The Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Group of Experts to Control Money Laundering*

The Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) is responsible for combating illicit drugs and related crimes, including money laundering. In 2006, the commission carried out a variety of anti-money laundering and counterterrorist financing initiatives. These included amending model regulations for the hemisphere to include techniques to combat terrorist financing, developing a variety of associated training initiatives, and participating in a number of anti-money laundering/counterterrorism meetings. This work in the area of money laundering and financial crimes also figures prominently in CICAD´s Multilateral Evaluation Mechanism (MEM), which involves the participation of all 34 member states; beginning this year, however, the mechanism will use reports form the Financial Action Task Force (FATF), Caribbean Action Task Force (CFATF), and Financial Action Task Force of South America (GAFISUD) to prepare its evaluation.

CICAD's Group of Experts on Money Laundering met twice in 2006, first in Washington in May and later in El Salvador in November. This year's agenda included three primary themes—seizures, international funds, and financial remittances—and included special presentations by the OAS Secretary General, as well as by representatives of the United Nations, the Inter-American Development Bank (IDB), GAFISUD, the Government of Spain, the OAS Office of Legal Cooperation, and the Inter-American Committee against Terrorism (CICTE).

In his opening remarks during the first meeting the Secretary General proposed a CICAD assistance program to help member states provide funds to the Commission by each member state setting aside a small percentage (less than one percent) of revenue from seized assets. This revenue would support CICAD activities, such as specialized training. He reiterated the proposal at the OAS General Assembly in the Dominican Republic. The proposal will need to be considered further in terms of its voluntary nature and member states will need to consider whether they have legal authority to use seized assets in this manner.

### Training and Technical Assistance

The Department if State Bureau of International Narcotics and Law Enforcement provided full or partial funding for many of the CICAD training programs conducted in 2006. Training efforts in money laundering control focused on judges, prosecutors, police officers, customs agents, the financial analysts and computer specialists of the financial intelligence units (FIUs), and compliance officers of financial institutions. Workshops for judges and prosecutors were held in the Dominican Republic, Honduras, Panama, Guatemala and Nicaragua. The courses were led by four international specialists (from Spain and Chile) as well as national experts. Subjects included, among others, money laundering doctrine, proof, international cooperation and special investigative techniques.

In a joint initiative with the United Nations and recently the IDB, mock trials were held in the Dominican Republic, El Salvador, Costa Rica and Chile. These exercises are based on real cases of money laundering and are aimed at judges, prosecutors and public defenders, as well as experts from financial intelligence units and the police who participated as witnesses in many cases.

"Train the trainer" training was also provided to law enforcement agents (police, customs, prosecutors) from Honduras, El Salvador, Nicaragua, Guatemala, Costa Rica, Panama, the Dominican Republic and Brazil. As part of the follow-up to the program, memoranda of understanding were signed with Uruguay, Bolivia, Paraguay and Peru, through which computer hardware was acquired so that the course could be replicated in each country.

With the assistance of the government of Spain and the participation of the United Nations Office on Drugs and Crime, CICAD carried out a pilot project to promote operations coordination among the police, financial intelligence units and prosecutors. A workshop, attended by Honduras, El Salvador, Nicaragua, Guatemala, Costa Rica, Panama, and the Dominican Republic, consisted of a mock investigation, based on real cases, during which agents from the institutions involved resolved a case of money laundering, and prepared the case for trial.

Technical assistance was focused on the establishment and development of financial intelligence units (FIUs) project. Beneficiaries were Costa Rica, El Salvador, Nicaragua, Panama, Honduras, the Dominican Republic, Uruguay, Ecuador and Colombia. The program, which was completed in December, provided assistance in the areas of staff training, organizational design, information system design, and technology acquisition. Staff participated in two regional workshops on basic tools for the analysis of financial information. In each of the countries, workshops included practical exercises in information analysis using computer software. In one of the sessions of these workshops, compliance officers from national financial institutions received special training to improve reports they submit to FIUs.

In the second half of 2006, the CICAD Anti-Money Laundering section began an ambitious new project for law enforcement agencies and prosecutors to develop a database classifying the many different types of money laundering, standardizing the terminology for describing each and cataloguing the real and potential law enforcement responses to detect, investigate and prosecute each type of money laundering. The database is being tested in workshops to explain its application. The first of these was held in Mexico on November 21-23, 2006

### Other Activities

Representatives participated in the following seminars, conferences and forums: GAFISUD, the first Meeting on Information Technology of the Financial Intelligence Units of South America, and the INTERPOL Group of Experts on Money Laundering. At the same time, contact was maintained with GAFISUD, CFATF, and the IMF to establish coordination for the programs and projects administered by these organizations.

## *Pacific Anti-Money Laundering Program (PALP)*

The Pacific Islands Forum (PIF) was formed in 1971, and includes the 16 independent and self-governing Pacific Island countries: Australia, Cook Islands, Federated States of Micronesia, Fiji, Kiribati, Nauru, New Zealand, Niue, Palau, Papua New Guinea, Republic of the Marshall Islands, Samoa, Solomon Islands, Tonga, Tuvalu and Vanuatu. The United States cooperates closely with the PIF and participates in the annual Post-Forum Dialogue with the PIF and member-states.

The U.S. State Department's Bureau for International Narcotics and Law Enforcement Affairs contributed $1.5 million to the PIF to fund the first year of the Pacific Anti-Money Laundering

Program (PALP)- a four-year program designed to develop viable anti-money laundering/ counterterrorist finance regimes in the fourteen non-FATF member states of the PIF. Full-time and intermittent residential mentors provide regional and bilateral training in all elements required to establish viable anti-money laundering/counterterrorist financing regimes that comport with international standards. PALP is committed to maximizing the institution-building benefits of its assistance by delivering it in both sequential and parallel steps. The steps, while tailored to each country's unique needs, include assistance in the following areas:

- Drafting and enacting comprehensive anti-money laundering and counterterrorist financing laws that have measures that enable states to freeze and seize assets and comply with the FATF's "40+9" recommendations on money laundering and terrorist financing;
- Establishing a regulatory regime to oversee compliance of the formal and informal financial sectors with international standards;
- Creating, equipping, and enhancing existing FIUs so that they can collect, analyze, collate, and disseminate suspicious transactions reports and other forms of financial intelligence to both help develop cases domestically and share information internationally through FIUs in other countries as part of transnational investigations; and
- Training law enforcement agents, prosecutors, and judges so that they have the skills to successfully investigate and prosecute financial crimes including the financing of terrorism.

## *United Nations Global Programme Against Money Laundering*

The United Nations is one of the most experienced global providers of anti-money laundering (AML) training and technical assistance and, since 9-11, counterterrorist financing, training, and technical assistance. The United Nations Global Programme against Money Laundering (GPML), part of the United Nations Office on Drugs and Crime (UNODC), was established in 1997 to assist Member States to comply with the UN Conventions and other instruments that deal with money laundering and terrorist financing. These now include the United Nations Convention against Trafficking in Narcotics and Psychotropic Substances (the Vienna Convention), the United Nations International Convention for the Suppression of the Financing of Terrorism, the United Nations Convention against Transnational Organized Crime (the Palermo Convention), and the United Nations Convention against Corruption (the Merida Convention). On September 2006, the UN General Assembly adopted the United Nations Global Counter-Terrorism Strategy. The Plan of Action contained in the Strategy encourages the UNODC to help countries comply with international norms and standards and to enhance international cooperation in these areas. The GPML is the focal point for anti-money laundering within the UN system and a key player in strengthening efforts to counter the financing of terrorism efforts. The Programme provides technical assistance and training in the development of related legislation, infrastructure and skills, directly assisting Member States in the detection, seizure and confiscation of illicit proceeds. Since 2001, GPML's technical assistance work on countering the financing of terrorism has in fact also received priority. The GPML now incorporates a focus on counterterrorist financing (CTF) in all its technical assistance work. In 2006, the GPML provided training and long-term assistance in the development of viable anti-money laundering/counterterrorism regimes to more than fifty countries.

## The Mentoring Programme

The GPML's Mentor Programme is one of the most successful and well-known activities of international AML/CTF technical assistance and training, and is increasingly serving as a model for other organizations' initiatives. It is one of the core activities of the GPML technical assistance program and is highly regarded by the AML/CTF community. The GPML's Mentor Programme has key advantages over more traditional forms of technical assistance. First, Mentors serve as residential advisors in a country or region for as long as one to four years and offer sustained skills and knowledge transfer. Second, mentoring constitutes a unique form of flexible, ongoing needs assessment, where the mentor can pinpoint specific needs over a period of months, and adjust his/her work plan to target assistance that responds to those needs. Third, the Member State has access to an "on-call" resource to provide advice on real cases and problems as they arise. Fourth, a mentor can facilitate access to foreign counterparts for international cooperation and mutual legal assistance at the operational level by using his/her contacts to act as a bridge to the international community.

The GPML Mentoring Programme provides targeted on-the-job training that adapts international standards to specific local/national situations, rather then the traditional training seminar. The concept originated in response to repeated requests from Member States for longer-term international assistance in this technically demanding and rapidly evolving field. The GPML provides experienced prosecutors and law enforcement personnel who work side-by-side with their counterparts in a target country for several months at a time on daily operational matters to help develop capacity. Some advise governments on legislation and policy, while others focus on operating procedures, either with law enforcement or with issues relating to country's FIU. By giving in-depth support upon request, the mentors have gained the confidence of the recipient institutions, which enables the achievement of concrete and significant outputs.

In 2006, a GPML prosecutorial mentor was placed in the Prosecutor General's Office of Namibia, providing assistance for the development of asset forfeiture mechanisms in Botswana, Namibia, Zambia and Zimbabwe. The Mentor provided legal inputs to amend relevant legislation in each country, specifically the AML regulations pursuant to the Proceeds of Crime Act of Namibia and the Proceeds of Serious Crime Act 1990 in Botswana. He also completed analysis of respective asset confiscation programmes.

The UN mentor based in Tanzania with the Secretariat of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) delivered training to 14 countries and assisted the ESAAMLG Secretariat in conducting the first ESAAMLG Developmental Strategic Implementation (DSI), a technical assistance needs analysis exercise in Lesotho in July. GPML placed a dedicated law enforcement advisor in Kenya to assist building financial investigation capacity for Ethiopia, Eritrea, Kenya, Tanzania and Uganda. A capacity enhancement workshop on financial investigations techniques for Kenyan law enforcement officials was conducted in November 2006. The Advisor together with the UN Mentor to ESAAMLG also delivered an AML/CFT awareness- raising seminar for the financial sector in Ethiopia and completed an AML/CFT needs assessment mission in that country. In collaboration with the World Bank and the U.S. Department of State, the GPML extended the appointment for a regional mentor for Central Asia in Almaty, Kazakhstan focusing on legislative assistance and FIU development, as well as an AML/CFT mentor in Hanoi, Vietnam to provide assistance to Vietnam, Lao PDR and Cambodia in the field of financial investigations and the overall development of viable AML/CTF regimes. In January, a law enforcement advisor for the Middle East and North Africa based in UNODC Field Office in Cairo started to provide technical assistance including legislative drafting and to conduct needs assessment missions. Mentors and experts supported the development of the legal, administrative, analytical and international co-operation capacity of other national governments. In addition, the GPML assisted in legislative drafting for many countries, including Yemen, Ghana, Kazakhstan, Kyrgyzstan Tajikistan and the countries of the

West African Economic and Monetary Union. The GPML conducted a workshop on AML/CTF for prosecutors in Central and Eastern Europe, jointly organized with the OSCE in September.

## Mentoring & Financial Intelligence Units

The GPML was among the first technical assistance providers to recognize the importance of countries' creating a financial intelligence capacity, and GPML mentors worked extensively with the development and the implementation phases of FIUs in several countries in the Eastern Caribbean, the Pacific and, most recently southeast Asia. Mentors working with FIUs, upon request of a Member State, will return to provide additional assistance to a country's FIU, as will likely occur for a six-month period in 2007 or 2008 with the FIU in Manila. The development of FIUs in the Eastern Caribbean played a key role in the removal of many of the jurisdictions being removed from the FATF Non-Cooperative and Countries and Territories list.

An FIU intermittent mentor provided assistance to emerging FIUs in Africa and the Caucasus, including a "train-the-trainers" program for law enforcement, the FIU, and prosecutors in Armenia.

A major initiative that may have global implications for many FIUs, is an ongoing initiative with UNODC IT Section that with the GPML has been working towards the development of a suspicious transactions reporting software package, GoAML, for potential deployment in FIUs that will soon be field-tested with the Nigerian FIU.

## Computer Based Training

Other highlights of GPML's work in 2006 included the ongoing development of its global computer-based training (CBT) initiative. The program provides 12 hours of interactive basic AML training for global delivery. Delivery continued in the Pacific, Central American, and Western Africa regions. CBT training classrooms were established in Dakar, Senegal at the financial intelligence unit (CENTIF) and the Police College as well as in classrooms in ten Caribbean jurisdictions. The GPML piloted CBT in multiple locations throughout Africa, Middle East and North Africa, Central Asia, and Latin America, and developed and piloted new language versions including Spanish, Amharic, Arabic and Russian.

The training program has flexibility in terms of language, level of expertise, target audience, and theme. Computer-based training is particularly applicable in countries and regions with limited resources and law enforcement skills as it can be used for a sustained period of time. As an approach, CBT lends itself well to the GPML's global technical assistance operations.

In response to countries' concerns about the difficulties of implementing AML/CTF policies in cash-based economies, and the prevalence in some regions of cash couriers, the GPML is working toward the development of CBT modules to address AML/CFT requirements in a cash-based context.

## Other GPML Initiatives

GPML contributed to the delivery of mock trials in Central and South America. This tailor-made activity was developed in response to repeated requests from Member States for practical realistic AML training. It combines training and practical aspects of the judicial work into one capacity building exercise. In 2006, the GPML, in a collaborative effort with the IMF, completed the revision of a model law on AML/CFT for civil law countries, encompassing worldwide AML/CFT standards and taking into account best legal practices. The GPML continued to work closely with the U.S. Department of Justice, U.S Treasury's Office of Technical Assistance (OTA) and the Organization for Security and Cooperation in Europe (OSCE) to deliver CTF training, particularly in the regions of Central Asia region, Southern Europe and Africa.

The GPML administers the Anti-Money Laundering International Database (AMLID) on the International Money Laundering Information Network (IMoLIN), an online, password-restricted analytical database of national AML/CFT legislation that is available only to public officials. The GPML also maintains an online AML/CTF legal library. IMoLIN (www.imolin.org) is a practical tool in daily use by government officials, law enforcement and lawyers. The Programme manages and constantly updates this database on behalf of the UN and ten major international partners in the field of anti-money laundering/countering the financing of terrorism: the Asia/Pacific Group on Money Laundering (APG), the Caribbean Financial Action Task Force (CFATF), the Commonwealth Secretariat, the Council of Europe-MONEYVAL- the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), the Eurasian Group (EAG), the Financial Action Task Force (FATF), Interpol, The Financial Action Task Force of South America (GAFISUD) and the Organization of American States (OAS). In February 2006, the GPML launched the second round of legal analysis utilizing the recently revised AMLID questionnaire. In this regard, the database currently reflects thirty-six revised questionnaires under the second round of legal analysis and an additional fifteen questionnaires are in various stages of being finalized. The updated AMLID questionnaire reflects new money laundering trends and standards, and takes provisions related to terrorist financing and other new developments in to account, including the revised FATF recommendations.

# Major Money Laundering Countries

Every year, U.S. officials from agencies with anti-money laundering responsibilities meet to assess the money laundering situations in 200 jurisdictions. The review includes an assessment of the significance of financial transactions in the country's financial institutions that involve proceeds of serious crime, steps taken or not taken to address financial crime and money laundering, each jurisdiction's vulnerability to money laundering, the conformance of its laws and policies to international standards, the effectiveness with which the government has acted, and the government's political will to take needed actions.

The 2007 INCSR assigned priorities to jurisdictions using a classification system consisting of three differential categories titled Jurisdictions of Primary Concern, Jurisdictions of Concern, and Other Jurisdictions Monitored.

The "Jurisdictions of Primary Concern" are those jurisdictions that are identified pursuant to the INCSR reporting requirements as "major money laundering countries." A major money laundering country is defined by statute as one "whose financial institutions engage in currency transactions involving significant amounts of proceeds from international narcotics trafficking." However, the complex nature of money laundering transactions today makes it difficult in many cases to distinguish the proceeds of narcotics trafficking from the proceeds of other serious crime. Moreover, financial institutions engaging in transactions involving significant amounts of proceeds of other serious crime are vulnerable to narcotics-related money laundering. The category "Jurisdiction of Primary Concern" recognizes this relationship by including all countries and other jurisdictions whose financial institutions engage in transactions involving significant amounts of proceeds from all serious crime. Thus, the focus of analysis in considering whether a country or jurisdiction should be included in this category is on the significance of the amount of proceeds laundered, not of the anti-money laundering measures taken. This is a different approach taken than that of the FATF Non-Cooperative Countries and Territories (NCCT) exercise, which focuses on a jurisdiction's compliance with stated criteria regarding its legal and regulatory framework, international cooperation, and resource allocations.

All other countries and jurisdictions evaluated in the INCSR are separated into the two remaining groups, "Jurisdictions of Concern" and "Other Jurisdictions Monitored," on the basis of a number of

factors that may include: (1) whether the country's financial institutions engage in transactions involving significant amounts of proceeds from serious crime; (2) the extent to which the jurisdiction is or remains vulnerable to money laundering, notwithstanding its money laundering countermeasures, if any (an illustrative list of factors that may indicate vulnerability is provided below); (3) the nature and extent of the money laundering situation in each jurisdiction (for example, whether it involves drugs or other contraband); (4) the ways in which the United States regards the situation as having international ramifications; (5) the situation's impact on U.S. interests; (6) whether the jurisdiction has taken appropriate legislative actions to address specific problems; (7) whether there is a lack of licensing and oversight of offshore financial centers and businesses; (8) whether the jurisdiction's laws are being effectively implemented; and (9) where U.S. interests are involved, the degree of cooperation between the foreign government and U.S. government agencies. Additionally, given concerns about the increasing interrelationship between inadequate money laundering legislation and terrorist financing, terrorist financing is an additional factor considered in making a determination as to whether a country should be considered an "Other Jurisdiction Monitored " or a "Jurisdiction of Concern". A government (e.g., the United States or the United Kingdom) can have comprehensive anti-money laundering laws on its books and conduct aggressive anti-money laundering enforcement efforts but still be classified a "Primary Concern" jurisdiction. In some cases, this classification may simply or largely be a function of the size of the jurisdiction's economy. In such jurisdictions quick, continuous and effective anti-money laundering efforts by the government are critical. While the actual money laundering problem in jurisdictions classified "Concern" is not as acute, they too must undertake efforts to develop or enhance their anti-money laundering regimes. Finally, while jurisdictions in the "Other" category do not pose an immediate concern, it will nevertheless be important to monitor their money laundering situations because, under certain circumstances, virtually any jurisdiction of any size can develop into a significant money laundering center.

## *Vulnerability Factors*

The current ability of money launderers to penetrate virtually any financial system makes every jurisdiction a potential money laundering center. There is no precise measure of vulnerability for any financial system, and not every vulnerable financial system will, in fact, be host to large volumes of laundered proceeds, but a checklist of what drug money managers reportedly look for provides a basic guide. The checklist includes:

- Failure to criminalize money laundering for all serious crimes or limiting the offense to narrow predicates.
- Rigid bank secrecy rules that obstruct law enforcement investigations or that prohibit or inhibit large value and/or suspicious or unusual transaction reporting by both banks and nonbank financial institutions.
- Lack of or inadequate "know-your-client" requirements to open accounts or conduct financial transactions, including the permitted use of anonymous, nominee, numbered or trustee accounts.
- No requirement to disclose the beneficial owner of an account or the true beneficiary of a transaction.
- Lack of effective monitoring of cross-border currency movements.
- No reporting requirements for large cash transactions.
- No requirement to maintain financial records over a specific period of time.

- No mandatory requirement to report suspicious transactions or a pattern of inconsistent reporting under a voluntary system; lack of uniform guidelines for identifying suspicious transactions.
- Use of bearer monetary instruments.
- Well-established nonbank financial systems, especially where regulation, supervision, and monitoring are absent or lax.
- Patterns of evasion of exchange controls by legitimate businesses.
- Ease of incorporation, in particular where ownership can be held through nominees or bearer shares, or where off-the-shelf corporations can be acquired.
- No central reporting unit for receiving, analyzing and disseminating to the competent authorities information on large value, suspicious or unusual financial transactions that might identify possible money laundering activity.
- Lack of or weak bank regulatory controls, or failure to adopt or adhere to Basel Committee's "Core Principles for Effective Banking Supervision", especially in jurisdictions where the monetary or bank supervisory authority is understaffed, under-skilled or uncommitted.
- Well-established offshore financial centers or tax-haven banking systems, especially jurisdictions where such banks and accounts can be readily established with minimal background investigations.
- Extensive foreign banking operations, especially where there is significant wire transfer activity or multiple branches of foreign banks, or limited audit authority over foreign-owned banks or institutions.
- Jurisdictions where charitable organizations or alternate remittance systems, because of their unregulated and unsupervised nature, are used as avenues for money laundering or terrorist financing.
- Limited asset seizure or confiscation authority.
- Limited narcotics, money laundering, and financial crime enforcement and lack of trained investigators or regulators.
- Jurisdictions with free trade zones where there is little government presence or other supervisory authority.
- Patterns of official corruption or a laissez-faire attitude toward the business and banking communities.
- Jurisdictions where the U.S. dollar is readily accepted, especially jurisdictions where banks and other financial institutions allow dollar deposits.
- Well-established access to international bullion trading centers in New York, Istanbul, Zurich, Dubai and Mumbai.
- Jurisdictions where there is significant trade in or export of gold, diamonds and other gems.
- Jurisdictions with large parallel or black market economies.
- Limited or no ability to share financial information with foreign law enforcement authorities.

# *Changes in INCSR Priorities for 2006*

Jurisdiction moving from the Primary Concern Column to the Concern column: *Hungary.*

Jurisdictions moving from the Concern Column to the Primary Concern Column: *Iran, Kenya.*

Jurisdictions moving from the Other Column to the Concern Column: *Iraq, Moldova, Senegal.*

In the Country/Jurisdiction Table on the following page, "major money laundering countries" that are in the "Jurisdictions of Primary Concern" column are identified for purposes of statutory INCSR reporting requirements. Identification as a "major money laundering country" is based on whether the country or jurisdiction's financial institutions engage in transactions involving significant amounts of proceeds from serious crime. It is not based on an assessment of the country or jurisdiction's legal framework to combat money laundering; its role in the terrorist financing problem; or the degree of its cooperation in the international fight against money laundering, including terrorist financing. These factors, however, are included among the vulnerability factors when deciding whether to place a country in the "concern" or "other" column. This year, the movement of Iraq from the Other Column to the Concern Column was based on its vulnerability to terrorist financing.

Note: Country reports are provided for only those countries listed in the "Other/Monitored" column that have received training or technical assistance funded directly or indirectly by INL in 2006. A report on Kosovo and the newly independent country of Montenegro also appears in this year's INCSR but a decision regarding their placement on the County/Jurisdiction Table has been postponed until next year.

# Country/Jurisdiction Table

## Countries/Jurisdictions of Primary Concern

Afghanistan
Antigua and Barbuda
Australia
Austria
Bahamas
Belize
Bosnia and Herzegovina
Brazil
Burma
Cambodia
Canada
Cayman Islands
China, People Rep
Colombia
Costa Rica
Cyprus
Dominican Republic
France
Germany
Greece
Guatemala
Guernsey
Haiti
Hong Kong
India
Indonesia
Iran
Isle of Man
Israel
Italy
Japan
Jersey
Kenya
Latvia
Lebanon
Liechtenstein
Luxembourg
Macau
Mexico
Netherlands
Nigeria
Pakistan
Panama
Paraguay
Philippines
Russia
Singapore
Spain
St. Kitts & Nevis
Switzerland
Taiwan
Thailand
Turkey
Ukraine
United Arab Emirates
United Kingdom
United States
Uruguay
Venezuela

## Countries/Jurisdictions of Concern

Albania
Algeria
Angola
Argentina
Aruba
Bahrain
Bangladesh
Barbados
Belarus
Belgium
Bolivia
British Virgin Islands
Bulgaria
Chile
Comoros
Cook Islands
Cote d'Ivoire
Czech Rep
Dominica
Ecuador
Egypt
El Salvador
Gibraltar
Grenada
Guyana
Honduras
Hungary
Iraq
Ireland
Jamaica
Jordan
Korea, North
Korea, South
Kuwait
Laos
Malaysia
Moldova
Monaco
Morocco
Netherlands Antilles
Nicaragua
Palau
Peru
Poland
Portugal
Qatar
Romania
Samoa
Saudi Arabia
Senegal
Serbia
Seychelles
Sierra Leone
Slovakia
South Africa
St. Lucia
St. Vincent
Syria
Tanzania
Turks and Caicos
Uzbekistan
Vanuatu
Vietnam
Yemen
Zimbabwe

## Other Countries/Jurisdictions Monitored

Andorra
Anguilla
Armenia
Azerbaijan
Benin
Bermuda
Botswana
Brunei
Burkina Faso
Burundi
Cameroon
Cape Verde
Central African Republic
Chad
Congo, Dem Rep of
Congo, Rep of
Croatia
Cuba
Denmark
Djibouti
East Timor
Equatorial Guinea
Eritrea
Estonia
Ethiopia
Fiji
Finland
Gabon
Gambia
Georgia
Ghana
Guinea
Guinea-Bissau
Iceland
Kazakhstan
Kyrgyz Republic
Lesotho
Liberia
Lithuania
Macedonia
Madagascar
Malawi
Maldives
Mali
Malta
Marshall Islands
Mauritania
Mauritius
Micronesia FS
Mongolia
Montserrat
Mozambique
Namibia
Nauru
Nepal
New Zealand
Niger
Niue
Norway
Oman
Papua New Guinea
Rwanda
San Marino
Sao Tome & Principe
Slovenia
Solomon Islands
Sri Lanka
Suriname
Swaziland
Sweden
Tajikistan
Togo
Tonga
Trinida and Tobago
Tunisia
Turkmenistan
Uganda
Zambia

# Introduction to Comparative Table

The comparative table that follows the Glossary of Terms below identifies the broad range of actions, effective as of December 31, 2006 that jurisdictions have, or have not, taken to combat money laundering. This reference table provides a comparison of elements that define legislative activity and identify other characteristics that can have a relationship to money laundering vulnerability.

### *Glossary of Terms*

1. "Criminalized Drug Money Laundering": The jurisdiction has enacted laws criminalizing the offense of money laundering related to drug trafficking.
2. "Criminalized Beyond Drugs": The jurisdiction has extended anti-money laundering statutes and regulations to include nondrug-related money laundering.
3. "Record Large Transactions": By law or regulation, banks are required to maintain records of large transactions in currency or other monetary instruments.
4. "Maintain Records Over Time": By law or regulation, banks are required to keep records, especially of large or unusual transactions, for a specified period of time, e.g., five years.
5. "Report Suspicious Transactions": By law or regulation, banks are required to record and report suspicious or unusual transactions to designated authorities. On the Comparative Table the letter "M" signifies mandatory reporting; "P" signifies permissible reporting.
6. "Financial Intelligence Unit": The jurisdiction has established an operative central, national agency responsible for receiving (and, as permitted, requesting), analyzing, and disseminating to the competent authorities disclosures of financial information concerning suspected proceeds of crime, or required by national legislation or regulation, in order to counter money laundering. These reflect those jurisdictions that are members of the Egmont Group.
7. "System for Identifying and Forfeiting Assets": The jurisdiction has enacted laws authorizing the tracing, freezing, seizure and forfeiture of assets identified as relating to or generated by money laundering activities.
8. "Arrangements for Asset Sharing": By law, regulation or bilateral agreement, the jurisdiction permits sharing of seized assets with third party jurisdictions which assisted in the conduct of the underlying investigation.
9. "Cooperates w/International Law Enforcement": By law or regulation, banks are permitted/required to cooperate with authorized investigations involving or initiated by third party jurisdictions, including sharing of records or other financial data.
10. "International Transportation of Currency": By law or regulation, the jurisdiction, in cooperation with banks, controls or monitors the flow of currency and monetary instruments crossing its borders. Of critical weight here are the presence or absence of wire transfer regulations and use of reports completed by each person transiting the jurisdiction and reports of monetary instrument transmitters.
11. "Mutual Legal Assistance": By law or through treaty, the jurisdiction has agreed to provide and receive mutual legal assistance, including the sharing of records and data.
12. "Non-Bank Financial Institutions": By law or regulation, the jurisdiction requires nonbank financial institutions to meet the same customer identification standards and adhere to the same reporting requirements that it imposes on banks.

13. "Disclosure Protection Safe Harbor": By law, the jurisdiction provides a "safe harbor" defense to banks or other financial institutions and their employees who provide otherwise confidential banking data to authorities in pursuit of authorized investigations.
14. "States Parties to 1988 UN Drug Convention": As of December 31, 2006, a party to the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, or a territorial entity to which the application of the Convention has been extended by a party to the Convention.[1]
15. "Criminalized the Financing of Terrorism." The jurisdiction has criminalized the provision of material support to terrorists and/or terrorist organizations.
16. "States Party to the UN International Convention for the Suppression of the Financing of Terrorism." As of December 31, 2006, a party to the International Convention for the Suppression of the Financing of Terrorism, or a territorial entity to which the application of the Convention has been extended by a party to the Convention.

[1] The United Kingdom extended its application of the 1988 Convention and the United Kingdom Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Gibraltar, Montserrat, Turks and Caicos, Isle of Man, Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

# Comparative Table

| Actions by Governments | Criminalized Drug Money Laundering | Criminalized Beyond Drugs | Record Large Transactions | Maintain Records Over Time | Report Suspicious Transactions (NMP) | Financial Intelligence Unit | System for Identifying/Forfeiting Asset s | Arrangements for Asset Sharing | Cooperates w/International Law Enf. | Int'l. Transportation of Currency | Mutual Legal Assistance | Non-Bank Financial Institutions | Disclosure Protection "Safe Harbor" | States Party to 1988 UN Convention | Criminalized Financing of Terrorism | Internat'l Terrorism Financing Convention |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Government/Jurisdiction** | | | | | | | | | | | | | | | | |
| Afghanistan | Y | Y | Y | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Albania | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Algeria | Y | Y | N | Y | M | N | Y | N | Y | Y | N | Y | Y | Y | Y | Y |
| Andorra | Y | Y | Y | Y | M | Y | Y | N | Y | N | Y | Y | Y | Y | N | N |
| Angola | Y | N | N | N | N | N | N | N | N | N | Y | N | N | Y | N | N |
| Anguilla[1] | Y | Y | Y | Y | M | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | N |
| Antigua & Barbuda | Y | Y | N | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Argentina | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | N | Y |
| Armenia | Y | Y | N | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Aruba | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N |
| Australia | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Austria | Y | Y | N | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Azerbaijan | Y | N | N | Y | N | N | N | N | N | Y | Y | N | Y | Y | Y | Y |
| Bahamas | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Bahrain | Y | Y | N | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Bangladesh | Y | Y | N | Y | M | N | N | N | N | Y | Y | N | N | Y | N | Y |
| Barbados | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Belarus | Y | Y | Y | Y | M | N | Y | N | Y | N | Y | Y | Y | Y | Y | Y |
| Belgium | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Belize | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Benin | Y | N | Y | N | M | N | Y | N | Y | Y | N | N | Y | Y | N | Y |

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

| Actions by Governments | Criminalized Drug Money Laundering | Criminalized Beyond Drugs | Record Large Transactions | Maintain Records Over Time | Report Suspicious Transactions (NMP) | Financial Intelligence Unit | System for Identifying/Forfeiting Assets | Arrangements for Asset Sharing | Cooperates w/International Law Enf. | Int'l. Transportation of Currency | Mutual Legal Assistance | Non-Bank Financial Institutions | Disclosure Protection "Safe Harbor" | States Party to 1988 UN Convention | Criminalized Financing of Terrorism | Internat'l Terrorism Financing Convention |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bermuda[1] | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N |
| Bolivia | Y | Y | N | Y | M | Y | Y | N | N | N | Y | N | Y | Y | N | Y |
| Bosnia & Herzegovina | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Botswana | Y | Y | Y | Y | M | N | Y | Y | Y | Y | Y | N | Y | Y | N | Y |
| Brazil | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y |
| British Virgin Islands[1] | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | N |
| Brunei Darussalam | Y | Y | N | Y | M | N | Y | N |  | N | Y | Y | N | Y | Y | Y |
| Bulgaria | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Burkina Faso | N | N | Y | N | N | N | N | N | N | N | N | N | N | Y | N | Y |
| Burma | Y | Y | Y | Y | M | N | Y | N | Y | N | Y | Y | Y | Y | N | Y |
| Burundi | N | N | N | Y | N | N | N | N | Y | N | N | N | N | Y | N | N |
| Cambodia | Y | N | Y | Y | M | N | N | N | Y | Y | N | N | N | Y | N | Y |
| Cameroon | Y | Y | Y | Y | M | N | Y | N | N | N | N | N | N | Y | N | N |
| Canada | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Cape Verde | Y | Y |  | Y | M | N | Y | N | Y |  | Y |  |  | Y | N | Y |
| Cayman Islands[1] | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N |
| Chad | Y | Y | Y | Y | M | N | Y | N | N | Y | N | N | N | Y | N | N |
| Chile | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y |  | Y | Y | Y |
| China (PRC) | Y | Y | Y | Y | M | N | Y | N | Y | Y | Y | Y | N | Y | Y | Y |
| Colombia | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | N | Y |
| Comoros | Y | Y | N | Y | M | N | Y | Y | Y | Y | Y | Y | Y | Y | N | Y |

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Congo (Dem. Republic) | Y | Y | Y | Y | M | N | Y | N | N | N | N | Y | Y | N | Y | N |
| Congo (Republic) | Y | Y | Y | Y | M | N | N | N | N | Y | Y | Y | Y | Y | N | N |
| **Actions by Governments** | **Criminalized Drug Money Laundering** | **Criminalized Beyond Drugs** | **Record Large Transactions** | **Maintain Records Over Time** | **Report Suspicious Transactions (NMP)** | **Financial Intelligence Unit** | **System for Identifying/Forfeiting Assets** | **Arrangements for Asset Sharing** | **Cooperates w/International Law Enf.** | **Int'l. Transportation of Currency** | **Mutual Legal Assistance** | **Non-Bank Financial Institutions** | **Disclosure Protection "Safe Harbor"** | **States Party to 1988 UN Convention** | **Criminalized Financing of Terrorism** | **Internat'l Terrorism Financing Convention** |
| Cook Islands | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Costa Rica | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y |
| Cote D'Ivoire | Y | Y | Y | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | N | Y |
| Croatia | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Cuba | Y | Y | N | N | P | N | Y | N | N | Y | N | N | N | Y | Y | Y |
| Cyprus | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Czech Republic | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Denmark | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Djibouti | Y | Y | Y | Y | M | N | Y | N | Y | N | Y | Y | Y | Y | Y | N |
| Dominica | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Dominican Republic | Y | Y | Y | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | N | N |
| East Timor | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |
| Ecuador | Y | Y | Y | Y | M | N | Y | Y | N | Y | Y | Y | N | Y | N | Y |
| Egypt | Y | Y | N | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y |
| El Salvador | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Equatorial Guinea | Y | Y | Y | Y | M | N | N | N | N | N | N | N | N | N | N | Y |
| Eritrea | Y | Y | Y | Y | N | N | N | N | Y | Y | N | N | N | Y | N | N |
| Estonia | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Ethiopia | Y | Y | Y | Y | M | N | Y | N | N | N | N | N | N | Y | N | N |
| Fiji | Y | Y | N | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | N | N |
| Finland | Y | Y | Y | Y | M | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y |
| France | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Gabon | N | N | Y | Y | M | N | N | N | N | N | N | N | N | N | N | N |
| Gambia | Y | Y | Y | Y | M | N | Y | N | N | N | N | Y | Y | Y | N | N |

| Actions by Governments | Criminalized Drug Money Laundering | Criminalized Beyond Drugs | Record Large Transactions | Maintain Records Over Time | Report Suspicious Transactions (NMP) | Financial Intelligence Unit | System for Identifying/Forfeiting Assets | Arrangements for Asset Sharing | Cooperates w/International Law Enf. | Int'l. Transportation of Currency | Mutual Legal Assistance | Non-Bank Financial Institutions | Disclosure Protection "Safe Harbor" | States Party to 1988 UN Convention | Criminalized Financing of Terrorism | Internat'l Terrorism Financing Convention |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Georgia | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | N | Y |
| Germany | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Ghana | Y | N | N | Y | N | N | Y | N | Y | Y | Y | Y | Y | Y | N | Y |
| Gibraltar[1] | Y | Y | Y | Y | M | Y | Y | Y | Y | N | Y | Y | Y | N | Y | N |
| Greece | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Grenada | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Guatemala | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Guernsey[1] | Y | Y | N | Y | M | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | N |
| Guinea | Y | N | Y | N | N | N | N | N | N | Y | N | N | N | Y | N | Y |
| Guinea-Bissau | Y | Y | N | Y | Y | N | N | N | N | Y | N | Y | Y | Y | N | N |
| Guyana | Y | Y | N | Y | M | N | Y | N | N | Y | Y | N | Y | Y | N | N |
| Haiti | Y | Y | Y | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | N | N |
| Honduras | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | N | Y |
| Hong Kong | Y | Y | N | Y | M | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y |
| Hungary | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Iceland | Y | Y | Y | Y | M | Y | Y | N | Y | N | Y | Y | Y | Y | Y | Y |
| India | Y | Y | Y | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Indonesia | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Iran | Y | Y | N | Y | M | Y | N | N | N | N | Y | N | N | Y | N | N |
| Iraq | Y | Y | N | Y | M | N | Y | N | N | Y | N | Y | Y | Y | Y | N |
| Ireland | Y | Y | Y | Y | M | Y | Y | N | Y | N | Y | Y | Y | Y | Y | Y |
| Isle of Man[1] | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N |
| Israel | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

| Actions by Governments | Criminalized Drug Money Laundering | Criminalized Beyond Drugs | Record Large Transactions | Maintain Records Over Time | Report Suspicious Transactions (NMP) | Financial Intelligence Unit | System for Identifying/Forfeiting Assets | Arrangements for Asset Sharing | Cooperates w/International Law Enf. | Int'l. Transportation of Currency | Mutual Legal Assistance | Non-Bank Financial Institutions | Disclosure Protection "Safe Harbor" | States Party to 1988 UN Convention | Criminalized Financing of Terrorism | Internat'l Terrorism Financing Convention |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Italy | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Jamaica | Y | Y | Y | Y | M | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Japan | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Jersey[1] | Y | Y | N | Y | M | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | N |
| Jordan | Y | Y | N | Y | M | N | N | Y | N | N | Y | Y | Y | Y | Y | Y |
| Kazakhstan | Y | N | N | Y | P | N | N | N | N | Y | Y | N | N | Y | N | Y |
| Kenya | Y | N | Y | Y | P | N | Y | N | Y | Y | Y | N | N | Y | N | Y |
| Korea (DPRK) | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |
| Korea (Republic of) | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | N | Y |
| Kosovo[2] | Y | Y | Y | Y | M | N | Y | N | Y | Y | Y | Y | Y | NA | N | NA |
| Kuwait | Y | Y | Y | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | N | N |
| Kyrgyzstan | N | N | N | N | P | N | Y | N | N | N | N | N | Y | Y | N | Y |
| Laos | Y | Y | N | N | N | N | N | N | N | Y | N | N | N | Y | N | N |
| Latvia | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Lebanon | Y | Y | Y | Y | M | Y | Y | N | Y | N | Y | Y | Y | Y | Y | N |
| Lesotho | N | N | Y | Y | M | N | N | N | Y | N | Y | N | Y | Y | N | Y |
| Liberia | Y | Y | Y | Y | M | N | N | N | N | Y | N | N | N | Y | N | Y |
| Libya | Y | Y | N | Y | M | N | N | N | Y | Y | N | Y | Y | Y | N | Y |
| Liechtenstein | Y | Y | Y | Y | M | Y | Y | Y | Y | N | Y | Y | Y | N | Y | Y |
| Lithuania | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Luxembourg | Y | Y | Y | Y | M | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y |
| Macau | Y | Y | N | Y | M | N | Y | N | Y | N | Y | Y | Y | Y | Y | Y |

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

[2] Kosovo is under the supervision of the UN and is not a sovereign state.

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Macedonia | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Madagascar | Y | Y | N | Y | N | N | Y | N | | N | Y | Y | Y | Y | N | Y |

| Actions by Governments | Criminalized Drug Money Laundering | Criminalized Beyond Drugs | Record Large Transactions | Maintain Records Over Time | Report Suspicious Transactions (NMP) | Financial Intelligence Unit | System for Identifying/Forfeiting Assets | Arrangements for Asset Sharing | Cooperates w/International Law Enf. | Int'l. Transportation of Currency | Mutual Legal Assistance | Non-Bank Financial Institutions | Disclosure Protection "Safe Harbor" | States Party to 1988 UN Convention | Criminalized Financing of Terrorism | Internat'l Terrorism Financing Convention |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Malawi | Y | Y | Y | Y | P | N | N | N | | N | N | N | N | Y | N | Y |
| Malaysia | Y | Y | N | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | N | N |
| Maldives | Y | N | N | N | M | N | Y | N | | N | | N | N | Y | Y | Y |
| Mali | Y | Y | N | Y | M | N | Y | N | Y | N | Y | Y | N | Y | N | Y |
| Malta | Y | Y | N | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Marshall Islands | Y | Y | Y | Y | M | Y | Y | Y | Y | N | Y | Y | Y | N | Y | Y |
| Mauritania | Y | Y | Y | Y | P | N | Y | N | Y | N | Y | N | Y | Y | N | Y |
| Mauritius | Y | Y | N | Y | M | Y | Y | N | Y | N | Y | Y | Y | Y | Y | Y |
| Mexico | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y |
| Micronesia | Y | Y | N | Y | N | N | Y | N | Y | N | Y | N | Y | Y | N | Y |
| Moldova | Y | Y | Y | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Monaco | Y | Y | N | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Mongolia | Y | Y | Y | Y | N | N | Y | N | N | Y | N | Y | Y | Y | N | Y |
| Montenegro | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | N |
| Montserrat[1] | Y | Y | N | Y | M | N | Y | Y | Y | N | Y | Y | Y | Y | Y | N |
| Morocco | N | N | N | Y | M | N | N | N | N | Y | Y | N | Y | Y | Y | Y |
| Mozambique | Y | Y | Y | Y | M | N | Y | Y | Y | Y | Y | Y | Y | Y | N | Y |
| Namibia | Y | Y | Y | Y | M | N | N | N | N | N | N | Y | N | Y | N | N |
| Nauru | Y | Y | N | Y | M | N | Y | Y | Y | N | Y | Y | Y | N | Y | N |
| Nepal | N | N | N | Y | N | N | Y | N | Y | N | N | N | N | Y | N | N |
| Netherlands | Y | Y | Y | Y | M | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y |

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

| Actions by Governments | Criminalized Drug Money Laundering | Criminalized Beyond Drugs | Record Large Transactions | Maintain Records Over Time | Report Suspicious Transactions (NMP) | Financial Intelligence Unit | System for Identifying/Forfeiting Assets | Arrangements for Asset Sharing | Cooperates w/International Law Enf. | Int'l. Transportation of Currency | Mutual Legal Assistance | Non-Bank Financial Institutions | Disclosure Protection "Safe Harbor" | States Party to 1988 UN Convention | Criminalized Financing of Terrorism | Internat'l Terrorism Financing Convention |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Netherlands Antilles | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | N |
| New Zealand | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Nicaragua | Y | N | Y | Y | M | N | Y | N | Y | Y | Y | N | N | Y | N | Y |
| Niger | Y | Y | Y | Y | M | N | Y | N | Y | N | N | Y | N | Y | N | Y |
| Nigeria | Y | Y | Y | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Niue[1] | Y | Y | Y | Y | M | N | Y | N | Y | N | Y | Y | Y | NA | N | NA |
| Norway | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Oman | Y | Y | Y | Y | M | N | Y | N | Y | N | Y | Y | Y | Y | N | N |
| Pakistan | Y | N | N | Y | M | N | Y | N | N | Y | Y | Y | N | Y | Y | N |
| Palau | Y | Y | Y | Y | M | N | Y | Y | Y | N | Y | Y | N | N | N | Y |
| Panama | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Papua New Guinea | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | Y |
| Paraguay | Y | Y | Y | Y | M | Y | N | N | Y | Y | Y | Y | Y | Y | N | Y |
| Peru | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Philippines | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | N | Y |
| Poland | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | N | Y |
| Portugal | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Qatar | Y | Y | Y | Y | M | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | N |
| Romania | Y | Y | Y | Y | M | Y | Y | N | Y | N | Y | Y | Y | Y | Y | Y |
| Russia | Y | Y | Y | Y | M | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y |
| Rwanda | N | N | N | N | M | N | N | N | Y | N | N | N | N | Y | N | Y |
| Samoa | Y | Y | Y | Y | M | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| San Marino | Y | Y | N | Y | M | Y | Y | N | Y | N | Y | Y | Y | Y | Y | Y |
| Sao Tome & Principe | N | N | N | N | N | N | N | N | N | N | N | N | N | Y | N | N |

[1] Niueans are citizens of New Zealand; Niue is not a member of the UN.

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Saudi Arabia | Y | Y | N | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | Y | N |
| Senegal | Y | Y | Y | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | N | Y |
| **Actions by Governments** | **Criminalized Drug Money Laundering** | **Criminalized Beyond Drugs** | **Record Large Transactions** | **Maintain Records Over Time** | **Report Suspicious Transactions (NMP)** | **Financial Intelligence Unit** | **System for Identifying/Forfeiting Assets** | **Arrangements for Asset Sharing** | **Cooperates w/International Law Enf.** | **Int'l. Transportation of Currency** | **Mutual Legal Assistance** | **Non-Bank Financial Institutions** | **Disclosure Protection "Safe Harbor"** | **States Party to 1988 UN Convention** | **Criminalized Financing of Terrorism** | **Internat'l Terrorism Financing Convention** |
| Serbia | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Seychelles | Y | Y | N | Y | M | N | Y | N | Y | N | Y | Y | Y | Y | Y | Y |
| Sierra Leone | Y | Y | N | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | N | Y |
| Singapore | Y | Y | Y | Y | M | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y |
| Slovakia | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Slovenia | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Solomon Islands | Y | Y | N | Y | N | N | N | N | N | N | N | N | N | N | N | N |
| South Africa | Y | Y | N | Y | M | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y |
| Spain | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Sri Lanka | N | N | N | N | N | N | N | N | N | N | Y | N | Y | Y | Y | Y |
| St Kitts & Nevis | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| St. Lucia | Y | Y | N | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | N | N |
| St. Vincent/Grenadines | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Suriname | Y | Y | N | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | N | N |
| Swaziland | Y | Y | Y | Y | M | N | Y | N | Y | N | Y | N | Y | Y | N | Y |
| Sweden | Y | Y | Y | Y | M | Y | Y | | Y | N | Y | Y | Y | Y | Y | Y |
| Switzerland | Y | Y | Y | Y | M | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y |
| Syria | Y | Y | Y | Y | M | N | Y | N | N | N | Y | Y | N | Y | N | Y |
| Taiwan[1] | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | NA | N | NA |
| Tajikistan | Y | Y | N | N | N | N | N | N | N | Y | Y | N | N | Y | Y | Y |
| Tanzania | Y | N | Y | Y | P | N | Y | N | Y | N | Y | N | Y | Y | Y | Y |
| Thailand | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |

[1] Taiwan is not a member of the UN.

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Togo | Y | N | Y | Y | N | N | Y | N | Y | N | Y | N | Y | Y | N | Y |
| Tonga | Y | Y | Y | Y | M | N | Y | N | Y | Y | N | N | N | Y | N | Y |

| Actions by Governments | Criminalized Drug Money Laundering | Criminalized Beyond Drugs | Record Large Transactions | Maintain Records Over Time | Report Suspicious Transactions (NMP) | Financial Intelligence Unit | System for Identifying/Forfeiting Assets | Arrangements for Asset Sharing | Cooperates w/International Law Enf. | Int'l. Transportation of Currency | Mutual Legal Assistance | Non-Bank Financial Institutions | Disclosure Protection "Safe Harbor" | States Party to 1988 UN Convention | Criminalized Financing of Terrorism | Internat'l Terrorism Financing Convention |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Trinidad & Tobago | Y | Y | Y | Y | M | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | N |
| Tunisia | Y | Y | Y | Y | M | N | Y | N | N | Y | N | N | Y | Y | Y | Y |
| Turkey | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Turkmenistan | Y | Y | N | Y | M | N | Y | N | Y | Y | Y | N | N | Y | Y | Y |
| Turks & Caicos[1] | Y | Y | Y | Y | M | N | Y | Y | Y | N | Y | Y | Y | Y | N | N |
| Uganda | Y | N | N | N | N | N | N | N | Y | N | N | N | Y | Y | Y | Y |
| Ukraine | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| United Arab Emirates | Y | Y | Y | Y | M | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| United Kingdom | Y | Y | Y | Y | M | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y |
| United States | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Uruguay | Y | Y | Y | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Uzbekistan | Y | Y | Y | Y | M | N | Y | N | Y | Y | Y | Y | Y | Y | Y | Y |
| Vanuatu | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | N |
| Venezuela | Y | Y | Y | Y | M | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y |
| Vietnam | Y | Y | Y | Y | M | N | Y | N | N | Y | Y | Y | N | Y | N | Y |
| Yemen | Y | Y | N | Y | M | N | N | N | Y | N | Y | Y | Y | Y | N | N |
| Zambia | Y | Y | N | Y | M | N | Y | N | Y | N | Y | N | | Y | N | N |
| Zimbabwe | Y | Y | N | Y | M | N | Y | N | N | Y | N | Y | N | Y | Y | N |

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

# Country Reports

## Afghanistan

Afghanistan is not a regional financial or banking center. However, its formal financial system is growing rapidly while its traditional informal financial system remains significant in reach and scale. Afghanistan is a major drug trafficking and drug producing country and the illicit narcotics trade is the primary source of laundered funds. Afghanistan passed anti-money laundering and terrorist financing legislation in late 2004, and efforts are being made to strengthen police and customs forces. However, there remain few resources and little expertise to combat financial crimes. The most fundamental obstacles continue to be legal, cultural and historical factors that conflict with more Western-style proposed reforms to the financial sector.

According to United Nations statistics, in 2005 and 2006, opium production increased and today Afghanistan accounts for over 90 percent of the world's opium production. Opium gum itself is sometimes used as a currency, especially by rural farmers, and it is used as a store of value in prime production areas. It is estimated that at least one third of Afghanistan's (licit plus illicit) GDP is derived directly from narcotics activities, and proceeds generated from the drug trade have reportedly fueled a growing real estate boom in Kabul, as well as a sharp increase in capital investment in rural poppy growing areas.

Much of the recent rise in opium production comes from Taliban strongholds in the southern part of the country. There are reports that the Taliban impose taxes on narcotics dealers, which undoubtedly helps finance their terrorist activities. Additional revenue streams for the Taliban and regional warlords come from "protecting" opium shipments, running heroin labs, and from "toll booths" established on transport and smuggling routes.

Afghan opium is refined into heroin by production labs, more of which are being established within Afghanistan's borders. The heroin is then often broken into small shipments and smuggled across porous borders for resale abroad. Payment for the narcotics outside the country is facilitated through a variety of means, including through conventional trade and the traditional hawala system that uses trade as the primary medium to balance accounts. In addition, the narcotics themselves are often used as tradable goods and as a means of exchange for automobiles, construction materials, foodstuffs, vegetable oils, electronics, and other goods between Afghanistan and neighboring Pakistan. Many of these goods are smuggled into Afghanistan from neighboring countries, particularly Iran and Pakistan, or enter via the Afghan Transit Trade without payment of customs duties or tariffs. Most of the trade goods imported into Afghanistan originate in Dubai. Invoice fraud, corruption, indigenous smuggling networks, underground finance, and legitimate commerce are all intertwined.

Afghanistan is widely served by the hawala system, which provides a range of financial and nonfinancial business services in local, regional, and international markets. Financial activities include foreign exchange transactions, funds transfers (particularly to and from neighboring countries with weak regulatory regimes for informal remittance systems), micro and trade finance, as well as some deposit-taking activities. While the hawala network may not provide financial intermediation of the same type as the formal banking system (i.e., deposit-taking for lending and investing purposes based on the assessment, underwriting, and pricing of risks), it is a traditional form of finance and deeply entrenched and widely used throughout Afghanistan and the neighboring region.

There are over 200 known hawala dealers in Kabul, with 100-300 additional dealers in each province. These dealers are loosely organized into informal provincial unions or guilds whose members maintain a number of agent-principal and partnership relationships with other dealers throughout the

country and internationally. Their record keeping and accounting practices are robust, efficient, and take note of currencies traded, international pricing, deposit balances, debits and credits with other dealers, lending, cash on hand, etc. Hawaladars are supposed to be licensed; however the licensing regime that existed from April 2004 until September of 2006 was overly burdensome and resulted in issuance of few licenses. In September of 2006, Da Afghanistan Bank (DAB)—Afghanistan's Central Bank—issued a new money service provider regulation that streamlined the licensing process and substantially reduced the licensing and ongoing compliance burden for hawaladars. The regulatory focus of the new regulation is on AML and CTF. The regulation requires and provides standard mechanisms for record keeping and reporting of large transactions. DAB has provided training sessions on the new regulation and has developed a streamlined application process. Several licenses have already been issued under the new regulation, with the majority of Kabul area hawaladars expected to obtain licenses in the near-term as a result of DAB outreach, law enforcement actions, pressure from commercial banks where they hold accounts, and customer demand for licensed providers. Options for strengthening the hawaladar unions and promoting self regulation are also being studied.

In early 2004, DAB worked in collaboration with international donors to establish the legislative framework for anti-money laundering and the suppression of the financing of terrorism. Although Afghanistan was unable to meet its initial commitment to enact both pieces of legislation by September 30, 2004, they were both finalized and signed into law by late October 2004.

The Anti-Money Laundering (AML) and Proceeds of Crime and Combating the Financing of Terrorism (CTF) laws incorporate provisions that are designed to meet the recommendations of the Financial Action Task Force (FATF) and address the criminalization of money laundering and the financing of terrorism, customer due diligence, the establishment of a Financial Intelligence Unit (FIU), international cooperation, extradition, and the freezing and confiscation of funds. The AML law also includes provisions to address cross-border currency reporting, and establishes authorities to seize and confiscate monies found to be undeclared or falsely declared, or determined to be transferred for illicit purposes. However, the capability to enforce these provisions is nearly non-existent, and furthermore, these provisions are largely unknown in many parts of the country.

Under the new AML law, an FIU has been established and is functioning as a semi-autonomous unit within DAB. Banks and other financial and nonfinancial institutions are required to report suspicious transactions and all cash transactions as prescribed by DAB to the FIU, which has the legal authority to freeze assets for up to 7 days. Currently, in excess of four thousand electronically formatted cash transaction reports are being received and processed each month. The FIU, originally set to be established in January 2005, was actually initiated in October 2005 with assignment of a General Director, office space, and other resources. At present the formal banking sector consists of three recently re-licensed state-owned banks, five branches of foreign banks, and six additional domestic banks. AML examinations have been conducted in half of these banks. The result is a growing awareness of AML requirements and deficiencies among the banks and a building of AML capacity. Additionally, the Central Bank has worked with the banking community to develop several ongoing topical working groups focused on AML issues (e.g. "know your customer" provisions and reporting of suspicious transactions).

The Supervision Department within the DAB was formed at the end of 2003, and is divided into four divisions: Licensing, General Supervision (which includes on-site and off-site supervision), Special Supervision (which deals with special cases of problem banks), and Regulation. The Department is charged with administering the AML and CTF legislation, conducting examinations, licensing new institutions, overseeing money service providers, and liaising with the commercial banking sector generally. The effectiveness of the Supervision Department in the AML area remains limited due to staffing, organization, and management issues.

The Ministry of Interior and the Attorney General's Office are the primary financial enforcement authorities. However, neither is able to conduct financial investigations, and both lack the training necessary to follow potential leads generated by an FIU, whether within Afghanistan or from international sources. Pursuant to the Central Bank law, a Financial Services Tribunal will be established to review certain decisions and orders of DAB. There is a need for significant training for judges and administrative staff before the Tribunal will be effective. The Tribunal will review supervisory actions of DAB, but will not prosecute cases of financial crime. At present, all financial crime cases are being forwarded to the Kabul Provincial Court, where there has been little or no activity in the last three years. The process to prosecute and adjudicate cases is long and cumbersome, and significantly underdeveloped.

Border security continues to be a major issue throughout Afghanistan. At present there are 21 border crossings that have come under central government control, utilizing international donor assistance as well as local and international forces. However, many of the border areas continue to be un-policed and therefore susceptible to illicit cross-border trafficking and trade-based money laundering. Many regional warlords also continue to control the international borders in their provincial areas, causing major security risks. Customs authorities, with the help of outside assistance, have made significant strides, but much work remains to be done. Customs collection has improved, but smuggling and corruption continue to be major concerns, as well as trade fraud, which includes false and over-and-under invoicing. Thorough cargo inspections are not conducted at any gateway. A pilot program for declaring large, cross-border currency transactions has been developed for the Kabul International Airport, but has not yet been implemented. If successful, this prototype will serve as the foundation for expansion to other crossings.

Under the Law on Combating the Financing of Terrorism, any nonprofit organization that wishes to collect, receive, grant, or transfer funds and property must be entered in the registry with the Ministry of Auqaf (Islamic Affairs). All nonprofit organizations are subject to a due diligence process which includes an assessment of accounting, record keeping, and other activities. However, the capacity of the Ministry to conduct such examinations is nearly non-existent, and the reality is that any organization applying for a registration is granted one. Furthermore, because no adequate enforcement authority exists, many organizations operating under a "tax-exempt" nonprofit status in Afghanistan go completely unregistered, and illicit activities are suspected on the part of a number of organizations.

The Government of Afghanistan (GOA) has now become a party to 12 of the UN conventions and protocols against terrorism and is a signatory to the International Convention for the Suppression of Acts of Nuclear Terrorism. Afghanistan is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. In July 2006, Afghanistan became a member in the Asia Pacific Group, a Financial Action Task Force Style Regional Body (FSRB), and has obtained observer status in the Eurasian Group, another FSRB. Additionally the FIU has initiated the process for joining the Egmont Group of Financial Intelligence Units.

The Government of Afghanistan has made progress over the past year in developing its overall AML/CTF regime. Improvement has been seen in development of the FIU, the reporting of financial intelligence, participation in international AML bodies, improvement in bank AML compliance awareness, systems, and reporting, and in efforts to bring money service providers into a legal and regulatory framework that will result in meaningful AML compliance. However, much work remains to be done. Afghanistan should develop secure, reliable, and capable relationships among departments and agencies involved in law enforcement. Afghanistan should develop the investigative capabilities of law enforcement authorities in the areas of financial crimes, particularly money laundering and terrorist finance. Judicial authorities should also be trained in money laundering prosecutions. Afghan customs authorities should implement cross-border currency reporting and be trained to recognize

forms of trade-based money laundering. Border enforcement should be a priority, both to enhance scarce revenue and to disrupt narcotics trafficking and illicit value transfer. Afghan authorities should work to address widespread corruption in commerce and government. Afghanistan should ratify the UN Convention against Corruption.

## Albania

As a transit country for trafficking in narcotics, arms, contraband, and humans, Albania remains at significant risk for money laundering. Major sources of criminal proceeds are drug-related crimes, robberies, customs offenses, prostitution, trafficking in weapons and automobiles, official corruption, tax crimes and fraud. Organized crime groups use Albania as a base of operations for conducting criminal activities in other countries, often sending the illicit funds back to Albania. The proceeds from these activities are easily laundered in Albania because of the lack of a strong formal economy and weak government controls. Money laundering is believed to be occurring through the investment of tainted money in real estate and business development projects. Customs controls on large cash transfers are not believed to be effective, due to a lack of resources and corruption of customs officials.

Albania's economy remains primarily cash-based. Electronic and ATM transactions are relatively few in number, but are growing rapidly as more banks introduce this technology. The number of ATMs rapidly expanded following the decision of the Government of Albania (GOA) to deliver salaries through electronic transfers. By the end of 2005, all central government institutions had converted to electronic pay systems. Credit card usage has also increased in Albania. However, thus far a small number of people possess them and usage is primarily limited to a few large vendors.

There are 17 banks in Albania, but only five of them are considered to have a significant national presence. According to the Bank of Albania (the Central Bank), 25 percent of the money in circulation is outside of the banking system, compared to an average of 10 percent in other Central and Eastern European transitioning economies. Albania is not considered an offshore financial center, nor do its current laws facilitate such types of activity. Although current law permits the operation of free trade zones, the GOA has not pursued the implementation of them and none are currently in operation.

The Albanian economy is particularly vulnerable to money laundering activity because it is a cash-based economy. The GOA estimates that proceeds from the informal sector account for approximately 30-60 percent of Albania's GDP. Albania collects 10 to 15 percent less of GDP in taxes than neighboring countries. Relatively high levels of foreign trade activity, coupled with weak customs controls, presents a gateway for money laundering in the form of fake imports and exports. The Bankers Association estimates that only 20-30 percent of transactions with trading partners take place through formal banking channels, encompassing only a small portion of total imports. Likewise, a significant portion of remittances enters the country through unofficial channels. It is estimated that only half of total remittances enter Albania through banks or money transfer companies. Black market exchange is still present in the country, especially in Tirana, despite repeated efforts by GOA institutions (Ministry of Interior, Bank of Albania, and Ministry of Finance) to impede such exchanges. There have been court decisions against illegal money remitters based on information received from foreign financial intelligence units (FIUs).

Albania criminalized money laundering in Article 287 of the Albanian Criminal Code of 1995, consolidated version as of December 1, 2004. However, the law was largely ineffectual as it required proof of a predicate offense.

Albania's original money laundering law was On the Prevention of Money Laundering, or Law No. 8610 of 17 May 2000. In June 2003, Parliament approved Law No. 9084, which strengthened the old Law No. 8610, and improved the Criminal Code and the Criminal Procedure Code. The new law

redefined the legal concept of money laundering, harmonizing the Albanian definition with that of the European Union (EU) and international conventions. Under the revised Criminal Code many powers were expanded and improved upon. The new law also revised the definition of money laundering, outlawed the establishment of anonymous accounts, and permitted the confiscation of accounts. Albania's money laundering law places reporting requirements on both financial institutions and individuals. Financial institutions are required to report to an anti-money laundering agency all transactions that exceed approximately $200,000 as well as those that involve suspicious activity. Private individuals (both Albanian and foreign) are required to report to customs authorities all cross-border transactions that exceed approximately $10,000. Declaration forms are available at border crossing points. The law also mandates the identification of beneficial owners. Banks and other institutions are required to maintain records of suspicious transaction reports (STRs) for ten years. All other reports are subject to a five-year record retention period. There have been cases of individuals sentenced for illegal transfer of money based on information from foreign FIUs, and the Albanian FIU occasionally shares cash smuggling reports with its counterparts in Turkey, Bulgaria, and Macedonia.

Financial institutions are required to report transactions within 48 hours if the origin of the money cannot be determined. In addition, there are requirements to report all financial transactions that exceed certain thresholds. However, financial institutions have no legal obligation to identify customers prior to opening an account. While most banks have internal rules mandating customer identification, Albania's money laundering law only requires customer identification prior to conducting transactions that exceed approximately $20,000 or when there is a suspicion of money laundering.

Albania's laws set forth an "all crimes" definition for the offense of money laundering. However, an issue of concern is the fact that the Albanian court system applies a difficult burden of proof in that it requires a prior or simultaneous conviction for the predicate crime before an indictment for money laundering can be issued. According to the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) mutual evaluation report (MER), whose team conducted the evaluation in September 2005, and which accepted the MER in July 2006, Albanian authorities estimated that Albania had two cases of money laundering and five convictions, with another five cases at the prosecutor's office. There is no information available regarding cases, prosecutions or convictions of money laundering offenses for 2006.Albanian law also has no specific laws pertaining to corporate criminal liability, however it may be possible (though unlikely) for legal entities to be prosecuted for money laundering under Article 45 of the Criminal Code.

In the case of intermediaries, it is the responsibility of the appropriate licensing authority to supervise such entities for compliance (e.g., Ministry of Justice for notaries, Ministry of Finance for accountants). Although regulations also cover nonbank financial institutions, enforcement has been poor in practice. There is an increasing number of STRs coming from banks as the banking sector becomes more mature, although the majority continues to come from tax and customs authorities and foreign counterparts. Currently, no law criminalizes negligence by financial institutions in money laundering cases. However, the Bank of Albania has established a task force to confirm banks' compliance with customer verification rules. Reporting individuals and entities are protected by law with respect to their cooperation with law enforcement agencies. However, given leaks of information from other agencies, reporting entities complain that reporting requirements compromise their client confidentiality.

Albania's money laundering law also mandates the establishment of an agency to coordinate the GOA's efforts to detect and prevent money laundering. Albania's FIU, the General Directorate for the Prevention of Money Laundering (DPPP), falls under the control of the Ministry of Finance and evaluates reports filed by financial institutions. If the agency suspects that a transaction involves the proceeds of criminal activity, it must forward the information to the prosecutor's office. In 2006, there

were a total of 15 suspicious activity reports that the FIU acted upon, out of a total of 46,630 reports received.

Law No. 9084 clarifies and improves the role of the FIU and increases its responsibility. It has been given additional status by its designation as the national center to combat money laundering. Also, the duties and responsibilities for the FIU have been clarified. The law also establishes a legal basis for increased cooperation between the FIU and the General Prosecutor's Office, while creating an oversight mechanism to ensure that the FIU fulfills, but does not exceed, its responsibilities and authority. Previously, coordination against money laundering and terrorist financing among agencies was sporadic. The new law establishes coordination on the both the policy and the technical level. On the policy level, an inter-ministerial group was established. The group is headed by Albania's Prime Minister and includes the participation of the Central Bank Governor and the General Prosecutor. On the technical level, a group of experts was established. The Albanian government is reportedly in the process of preparing a new draft law on money laundering.

In addition to the FIU, the government bodies responsible for investigating financial crimes are the Ministry of Interior (through its Organized Crime and Witness Protection Departments), the General Prosecutor's Office, and the State Intelligence Service. Money laundering and terrorist financing are relatively new issues for GOA institutions, and responsible agencies are neither adequately staffed nor fully trained to handle money laundering and terrorist financing issues.

Albanian law also allows freezing or blocking of financial transactions believed to involve money laundering. In 2004, Albania passed a comprehensive anti-Mafia law, Law No. 9284, which contains strong civil asset seizure and forfeiture provisions, subjecting the assets of suspected persons, their families, and close associates to seizure. The law also places the burden to prove a legitimate source of funding for seized assets on the defendant.

Until 2004, the GOA used its anti-money laundering law to freeze the assets of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions committee's consolidated list. In 2004, Law No. 9258, "On Measures Against Terrorist Financing," was enacted, criminalizing the financing of terrorism and mandating strong penalties for any actions or organizations linked with terrorism. The law permits the GOA to administratively sequester or freeze assets of any terrorist designated pursuant to Security Council resolutions, as well as pursuant to certain bilateral or multilateral requests. The Ministry of Finance has already implemented this law. In addition to the one freeze action conducted in 2004, the GOA has frozen the assets of seven additional individuals or entities in 2005, and supports USG and UN designation efforts.

The Ministry of Finance is the main entity responsible for issuing freeze orders. The order is executed by the Minister of Finance and then delivered by the FIU to other government agencies that take action to freeze any assets found belonging to the named individual or entity. In the case of individuals or entities whose names appear on the UNSCR 1267 consolidated list, the sequestration orders remain in force as long as their names remain on the list. In the case of individuals under investigation or prosecution for money laundering, their assets may remain frozen until a court decision to the contrary is issued (such investigative freezes may not exceed three years). If a person is found guilty, his assets are ordered confiscated and any proceeds are transferred to the state budget. The Agency for the Administration of Sequestered and Confiscated Assets (AASCA) was established in June 2005, following a Council of Ministers decision. The purpose of the agency is to safeguard sequestered assets and to dispose of assets ordered confiscated. After a difficult start, the GOA first staffed the AASCA in early December 2005. However, the agency receives little support from the Ministry of Finance and has also experienced a large turnover in staffing.

Between 2001 and 2005, the GOA seized $4.72 million in liquid criminal and terrorist assets ($3.14 million for terrorism financing and $1.58 million for money laundering) and about $5 million in real estate ($2.3 million in 2005). In 2005, the previous freezing orders were converted under the new law

against terrorism financiers. As of 2005, there have been eight freeze orders issued, involving 56 bank accounts frozen in six different commercial banks. Fifty-four of these are related to terrorist financing. Each of the eight freeze orders issued by the Ministry of Finance in relation to persons involved in terrorism financing has been referred to the Prosecutor's Office for further investigation.

Although the GOA has not passed specific legislation addressing alternative remittance systems or charitable organizations, officials state that such informal transactions are covered under recent laws. Additionally, although the GOA does not normally monitor the use of funds by charitable organizations, the Ministry of Finance has explored additional legislation that would include such oversight. As of 2006, charitable organizations are required to present their books to the tax office. The GOA has aggressively acted against charities that are suspected of wrongdoing, resulting in the removal of three of them from the country.

Albania is a member of MONEYVAL and participates in the Southeastern Europe Cooperative Initiative (SECI). The Albanian FIU is a member of the Egmont Group, and continues to enlarge its cooperation with regional counterparts. The FIU has the ability to enter into bilateral or multilateral information sharing agreements on its own authority and has signed MOUs with 29 countries. Most recently, in February 2006, the Albanian FIU signed an MOU with its Kosovo counterpart that will allow the two FIUs to share information relating to money laundering. The FIU also participates in regional anti-money laundering seminars and conferences.

Albania is a party to the UN International Convention for the Suppression of the Financing of Terrorism; the UN Convention against Transnational Organized Crime; and the 1988 UN Drug Convention. In May 2006, Albania ratified the UN Convention against Corruption.

The Government of Albania has enhanced its anti-money laundering/counterterrorist financing regime; however, additional improvements are greatly needed. Albania should amend Article 287 of the Criminal Code to allow authorities to prosecute money laundering without first obtaining a conviction for a predicate offense. The FIU should create or obtain a database to allow analysis of the large volume of currency transaction reports (CTRs) and suspicious transaction reports received so that these reports currently received in hard copy can be analyzed. Training for the FIU should also be a high priority, as its staff is largely new and inexperienced. Training and modernization for the other facets of financial crime investigation should also be in order. The Albanian police force still has no central database and its investigators lack training in modern financial investigation techniques. The Prosecutor's Office also lacks well-trained prosecutors to effectively manage and try cases. Albania should also incorporate into its anti-money laundering legislation specific provisions regarding corporate criminal liability, customer identification procedures, and the adequate oversight of money remitters and charities.

## Algeria

Algeria is not a regional financial center or an offshore financial center. The extent of money laundering through formal financial institutions is thought to be minimal due to stringent exchange control regulations and an antiquated banking sector. The partial convertibility of the Algerian dinar enables the Bank of Algeria (Algeria's Central Bank) to monitor all international financial operations carried out by public and private banking institutions.

Algeria first criminalized terrorist financing through the adoption of Ordinance 95.11 on February 24, 1994, making the financing of terrorism punishable by five to ten years of imprisonment. On February 5, 2005, Algeria enacted public law 05.01, entitled "The Prevention and Fight against Money Laundering and Financing of Terrorism." The law aims to strengthen the powers of the Cellule du Traitement du Renseignement Financier (CTRF), an independent financial intelligence unit (FIU) within the Ministry of Finance (MOF) created in 2002. This law seeks to bring Algerian law into

conformity with international standards and conventions. It offers guidance for the prevention and detection of money laundering and terrorist financing, institutional and judicial cooperation, and penal provisions.

Algerian financial institutions, as well as Algerian customs and tax administration agents, are required to report any activities they suspect of being linked to criminal activity, money laundering, or terrorist financing to CTRF and comply with subsequent CTRF inquiries. They are obligated to verify the identity of their customers or their registered agents before opening an account; they must furthermore record the origin and destination of funds they deem suspicious. In addition, these institutions must maintain confidential reports of suspicious transactions and customer records for at least five years after the date of the last transaction or the closing of an account.

The new legislation extends money laundering controls to specific, nonbank financial professions such as lawyers, accountants, stockbrokers, insurance agents, pension managers, and dealers of precious metals and antiquities. Provided information is shared with CTRF in good faith, the law offers immunity from administrative or civil penalties for individuals who cooperate with money laundering and terrorist finance investigations. Under the law, assets may be frozen for up to 72 hours on the basis of suspicious activity; such freezes can only be extended with judicial authorization. Financial penalties for noncompliance range from 50,000 to 5 million Algerian dinars (approximately U.S. $700 to U.S. $70,000). In addition to its provisions pertaining to money laundered from illicit activities, the law allows the investigation of terrorist-associated funds derived from “clean” sources.

The law also provides significant authority to the Algerian Banking Commission, the independent body established under authority of the Bank of Algeria to supervise banks and financial institutions, to inform CTRF of suspicious or complex transactions. The law furthermore gives the Algerian Banking Commission, CTRF, and the Algerian judiciary wide latitude to exchange information with their foreign government counterparts in the course of money laundering and terrorist finance investigations, provided confidentiality for suspected entities is insured. A clause excludes the sharing of information with foreign governments in the event legal proceedings are already underway in Algeria against the suspected entity, or if the information is deemed too sensitive for national security reasons.

On November 14, 2005, the Government of Algeria issued Executive Decree 05-442, establishing a deadline of September 1, 2006 after which all payments in excess of $70,000 must be made by check, wire transfer, payment card, bill of exchange, promissory note, or other official bank payment. While nonresidents are exempt from this requirement, they must (like all travelers to and from the country) report foreign currency in their possession to the Algerian Customs Authority. The government suspended the deadline in September 2006, however, in response to the slow implementation of a nation-wide electronic check-clearing system that failed to gain the confidence of the Algerian business community.

The Ministry of Interior is charged with registering foreign and domestic nongovernmental organizations in Algeria. While the Ministry of Religious Affairs legally controls the collection of funds at mosques for charitable purposes, some of these funds probably escape the notice of government monitoring efforts.

There are reports that Algerian customs and law enforcement authorities are increasingly concerned with cases of customs fraud and trade-based money laundering. Algerian authorities are taking steps to coordinate information sharing between concerned agencies.

In November 2004, Algeria became a member of the Middle East and North Africa Financial Action Task Force (MENA FATF). Algeria is a party to the UN Convention against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, and the 1988 UN Drug Convention. In addition, Algeria is a signatory to various UN, Arab, and African conventions against

terrorism, trafficking in persons, and organized crime. The Ministry of Justice is expected to create a pool of judges trained in financial matters.

Over the last three years, Algeria has taken significant steps to enhance its statutory regime against anti-money laundering and terrorist financing. It needs to move forward now to implement those laws and eliminate bureaucratic barriers among various government agencies by empowering CTRF, which in 2006 investigated only 15 suspicious transactions, to be the focal point for the AML/CTF investigations. In addition, given the scope of Algeria's informal economy, it should renew its initiative to limit the size of cash transactions. Algerian law enforcement and customs authorities should be trained in recognizing and investigating trade-based money laundering, value transfer, and bulk cash smuggling used for financing terrorism and other illicit financial activities.

## Angola

Angola is not a regional or offshore financial center and has not prosecuted any known cases of money laundering. The laundering of funds derived from continuous and widespread high-level corruption is a concern, as is the use of diamonds as a vehicle for money laundering. The Government of the Republic of Angola (GRA) has taken steps to guard against money laundering in the diamond industry by participating in the Kimberley Process, an international certification scheme designed to halt trade in "conflict" diamonds in countries such as Angola. Angola has implemented a control system in accordance with the Kimberley Process. However, through the method of "mixing parcels" of licit and illicit diamonds, the Kimberly certification process can be compromised. Corruption and Angola's long and porous borders further facilitate smuggling and the laundering of diamonds.

Angola currently has no comprehensive laws, regulations, or other procedures to detect money laundering and financial crimes, although some related crimes are addressed through other provisions of the criminal code. Additional laws remain in draft form only. Legislation governing foreign exchange controls allows the Central Bank's Supervision Division, the governmental entity charged with money laundering issues, to exercise some authority against illicit banking activities. The Central Bank of Angola has the authority to freeze assets, but Angola does not presently have an effective system for identifying, tracing, or seizing assets. Instead, such crimes are addressed through other provisions of the criminal code. For example, Angola's counter narcotics laws criminalize money laundering related to narcotics trafficking. One of three draft laws designed to reform the banking sector specifically targets money laundering. The money laundering bill, which is currently under consideration in the Angolan Congress, was drafted with the assistance of the World Bank.

The high cash flow in Angola makes its financial system an attractive site for money laundering. Because of a lack of a domestic interbank dollar clearing system, even dollar transfers between domestic Angolan banks are logged as "international" transfers, thus creating an incentive to settle transfers in cash. The local banking system imports approximately $200-300 million in currency per month, largely in dollars, without a corresponding cash outflow. Local bank representatives have reported that clients have walked into banks with up to $2 million in a briefcase to make a deposit. There are no currency transaction reports that cover these large cash transactions. Massive cash flows occur in a banking system ill-equipped to detect and report suspicious activity. The Central Bank has no workable data management system and only rudimentary analytic capability. It cannot develop suspicious transaction reports (STRs), much less analyze them or search for patterns.

Corruption is a pervasive problem in Angolan society and is found in commerce and at the highest levels of government. Angola is rated 142 out of 163 countries in Transparency International's 2006 International Corruption Perception Index.

Angola is party to the 1988 UN Drug Convention and the UN Convention against Corruption. Angola has signed but not yet ratified the UN Convention against Transnational Organized Crime. Angola has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Angola should pass its pending legislation and criminalize money laundering beyond drug offenses and terrorist financing. As part of legislation that adheres to world standards, the GRA should establish a system of financial transparency reporting requirements and a corresponding Financial Intelligence Unit. The GRA should then move quickly to implement the legislation and bolster the capacity of law enforcement to investigate financial crimes. Angola's judiciary should prioritize the prosecution of financial crimes, including corruption. The GRA should become a party to both the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism. The GRA should increase efforts to combat official corruption, including an effective system to identify, trace, seize, and forfeit assets.

## Antigua and Barbuda

As with other countries in the region, illicit proceeds from the transshipment of narcotics are laundered in Antigua and Barbuda. However, its offshore financial sector as well as its internet gaming industry remain primary vulnerabilities in Antigua and Barbuda. In 2006, Antigua and Barbuda reported 16 offshore banks, two offshore trusts, two offshore insurance companies, 6,303 international business corporations (IBCs), and 30 internet gaming companies. Antigua and Barbuda has five domestic casinos that also are vulnerable to money laundering.

The International Business Corporations Act 1982 (IBCA), as amended, is the governing legal framework for offshore businesses in Antigua and Barbuda. The IBCA requires offshore banks to maintain full details of all transactions in relation to deposits and withdrawals, and to retain the information obtained for a period of six years. No offshore bank may serve as the originator or recipient in the transfer of funds on behalf of an entity who is not an account holder. Bearer shares are permitted through a registered agent. However, the registered agent must maintain a register that includes such information as the names of the beneficial owners and the number of shares issued. Failure to do so could result in a fine of $50,000. Any entity licensed under the IBCA must maintain a physical presence with at least one full-time employee, and maintain all files and records for the company. Internet gaming companies must incorporate as an IBC, while land-based casinos must incorporate as a domestic company. As such, internet gaming companies must also meet the physical presence requirement, and are considered to have physical presence when the primary server is located in Antigua and Barbuda. Deemed a financial institution under the IBCA, internet gaming companies are also required to enforce know-your-customer verification procedures and maintain records relating to all gaming and financial transactions of each customer for six years. In addition, internet gaming companies must submit quarterly financial statements in addition to annual statements.

The Eastern Caribbean Central Bank (ECCB) supervises Antigua and Barbuda's domestic banking sector. In 2002, the IBCA was amended to create the Financial Services Regulatory Commission (FSRC) as the regulatory and supervisory authority that oversees offshore financial sectors, including internet gaming companies. The FSRC is an autonomous body supervised by a four-member Board comprised of public officials, and is presently chaired by the Solicitor General. The FSRC is also responsible for issuing IBC licenses and maintaining the register for all corporations. The FSRC is funded through the revenue generated by registration and licensing fees. Amendments to the IBCA in 2005 provide the FSRC with the ability to decline or revoke a license if it has reason to suspect that the corporation may be used for criminal purposes. To ensure compliance with legislation and regulations, the FSRC conducts annual on-site examinations and off-site examinations of offshore financial institutions as well as certain domestic nonbanking financial institutions, such as insurance companies, trusts, and money remitters.

The Government of Antigua and Barbuda (GOAB) reportedly receives approximately $2.8 million per year from license fees and other charges related to the internet gaming industry. A nominal free trade zone in the country also seeks to attract investment in priority areas of the GOAB. Casinos and sports book-wagering operations in Antigua and Barbuda's Free Trade Zone are supervised by the Office of National Drug Control Policy (ONDCP) and the Directorate of Offshore Gaming (DOG), a department within the FSRC. In 2001, the DOG issued Interactive Gaming and Interactive Wagering Regulations in order to establish regulations for the licensing of the industry and address possible money laundering through client accounts of internet gambling operations.

The Money Laundering Prevention Act (MLPA) 1996, as amended, is the cornerstone of Antigua and Barbuda's anti-money laundering legislation. The MLPA makes it an offense for any person to obtain, conceal, retain, manage, or invest illicit proceeds or bring such proceeds into Antigua and Barbuda if that person knows or has reason to suspect that they are derived directly or indirectly from unlawful activity. The MLPA covers institutions defined under the Banking Act, IBCA, and the Financial Institutions (Non-Banking) Act, which include offshore banks, IBCs, money service businesses, credit unions, building societies, trust businesses, casinos, internet gaming companies, and sports betting companies. Intermediaries such as lawyers and accountants are not included in the MLPA. The MLPA requires reporting entities to report suspicious activity suspected to be related to money laundering, whether a transaction was completed or not. There is no reporting threshold imposed on banks and financial institutions except for internet gaming companies, which are required to report to all payouts over $25,000. The MLPA also requires banks to monitor transactions involving individuals, businesses, and other financial institutions from countries that have not adopted a comprehensive anti-money laundering regime.

The Office of National Drug Control and Money Laundering Policy (ONDCP) Act 2003 establishes the ONDCP as the financial intelligence unit (FIU) of Antigua and Barbuda. An independent organization, the ONDCP is under the Ministry of National Security and is primarily responsible for the enforcement of the MLPA and for directing the GOAB's anti-money laundering efforts in coordination with the FSRC. The ONDCP assumes the role and fulfills the responsibilities of the Supervisory Authority as described in the MLPA, which includes the supervision of all financial institutions in respect to filing suspicious activity reports (SARs). As of October 2006, the ONDCP received 52 SARs of which 20 were investigated. In addition to receiving SARs, auditors of financial institutions review their compliance program and submit reports to the ONDCP for analysis and recommendations. The director of the ONDCP has the ability to appoint law enforcement officers to investigate narcotics trafficking, fraud, money laundering, and terrorist financing offenses. In 2005, two arrests were made on money laundering charges, but no arrests, prosecutions or convictions were reported in 2006.

In 2002, the ONDCP published guidelines which detail reporting entities' responsibilities including internal controls, customer identification, record keeping, reporting SARs, and anti-money laundering training for staff. The ONDCP has developed an anti-money laundering awareness training program and has trained a number of financial institutions, GOAB officials, and law enforcement officials with respect to their duties and responsibilities under the law.

The ONDCP has the ability to direct a financial institution to freeze property up to seven days, while it makes an application for a freeze order. A freeze order is made based upon a defendant being charged or about to be charged with a money laundering offense, or if the defendant is suspected of engaging in money laundering activity. Under the MLPA, a freeze order will lapse after 30 days unless charges are brought against the defendant, or an application for a civil forfeiture order has been filed. The Misuse of Drugs Act empowers the court to forfeit assets related to drug offenses. Forfeited assets are placed into the Forfeiture Fund and can be used by the ONDCP. The GOAB is currently working on asset forfeiture agreements with other jurisdictions. An MOU was recently signed with Canada.

Regardless of its own civil forfeiture laws, currently the GOAB can only provide forfeiture assistance in criminal forfeiture cases.

In the past few years, the GOAB has frozen approximately $6 million in Antigua and Barbuda financial institutions as a result of U.S. requests and has repatriated approximately $4 million. On its own initiative, the GOAB froze over $90 million believed to be connected to money laundering cases still pending in the United States and other countries. In 2005, the GOAB cooperated extensively with U.S. law enforcement in an investigation that resulted in a seizure of $1.022 million.

The ONDCP, with Cabinet approval, may enter into written agreements with other government agencies and foreign counterparts. Currently, the ONDCP has memoranda of understanding (MOUs) with the Royal Antigua and Barbuda Police Force, Customs, Immigration, and the Antigua and Barbuda Defense Force. The ONDCP also has an MOU with the FSRC, and expects to sign an MOU with the ECCB in 2007.

All travelers are required to fill out a Customs declaration form indicating if they are carrying in excess of $10,000 in cash or currency. The GOAB Customs Department maintains statistics on cross-border cash reports and seizures for failure to report. This information is shared with the ONDCP and the Police.

The GOAB enacted the Prevention of Terrorism Act 2001, amended in 2005, to implement the Counter Terrorism Conventions of the United Nations. The Act empowers the ONDCP to nominate any entity as a "terrorist entity" and to seize and forfeit terrorist funds. The law covers any finances in any way related to terrorism. The Act also provides the authority for the seizure of property used in the commission of a terrorist act; seizure and restraint of property that has been, is being or may be used to commit a terrorism offence; forfeiture of property on conviction of a terrorism offence; and forfeiture of property owned or controlled by terrorists. The Act requires financial institutions to report every three months whether they are in possession of any property owned or controlled by or on behalf of a terrorist group. In addition, financial institutions must report every transaction that is suspected to be related to the financing of terrorism to the ONDCP.

The Attorney General may revoke or deny the registration of a charity or nonprofit organization if it is believed funds from the organization are being used for financing terrorism. The GOAB circulates lists of terrorists and terrorist entities to all financial institutions in Antigua and Barbuda. No known evidence of terrorist financing has been discovered in Antigua and Barbuda to date. The GOAB has not undertaken any specific initiatives focused on the misuse of charities and nonprofit entities

The GOAB continues its bilateral and multilateral cooperation in various criminal and civil investigations and prosecutions. The amended Banking Act of 2004 enables the ECCB to share information directly with foreign regulators through an MOU. In 1999, a Mutual Legal Assistance Treaty (MLAT) and an Extradition Treaty with the United States entered into force. An extradition request related to a fraud and money laundering investigation remains pending under the treaty. The GOAB signed a Tax Information Exchange Agreement with the United States in December 2001. Because of such assistance, the GOAB has benefited through an asset sharing agreement and has received asset sharing revenues from the United States.

Antigua and Barbuda is a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD), and the Caribbean Financial Action Task Force (CFATF). The ONDCP joined the Egmont Group in June 2003. Antigua and Barbuda is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. On June 21, 2006 Antigua and Barbuda acceded to the UN Convention against Corruption.

The GOAB should implement and vigorously enforce all provisions of its anti-money laundering legislation including the strict and effective supervision of its offshore sector and gaming industry.

Despite the comprehensive nature of the law, Antigua and Barbuda has yet to prosecute a money laundering case. Moreover, there is an over-reliance on SARs to initiate investigations. Law enforcement and customs authorities should be trained to recognize money laundering typologies that fall outside the formal financial sector. The GOAB should vigorously enforce its anti-money laundering laws by actively prosecuting money laundering and other financial crimes.

## Argentina

Argentina is neither an important regional financial center nor an offshore financial center. Money laundering related to narcotics trafficking, corruption, contraband and tax evasion is believed to occur throughout the financial system, in spite of the efforts of the Government of Argentina (GOA) to stop it. The financial sector's gradual recovery from the 2001-02 financial crisis and post-crisis capital controls may have reduced the incidence of money laundering through the banking system. However, transactions conducted through nonbank sectors and professions, such as the insurance industry, financial advisors, accountants, notaries, trusts and companies, real or shell, remain viable mechanisms to launder illicit funds. Tax evasion is the predicate crime in the majority of Argentine money laundering investigations. Argentina has a long history of capital flight and tax evasion, and Argentines hold billions of dollars offshore, much of it legitimately earned money that was never taxed.

The GOA took several important steps to combat money laundering in 2006, including enacting amendments to its money laundering legislation with the passage of Law 26.087 in March, granting greater authority to Argentina's financial intelligence unit (the Unidad de Información Financiera, or UIF), creating a new National Coordination Unit in the Ministry of Justice and Human Rights to oversee and manage overall GOA anti-money laundering efforts, and creating a Special Prosecutors Unit within the Attorney General's Office for money laundering and terrorism finance cases. In addition, the Central Bank of Argentina (BCRA) completed plans for a specialized bank examination unit, announced in 2005, devoted specifically to money laundering and terrorism finance. On December 20, 2006, President Kirchner approved Argentina's long-awaited draft antiterrorism and counterterrorism financing law, which he sent to Congress for approval on the same day

Argentina's primary anti-money laundering legislation is Law 25.246 of May 2000. Law 25.246 expands the predicate offenses for money laundering to include all crimes listed in the Penal Code, sets a stricter regulatory framework for the financial sectors, and creates the UIF under the Ministry of Justice and Human Rights. The law requires customer identification, record keeping, and reporting of suspicious transactions by all financial entities and businesses supervised by the Central Bank, the Securities Exchange Commission (Comisión Nacional de Valores, or CNV), and the Superintendence for Insurance (Superintendencia de Seguros de la Nación, or SSN). The law forbids institutions to notify their clients when filing suspicious transaction reports (STRs), and provides a safe harbor from liability for reporting such transactions. Reports that are deemed by the UIF to warrant further investigation are forwarded to the Attorney General's Office. As of October 31, 2006, the UIF had received 2174 reports of suspicious or unusual activities since its inception in 2002, forwarded 136 suspected cases of money laundering to prosecutors for review, and assisted prosecutors with 107 cases. There have been only two money laundering convictions in Argentina since money laundering was first criminalized in 1989, and none since the passage of Law 25.246 in 2000.

On March 29, 2006, the Argentine Congress passed Law 26.087, amending and modifying Law 25.246, in order to address Financial Action Task Force (FATF) concerns regarding the inadequacies in Argentine money laundering and terrorism financing legislation and enforcement. The FATF conducted a mutual evaluation of Argentina in October 2003, which was accepted at the FATF plenary in June 2004 and at the plenary meetings of the Financial Action Task Force for South America (GAFISUD) in July 2004. While the evaluation of Argentina showed the UIF to be functioning

satisfactorily, it identified weaknesses in Argentina's anti-money laundering legislation, as well as the lack of terrorist financing legislation or a national anti-money laundering and counterterrorist financing coordination strategy.

Law 26.087 responds to many of the deficiencies noted by the FATF. It makes substantive improvements to existing law, including lifting bank, stock exchange and professional secrecy restrictions on filing suspicious activity reports; partially lifting tax secrecy provisions; clarifying which courts can hear requests to lift tax secrecy requests, and requiring decisions within 30 days. Law 26.087 also lowers the standard of proof required before the UIF can pass cases to prosecutors, and eliminates the so-called "friends and family" exemption contained in Article 277 of the Argentine Criminal Code for cases of money laundering, while narrowing the exemption in cases of concealment. Overall, the law clarifies the relationship, jurisdiction, and responsibilities of the UIF and the Attorney General's Office, and improves information sharing and coordination. The law also reduces restrictions that have prevented the UIF from obtaining information needed for money laundering investigations by granting greater access to STRs filed by banks. However, the law does not lift financial secrecy provisions on records of large cash transactions, which are maintained by banks when customers conduct a cash transaction exceeding 10,000 pesos (approximately $3,225). Also in response to FATF concerns, as noted in the mutual evaluation report, the Argentine government established a new National Coordination Unit in the Ministry of Justice and Human Rights. The National Coordination Unit represents Argentina at the FATF and GAFISUD, has the lead in developing money laundering and terrorism financing legislation, and manages the government's overall anti-money laundering and counterterrorist financing efforts.

The UIF, which began operating in June 2002, has issued resolutions widening the range of institutions and businesses required to report on suspicious or unusual transactions to the UIF beyond those identified in Law 25.246. Obligated entities include the tax authority (Administración Federal de Ingresos Publicos, or AFIP), Customs, banks, currency exchange houses, casinos, securities dealers, insurance companies, postal money transmitters, accountants, notaries public, and dealers in art, antiques and precious metals. The resolutions issued by the UIF also provide guidelines for identifying suspicious or unusual transactions. All suspicious or unusual transactions, regardless of the amount, must be reported directly to the UIF. Prior to the passage of Resolution 4/2005 in 2005, only suspicious or unusual transactions that exceeded 50,000 pesos (approximately $16,130) had to be reported; prior to 2004, suspicious transactions that were below a 500,000 peso threshold were first reported to the appropriate supervisory body for pre-analysis. Obligated entities are required to maintain a database of information related to client transactions, including suspicious or unusual transaction reports, for at least five years and must respond to requests from the UIF for further information within 48 hours.

In September 2006, Congress passed Law 26.119, which amends Law 25.246 to modify the composition of the UIF. The new law reorganizes the UIF's executive structure, changing it from a five-member directorship with rotating presidency to a structure that has a permanent, politically-appointed president and vice-president. Law 26.119 also establishes a UIF Board of Advisors, comprised of representatives of key government entities, including the Central Bank, AFIP, the Securities Exchange Commission, the national counternarcotics secretariat (SEDRONAR), and the Justice, Economy, and Interior Ministries. The Board of Advisors' opinions on UIF decisions and actions are nonbinding.

The Central Bank requires by resolution that all banks maintain a database of all transactions exceeding 10,000 pesos, and periodically submit the data to the Central Bank. Law 25.246 requires banks to make available to the UIF upon request records of transactions involving the transfer of funds (outgoing or incoming), cash deposits, or currency exchanges that are equal to or greater than 10,000 pesos. The UIF further receives copies of the declarations to be made by all individuals (foreigners or Argentine citizens) entering or departing Argentina with over US$10,000 in currency or monetary

instruments. These declarations are required by Resolutions 1172/2001 and 1176/2001 issued by the Argentine Customs Service in December 2001. In 2003, the Argentine Congress passed Law 22.415/25.821, which would have provided for the immediate fine of 25 percent of the undeclared amount, and for the seizure and forfeiture of the remaining undeclared currency and/or monetary instruments. However, the President vetoed the law because it allegedly conflicted with Argentina's commitments to MERCOSUR (Common Market of the Southern Cone).

Argentina's Narcotics Law of 1989 authorizes the seizure of assets and profits, and provides that these or the proceeds of sales will be used in the fight against illegal narcotics trafficking. Law 25.246 provided that proceeds of assets forfeited under this law can also be used to fund the UIF.

Although Law 25.246 of 2000 expands the number of predicate offenses for money laundering beyond narcotics-related offenses and created the UIF, it limits the UIF's role to investigating only money laundering arising from six specific crimes. The law also defines money laundering as an aggravation after the fact of the underlying crime. A person who commits a crime cannot be prosecuted for laundering money obtained from the crime; only someone who aids the criminal after the fact in hiding the origins of the money can be guilty of money laundering. Another impediment to Argentina's anti-money laundering regime is that only transactions (or a series of related transactions) exceeding 50,000 pesos can constitute money laundering. Transactions below 50,000 pesos can constitute only concealment, a lesser offense.

Terrorism and terrorist acts are not yet criminalized under Argentine law. Because these acts are not autonomous offenses, terrorist financing is not a predicate offense for money laundering. During 2005 and 2006, several bills were introduced in the Congress to implement the provisions of international treaties on terrorist financing under Argentine law. Various ministries in the government, as well as the "Comisión Mixta" (Mixed Commission—comprised of the Central Bank, Congress, Ministry of Economy, SEDRONAR, and Judicial branch), also developed draft counterterrorism finance laws. Argentina's new National Coordinator reviewed and harmonized the draft laws, and completed a final draft for the President to submit to Congress. The President approved the draft and sent it to Congress on December 20, 2006. Congress will consider it in March 2007, or in February if the President calls an extraordinary session. The draft law criminalizes both acts of terrorism and the financing of terrorism, and if approved, would provide the legal foundation for the UIF, Central Bank, and other law enforcement bodies to investigate and prosecute such crimes. FATF members will review either the draft or the newly enacted law during the February 2007 FATF Plenary to determine whether it meets international standards.

In the absence of terrorist financing legislation, the Central Bank issued Circular A 4273 in 2005 (titled "Norms on 'Prevention of Terrorist Financing'"), requiring banks to report any detected instances of the financing of terrorism. The Central Bank has regularly updated and modified the original Circular, with the most recent modification being Circular A 4599 of November 17, 2006. Bankers complain that the regulation is not backed by any legal definition of what constitutes terrorist financing in Argentina, and that the absence of domestic legislation means that they are not protected from lawsuits by clients if they report suspected cases of terrorist financing. The draft counterterrorism law currently before Congress would provide the necessary legal backing for the Central Bank's administrative measures. The Central Bank of Argentina also issued Circular B-6986 in 2004, instructing financial institutions to identify and freeze the funds and financial assets of the individuals and entities listed on the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. It modified this circular with Resolution 319 in October 2005, which expands Circular B-6986 to require financial institutions to check transactions against the terrorist lists of the United Nations, United States, European Union, Great Britain, and Canada. No assets have been identified or frozen to date.

On December 6, 2006, the U.S. Department of Treasury designated nine individuals and two entities in the Triborder Area between Argentina, Brazil and Paraguay that have provided financial or logistical support to Hizballah. According to the designation, the nine individuals operate in the Triborder Area and all have provided financial support and other services for Specially Designated Global Terrorist Assad Ahmad Barakat, who was previously designated by the U.S. Treasury in June 2004 for his support to Hizballah leadership. The two entities, Galeria Page and Casa Hamze, are located in Ciudad del Este, Paraguay, and have been utilized in generating or moving terrorist funds. The GOA has publicly disagreed with the designations, stating that the United States has not provided any new information that would prove terrorist financing activity is occurring in the Triborder Area.

Working with the U.S. Department of Homeland Security's Office of Immigration and Customs Enforcement (ICE), Argentina has established a Trade Transparency Unit (TTU). The TTU examines anomalies in trade data that could be indicative of customs fraud and international trade-based money laundering. The TTU will generate, initiate, and support investigations and prosecutions related to trade-based money laundering and the movement of criminal proceeds across international borders. One key focus of the TTU, as well as of other TTUs in the region, will be financial crimes occurring in the Triborder Area, which is bound by Puerto Iguazu, Argentina, Foz do Iguacu, Brazil, and Ciudad del Este, Paraguay. The creation of the TTU was a positive step towards complying with FATF Special Recommendation VI on Terrorist Financing via alternative remittance systems. Trade- based systems such as hawala often use fraudulent trade documents and over and under invoicing schemes to provide counter valuation in value transfer and settling accounts.

The GOA remains active in multilateral counternarcotics and international anti-money laundering organizations. It is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering, FATF and GAFISUD. The GOA is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the Inter-American Convention against Terrorism, and the UN Convention against Transnational Organized Crime. Argentina ratified the UN Convention against Corruption on August 28, 2006. Argentina participates in the "3 Plus 1" Security Group (formerly the Counter-Terrorism Dialogue) between the United States and the Triborder Area countries. The UIF has been a member of the Egmont Group since July 2003, and has signed memoranda of understanding regarding the exchange of information with a number of other financial intelligence units. The GOA and the USG have a Mutual Legal Assistance Treaty that entered into force in 1993, and an extradition treaty that entered into force in 2000.

With strengthened mechanisms available under Laws 26.119, 26.087 and 25.246, the ratification of the UN International Convention for the Suppression of the Financing of Terrorism, a reorganized UIF, and enhanced enforcement capability via the Special Prosecutors Unit and Central Bank's specialized bank examination unit, Argentina has the legal and regulatory capability to prevent and combat money laundering more effectively. Additional legislative and regulatory changes would significantly improve the anti-money laundering and counterterrorist financing regime in Argentina, particularly the passage of the domestic legislation criminalizing the financing of terrorism that is currently before Congress. The GOA should enact legislation to expand the UIF's role to enable it to investigate money laundering arising from all crimes, rather than just six enumerated crimes; establish money laundering as an independent offense; and eliminate the currently monetary threshold of 50,000 pesos required to establish a money laundering offense. To comply with the latest FATF recommendation on the regulation of bulk money transactions, Argentina will also need to review the legislation vetoed in 2003 to find a way to regulate such transactions consistent with its MERCOSUR obligations. Continuing priorities are the effective sanctioning of officials and institutions that fail to comply with the reporting requirements of the law, the pursuit of a training program for all levels of the criminal justice system, and the provision of the necessary resources to the UIF to carry out its mission. There is also a need for increased public awareness of the problem of money laundering and its connection to

narcotics, corruption and terrorism. Finally, the new National Coordinator's Office should alleviate the past problems of inadequate coordination and cooperation between government agencies.

## Aruba

Aruba is an autonomous and largely self-governing Caribbean island under the sovereignty of the Kingdom of the Netherlands; foreign, defense and some judicial functions are handled at the Kingdom level. Due to its geographic location and excellent infrastructure, Aruba is both attractive and vulnerable to money launderers and narcotics trafficking.

Aruba has four commercial and two offshore banks, one mortgage bank, two credit unions, an investment bank, a finance company, eleven credit institutions and eleven casinos. The island also has six registered money transmitters, two exempted U.S. money transmitters (Money Gram and Western Union), eight life insurance companies, fourteen general insurance companies, two captive insurance companies, and eleven company pension funds. As of October 27, 2006, there were 5,343 limited liability companies (NVs), of which 372 were offshore limited liability companies or offshore NVs, which may operate until 2007-2008. In addition, there are approximately 2,763 Aruba Exempt Companies (AECs), which mainly serve as vehicles for tax minimization, corporate revenue routing, and asset protection and management.

The offshore NVs and the AECs are the primary methods used for international tax planning in Aruba. The offshore NVs pay a small percentage tax and are subject to more regulation than the AECs. The AECs pay an annual $280 registration fee and must have a minimum of $6,000 in authorized capital. Both offshore NVs and AECs can issue bearer shares. A local managing director is required for offshore NVs. The AECs must have a local registered agent, which must be a trust company.

In 2001, the Government of Aruba (GOA) made a commitment to the Organization for Economic Cooperation and Development (OECD), in connection with the Harmful Tax Practices initiative, to modernize fiscal legislation in line with OECD standards. In 2003, the GOA introduced a New Fiscal Regime (NFR) containing a dividend tax and imputation credits. As of July 1, 2003, the incorporation of low tax offshore NVs was halted. The NFR contains a specific exemption for the AEC. Nevertheless, as a result of commitments to the OECD, the regime was brought in line with OECD standards as of January 2006. As a result of the NFR, Aruba's offshore regime will cease operations by the end of 2008.

Aruba currently has three designated free zones: Oranjestad Free Zone, Bushiri Free Zone and the Barcadera Free Zone, which are managed and operated by Free Zone Aruba (FZA) NV, a government limited liability company. Originally, only companies involved in trade or light industrial activities, including servicing, repairing and maintenance of goods with a foreign destination, could be licensed to operate within the free zones. However, State Ordinance Free Zones 2000 extended licensing to service-oriented companies (excluding financial services). Before being admitted to operate in the free zone, companies must submit a business plan along with personal data of managing directors, shareholders and ultimate beneficiaries, and must establish a limited liability company founded under Aruban law intended exclusively for free zone operations. Aruba took the initiative in the Caribbean Financial Action Task Force (CFATF) to develop regional standards for free zones in an effort to control trade-based money laundering. The guidelines were adopted at the CFATF Ministerial Council in October 2001. Free Zone Aruba NV is continuing the process of implementing and auditing the standards that have been developed.

Aruba was co-chair for the CFATF Typology on International Trade, which took place in Guatemala City in October 2006. Aruba presented the integrity system developed by Free Zone Aruba NV for the free trade zones, and requested feedback from the participating countries and international organizations. Resulting from Aruba's proposed typology is research on free trade zones in the region

in order to identify vulnerabilities, which should lead to an update of the CFATF Guidelines and provide important information for the Financial Action Task Force (FATF) work that is being done to counter trade-based money laundering.

The Central Bank of Aruba is the supervisory and regulatory authority for credit institutions, insurance companies, company pension funds and money transfer companies. The State Ordinance on the Supervision of Insurance Business (SOSIB) and the Implementation Ordinance on SOSIB brought insurance companies under the supervision of the Central Bank and require those established after July 1, 2001, to obtain a license. The State Ordinance on the Supervision of Money-Transfer Companies, effective August 12, 2003, places money transfer companies under the supervision of the Central Bank. Quarterly reporting requirements became effective in 2004. A State Ordinance on the supervision of trust companies, which will designate the Central Bank as the supervisory authority, is currently being drafted.

The anti-money laundering legislation in Aruba extends to all crimes that have a potential penalty of more than four years' imprisonment, including tax offenses. Aruba's criminal code allows for conviction-based forfeiture of assets. All financial and nonfinancial institutions are obligated to identify clients that conduct transactions over 20,000 Aruban guilders (approximately $11,300), and report suspicious transactions to Aruba's financial intelligence unit, the Meldpunt Ongebruikelijke Transacties (MOT). Obligated entities are protected from liability for reporting suspicious transactions. On July 1, 2001, reporting and identification requirements were extended by law to casinos and insurance companies.

The MOT is authorized to inspect all banks, money remitters, casinos, insurance companies and brokers for compliance with reporting requirements for suspicious transactions and the identification requirements for all financial transactions. The MOT is currently staffed by 12 employees. By September 2006, the MOT received 5,017 suspicious transaction reports, resulting in 86 investigations conducted and 22 cases transferred to the appropriate authorities. In June 2000, Aruba enacted a State Ordinance making it a legal requirement to report the cross-border transportation of currency in excess of 20,000 Aruban guilders to the customs department. The law also applies to express courier mail services. Reports generated are forwarded to the MOT to review, and in 2005, approximately 872 such reports were submitted. No data was provided for 2006.

The MOT shares information with other national government departments. On April 2, 2003, the MOT signed an information exchange agreement with the Aruba Tax Office, which is in effect and being implemented. Recently, the MOT and the Central Bank signed an information exchange memorandum of understanding (MOU), effective January 2006. The MOT is not linked electronically to the police or prosecutor's office. The MOT is a member of the Egmont Group and is authorized by law to share information with members of the Egmont Group through MOUs.

Aruba signed a multilateral directive with Colombia, Panama, the United States and Venezuela to establish an international working group to fight money laundering occurring through the Black Market Peso Exchange (BMPE). The final set of recommendations on the BMPE was signed on March 14, 2002. The working group developed policy options and recommendations to enforce actions that will prevent, detect and prosecute money laundering through the BMPE. The GOA is in the process of implementing the recommendations.

In 2004, the Penal Code of Aruba was modified to criminalize terrorism, the financing of terrorism, and related criminal acts. The Kingdom of the Netherlands is party to the UN International Convention for the Suppression of the Financing of Terrorism; however, its ratification extends only to the Kingdom in Europe.

Aruba participates in the FATF and the FATF mutual evaluation program through representation in the Kingdom of the Netherlands. The GOA has a local FATF committee comprised of officials from

different departments of the Aruban Government, under the leadership of the MOT, to oversee the implementation of FATF recommendations. The local FATF committee reviewed the GOA anti-money laundering legislation and proposed, in accordance with the nine FATF Special Recommendations on Terrorist Financing, amendments to existing legislation and introduction of new laws. Currently, Aruba is in compliance with seven of the nine FATF Special Recommendations. Aruba plans to introduce the Sanctions Ordinance to become fully compliant with the Special Recommendations. The GOA and the Netherlands formed a separate committee in 2004 to ensure cooperation of agencies within the Kingdom of the Netherlands in the fight against cross-border organized crime and international terrorism.

In 1999, the Netherlands extended application of the 1988 UN Drug Convention to Aruba. The Mutual Legal Assistance Treaty between the Netherlands and the United States applies to Aruba, though it is not applicable to requests for assistance relating to fiscal offenses addressed to Aruba. The Tax Information Exchange Agreement with the United States, signed in November 2003, became effective in September 2004. The GOA is a member of CFATF. The MOT became a member of the Egmont Group in 1997.

The Government of Aruba has shown a commitment to combating money laundering by establishing an anti-money laundering regime generally consistent with the recommendations of the FATF and the CFATF. Aruba should immobilize bearer shares under its fiscal framework and should enact its long-pending ordinance addressing the supervision of trust companies. Aruba should introduce the Sanctions Ordinance to become fully compliant with the FATF Special Recommendations on Terrorist Financing.

## Australia

Australia is one of the major centers for capital markets in the Asia-Pacific region. Annual turnover across Australia's over-the-counter and exchange-traded financial markets was AUD82 trillion (approximately $61.50 trillion) in 2005. Australia's total stock market capitalization is over AUD1.2 trillion (approximately $905 billon), making it the eighth largest market in the world, and the third largest in the Asia-Pacific region behind Japan and Hong Kong. Australia's foreign exchange market is ranked seventh in the world by turnover, with the U.S. dollar and the Australian dollar the fourth most actively traded currency pair globally. While narcotics offences provide a substantial source of proceeds of crime, the majority of illegal proceeds are derived from fraud-related offences. One Australian Government estimate suggested that the amount of money laundered in Australia ranges between AUD2-3 billion (approximately $1.5-$2.25 billion) per year.

The Government of Australia (GOA) has maintained a comprehensive system to detect, prevent, and prosecute money laundering. The last four years have seen a noticeable increase in activities investigated by Australian law enforcement agencies that relate directly to offenses committed overseas. Australia's system has evolved over time to address new money laundering and terrorist financing risks identified through continuous consultation between government agencies and the private sector.

In March 2005, the Financial Action Task Force (FATF) conducted its on-site Mutual Evaluation (FATFME) of Australia's anti-money laundering/counterterrorism financing (AML/CTF) system. Australia is one of the first member countries to be evaluated under FATF's revised recommendations. The FATF's findings from the mutual evaluation of Australia were published in October 2005 and Australia was found to be compliant or largely complaint with just over half of the FATF Recommendations. The FATFME noted that although Australia "has a comprehensive money laundering offense… the low number of prosecutions …indicates…that the regime is not being effectively implemented."

In response, the GOA has committed to reforming Australia's AML/CTF system to implement the revised FATF Forty plus Nine recommendations. The Attorney General's Department (AGD) is coordinating this process, now underway, which is expected to significantly reshape Australia's current AML/CTF regime in line with current international best practices.

Australia criminalized money laundering related to serious crimes with the enactment of the Proceeds of Crime Act 1987. This legislation also contained provisions to assist investigations and prosecution in the form of production orders, search warrants, and monitoring orders. It was superseded by two acts that came into force on January 1, 2003 (although proceedings that began prior to that date under the 1987 law will continue under that law). The Proceeds of Crime Act 2002 provides for civil forfeiture of proceeds of crime as well as for continuing and strengthening the existing conviction-based forfeiture scheme that was in the Proceeds of Crime Act 1987. The Proceeds of Crime Act 2002 also enables freezing and confiscation of property used in, intended to be used in, or derived from, terrorism offenses. It is intended to implement obligations under the UN International Convention for the Suppression of the Financing of Terrorism and resolutions of the UN Security Council relevant to the seizure of terrorism-related property. The Act also provides for forfeiture of literary proceeds where these have been derived from commercial exploitation of notoriety gained from committing a criminal offense.

The Proceeds of Crime (Consequential Amendments and Transitional Provisions) Act 2002 (POCA 2002), repealed the money laundering offenses that had previously been in the Proceeds of Crime Act 1987 and replaced them with updated offenses that have been inserted into the Criminal Code. The new offenses are graded according both to the level of knowledge required of the offender and the value of the property involved in the activity constituting the laundering. As a matter of policy all very serious offenses are now gradually being placed in the Criminal Code. POCA 2002 also enables the prosecutor to apply for the restraint and forfeiture of property from proceeds of crime. POCA 2002 further creates a national confiscated assets account from which, among other things, various law enforcement and crime prevention programs may be funded. Recovered proceeds can be transferred to other governments through equitable sharing arrangements.

Underneath the framework of offenses, the Financial Transaction Reports Act (FTR Act) of 1988 was enacted to combat tax evasion, money laundering, and serious crimes. The FTR Act requires banks and nonbanking financial entities (collectively referred to as cash dealers) to verify the identities of all account holders and signatories to accounts, and to retain the identification record, or a copy of it, for seven years after the day on which the relevant account is closed. A cash dealer, or an officer, employee, or agent of a cash dealer, is protected against any action, suit, or proceeding in relation to the reporting process. The FTR Act also establishes reporting requirements for Australia's financial services sector. Required to be reported are: suspicious transactions, cash transactions equal to or in excess of AUD10,000 (approximately $7,500), and all international funds transfers into or out of Australia, regardless of value. The FTR Act also obliges any person causing an international movement of currency of Australian AUD10,000 (or a foreign currency equivalent) or more, into or out of Australia, either in person, as a passenger, by post or courier to make a report of that transfer.

FTR Act reporting also applies to nonbank financial institutions such as money exchangers, money remitters, stockbrokers, casinos and other gambling institutions, bookmakers, insurance companies, insurance intermediaries, finance companies, finance intermediaries, trustees or managers of unit trusts; issuers, sellers, and redeemers of travelers checks, bullion sellers, and other financial services licensees. Solicitors (lawyers) also are required to report significant cash transactions. Accountants do not have any FTR Act obligations. However, they do have an obligation under a self-regulatory industry standard not to be involved in money laundering transactions.

The FTR Act established the Australian Transaction Reports Analysis Centre (AUSTRAC), Australia's financial intelligence unit (FIU). AUSTRAC collects, retains, compiles, analyzes, and

disseminates FTR information. AUSTRAC is Australia's AML/CTF regulator. AUSTRAC also provides advice and assistance to revenue collection, social justice, national security, and law enforcement agencies, and issues guidelines to cash dealers regarding their obligations under the FTR Act and regulations. As such, AUSTRAC plays a central role in Australia's AML system both domestically and internationally. During the 2005-06 Australian financial year, AUSTRAC's FTR information was used in 1,582 operational matters. Of these, in 431 matters FTR information was identified as being very valuable to outcomes. Results from the Australian Taxation Office shows that the FTR information contributed to more than AUD90.7 million (approximately $68 million) in Australian Taxation Office assessments during the year. In 2005-06, AUSTRAC received 13,880,944 financial transaction reports, with 99.6 percent of the reports submitted electronically through the EDDS Web system. AUSTRAC received 24,801 suspect transaction reports (SUSTRs), an increase of 44.1 percent from the precious year.

In 2006, there was a significant increase in the total number of financial transaction reports received by AUSTRAC. Significant cash transactions reports (SCTRs) account for 17 percent of the total number of FTRs reported to AUSTRAC in the 2005-06 Australian financial year and are reported by cash dealers and solicitors. In 2005-06, AUSTRAC received 2,416,427 SCTRs, an increase of 5.6 percent from the previous year. Cash dealers are required to report all international funds transfer instructions (IFTIs) to AUSTRAC. Cash dealers reported 11,411,961 IFTIs to AUSTRAC-a 11.4 percent increase from 2005. International currency transfer reports (ICTR) are primarily declared to the Australian Customs Service by individuals when they enter or depart from Australia. AUSTRAC received 27,755 ICTRs—a 6.0 percent increase from the previous year. In April 2005, the Minister for Justice and Customs launched AUSTRAC's AML eLearning application. This application has been well received by cash dealers as a tool in providing basic education on the process of money laundering, the financing of terrorism, and the role of AUSTRAC in identifying and assisting investigations of these crimes

APRA is the prudential supervisor of Australia's financial services sector. AUSTRAC regulates anti-money laundering/counterterrorist financing (AML/CTF) compliance. AUSTRAC's powers include criminal but not administrative sanctions for noncompliance. AUSTRAC has conducted very few compliance audits in recent years and places a great deal of emphasis on educating and continuously engaging the private sector regarding the evolution of AML/CTF regime and the attendant reporting requirements. The FATFME noted that a comprehensive system for AML/CTF compliance for the entire financial sector needed to be established by the GOA, as does an administrative penalty regime for AML/CTF noncompliance.

In June 2002, Australia passed the Suppression of the Financing of Terrorism Act 2002 (SFT Act). The aim of the SFT Act is to restrict the financial resources available to support the activities of terrorist organizations. This legislation criminalizes terrorist financing and substantially increases the penalties that apply when a person uses or deals with suspected terrorist assets that are subject to freezing. The SFT Act enhances the collection and use of financial intelligence by requiring cash dealers to report suspected terrorist financing transactions to AUSTRAC, and relaxes restrictions on information sharing with relevant authorities regarding the aforementioned transactions. The SFT Act also addresses commitments Australia has made with regard to the UNSCR 1373 and is intended to implement the UN International Convention for the Suppression of the Financing of Terrorism. Under this Act three accounts related to an entity listed on the UNSCR 1267 Sanction Committee's consolidated list, the International Sikh Youth Federation, were frozen in September 2002. There have been no arrests or prosecutions under this legislation. The Security Legislation Amendment (Terrorism) Act 2002 also inserted new criminal offenses in the Criminal Code for receiving funds from, or making funds available to, a terrorist organization

The Anti-Terrorism Act (No.2) 2005 (AT Act), which took effect on December 14, 2006, amends offenses related to the funding of a terrorist organization in the Criminal Code so that they also cover

the collection of funds for or on behalf of a terrorist organization. The AT Act also inserts a new offense of financing a terrorist. The SFT Act amendments to the FTR Act were a significant milestone in the enhancement of AUSTRAC's international efforts. These amendments gave the Director of AUSTRAC the right to establish agreements with international counterparts to directly exchange intelligence, spontaneously and upon request. A review of the FTR Act is currently being undertaken to improve procedures, implement international best practices, and address further aspects of terrorist financing, including alternative remittance systems.

Investigations of money laundering reside with the Australian Federal Police (AFP) and Australian Crime Commission (Australia's only national multi- jurisdictional law enforcement agency). The AFP is the primary law enforcement agency for the investigation of money laundering and terrorist-financing offences in Australia at the Commonwealth level and has both a dedicated Financial Crimes Unit and Financial Investigative Teams (FIT) consisting of 44 members with primary responsibility for asset identification/restraint and forfeiture under the POCA 2002. The Commonwealth Director of Public Prosecutions (CDPP) prosecutes offences against Commonwealth law and to recover proceeds of Commonwealth crime. The main cases prosecuted by the CDPP involve drug importation and money laundering offences. No convictions for money laundering have been reported for 2006.

In April 2003, the AFP established a Counter Terrorism Division to undertake intelligence-led investigations to prevent and disrupt terrorist acts. Eleven Joint Counter Terrorism Teams (JCTT), including investigators and analysts with financial investigation skills and experience, are conducting a number of investigations specifically into suspected terrorist financing in Australia. The AFP also works closely with overseas counterparts in the investigation of terrorist financing, and has worked closely with the FBI on matters relating to terrorist financing structures in South East Asia. In 2006, AFP introduced mandatory consideration of potential money laundering and crime proceeds into its case management processes, thereby ensuring that case officers explore the possibility of money laundering and crime proceeds actions in all investigations conducted by the AFP.

A draft AML/CTF bill developed by the AGD and a package of draft AML/CTF Rules, developed by AUSTRAC, were released for public comment in December 2005 and received Royal Assent on December 12, 2006. The AML/CTF Act covers the financial sector, gambling, bullion dealing and any other professionals or businesses that provide particular designated services and imposes a number of obligations including customer due diligence, reporting requirements, record keeping, and establishing AML/CTF programs. The Act will implement a risk-based approach to regulation. Implementation will occur over a two-year period and include consultation with reporting entities. Under the Act, AUSTRAC will now have an expanded role as the national AML/CTF regulator with supervisory, monitoring and enforcement functions over a diverse range of business sectors.

The package of draft legislation and rules formed the basis for consultations on proposed enhancements to current customer due diligence, reporting and record keeping obligations, and deficiencies in regulatory coverage identified in Australia's FATF Mutual Evaluation Report. The consultation package represented a first tranche of reforms. The final component of the first tranche commences in December 2008.

Once the first tranche of AML/CTF reforms are implemented. the Australian Government will consider a second tranche of reforms (to begin in 2007), extending to real estate agents, jewelers, and specified nonfinancial legal and accounting services. Lawyers and accountants are also included in the first tranche, but only where they compete with the financial sector and not for general services, which will be included in the second tranche. The proposed legislative framework authorizes operational details to be settled in AML/CTF Rules, which will be developed by (AUSTRAC) in consultation with industry.

Australia is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime and its

protocol on migrant smuggling. In September, 1999, a Mutual Legal Assistance Treaty between Australia and the United States entered into force. Australia participates actively in a range of international fora including the FATF, the Pacific Islands Forum, and the Commonwealth Secretariat. Through its funding and hosting of the Secretariat of the Asia/Pacific Group on Money Laundering, of which it serves as permanent co-chair, the GOA has elevated money laundering and terrorist financing issues to a priority concern among countries in the Asia/Pacific region. AUSTRAC is an active member of the Egmont Group of Financial Intelligence Units (FIUs). AUSTRAC has signed exchange Instruments, mostly in the form of Memoranda of understanding (MOUs) allowing the exchange of financial intelligence with FinCEN and the FIUs of 45 other countries.

Following the bombings in Bali in October 2002, the Australian Government announced an AUD10 million (approximately $7.5 million) initiative managed by the Australian Agency for International Development (AusAID), to assist in the development of counterterrorism capabilities in Indonesia. As part of this initiative, the AFP has established a number of training centers such as the Jakarta Centre for Law Enforcement Cooperation. As part of Australia's broader regional assistance initiatives, AUSTRAC continued its South East Asia Counter Terrorism Program of providing capacity building assistance to 10 South East Asian nations, to develop capacity in detecting and dealing with terrorist financing and money laundering. AUSTRAC is also providing further assistance in terms of IT system enhancement to the Indonesian FIU, PPATK (Indonesian Financial Transaction Reports and Analysis Center). AUSTRAC has provided training and other technical assistance to other developing FIUs in Southeast Asia. In the Pacific region, AUSTRAC has developed and provided unique software and training for personnel to five nascent Pacific island FIUs to fulfill their domestic obligations and share information with foreign analogs. AUSTRAC is also providing a larger scale information management system solution for the Fiji FIU to enable the collection and analysis of financial transaction reports. The AGD received a grant of AUD 7.7 million (approximately $5.75) to develop a four year program to enhance AML/CTF regimes for the Pacific island jurisdictions. The AGD's program will work cooperatively with the U.S. Department of State-funded Pacific Islands Anti-Money Laundering Program (PALP). The PALP, a four-year program, will be managed by the Pacific Islands Forum (PIF) and will employ residential mentors to develop or enhance existing AML/CTF regimes in the fourteen non-FATF member states of the PIF.

The GOA continues to pursue a comprehensive, anti-money laundering/counterterrorist financing regime that meets the objectives of the revised FATF Forty Recommendations and Nine Special Recommendations on Terrorist Financing. To enhance its AML/CTF regime, as noted in the FATF mutual evaluation, AUSTRAC has been provided with substantially increased powers to ensure compliance. There will be more on-site compliance audits and AUSTRAC can require regular compliance reports from reporting entities; can initiate monitoring orders and statutory demands for information and documents; can seek civil penalty orders, remedial directions and injunctions; and, can require a reporting entity to subject itself to an external audit of its AML/CTF program. The AML/CTF Act also provides for greater coordination amongst the regulatory agencies of its financial, securities and insurance sectors.

The GOA is continuing its exemplary leadership role in emphasizing money laundering/terrorist finance issues and trends within the Asia/Pacific region and its commitment to providing training and technical assistance to the jurisdictions in that region. Having significantly enhanced its increased focus on AML/CTF deterrence, the Government of Australia should increase its efforts to prosecute and convict money launderers.

## Austria

Austria is not an important financial center, offshore tax haven, or banking center, but Austrian banking groups control significant shares of the banking markets in Central, Eastern and Southeastern

Europe. According to the 2004 IMF Financial Stability Assessment report, Austria also has one of the highest numbers of per capita bank and branches in the world, with about 900 banks and one bank branch for every 1500 people. Austria does not have a reputation as a major money laundering country. However, like any financial marketplace, Austria's financial and nonfinancial institutions are vulnerable to money laundering. The percentage of undetected organized crime is thought to be enormous, with much of it coming from the former Soviet Union. Money that organized crime launders derives primarily from serious fraud, corruption, narcotics trafficking and trafficking in persons.

Money laundering occurs within the Austrian banking system as well as in nonbank financial institutions and businesses. Criminal groups seem increasingly to use money transmitters and informal money transfer systems to launder money. The Internet and offshore companies also play an important role in such crime.

Austria criminalized money laundering in 1993. Predicate offenses include terrorist financing and many other serious crimes. Regulations are stricter for money laundering by criminal organizations and terrorist "groupings," because in such cases the law requires no proof that the money stems directly or indirectly from prior offenses.

Amendments to the Customs Procedures Act and the Tax Crimes Act, effective May 1, 2004, address the problem of cash couriers and international transportation of currency and monetary instruments from illicit sources. Austrian customs authorities do not automatically screen all persons entering Austria for cash or monetary instruments. However, if asked, anyone carrying 10,000 euros (approximately $12,400) or more must declare the funds and provide information on their source and use. To implement the new European Union (EU) regulation on controls of cash entering or leaving the EU, the Government of Austria (GOA) recently amended the Customs Procedures Act and the Tax Crimes Act, lowering the threshold for the "if asked" declaration obligation to 10,000 euros from 15,000 euros ($18,600) as of August 1, 2006. Spot checks for currency at border crossings will continue. Customs officials have the authority to seize suspect cash at the border. An increasing problem is the use of prepaid cards and credit cards loaded with cash.

The Banking Act of 1994 creates customer identification, record keeping, and staff training obligations for the financial sector. Entities subject to the Banking Act include banks, leasing and exchange businesses, safe custody services, and portfolio advisers. The law requires identification of all customers when entering an ongoing business relationship. This would include all cases of opening a checking account, a passbook savings account, a securities deposit account, etc. In addition, the Banking Act requires customer identification for all transactions of more than 15,000 euros ($18,600) for customers without a permanent business relationship with the bank. The law also requires banks and other financial institutions to keep records on customers and account owners. The Securities Supervision Act of 1996, which covers trade of securities, shares, money market instruments, options and other instruments listed on an Austrian stock exchange or any regulated market in the EU, refers to the Banking Act's identification regulations. The Insurance Act of 1997 includes similar regulations for insurance companies underwriting life policies. Since January 1, 2004, money remittance businesses require a banking license from the Financial Market Authority (FMA) and are subject to supervision. Informal remittance systems like hawala exist in Austria but are subject to administrative fines for carrying out banking business without a license.

The Banking Act protects bankers and all other reporting individuals (auctioneers, real estate agents, lawyers, notaries, etc.) with respect to their cooperation with law enforcement agencies. They are also not liable for damage claims resulting from delays in completing suspicious transactions. There is no requirement for banks to report large currency transactions, unless they are suspicious. The Austrian Financial Intelligence Unit (AFIU), however, regularly provides information to banks to raise awareness of large cash transactions.

Since October 2003, financial institutions have adopted tighter identification procedures, requiring all customers appearing in person to present an official photo identification card. These procedures also apply to trustees of accounts, who must disclose the identity of the account beneficiary. However, the procedures still allow customers to carry out non-face-to-face transactions, including Internet banking, on the basis of a secure electronic signature or a copy of a picture ID and a legal business declaration submitted by registered mail.

The Banking Act includes a due diligence obligation, and the law holds individual bankers responsible if their institutions launder money. In addition, banks have signed a voluntary agreement to prohibit active support of capital flight. The Federal Economic Chamber's Banking and Insurance Department, in cooperation with all banking and insurance associations, has also published an official Declaration of the Austrian Banking and Insurance Industries to Prevent Financial Transactions in Connection with Terrorism.

Amendments in 2003 to the Austrian Gambling Act, the Business Code, and the Austrian laws governing lawyers, notaries, and accounting professionals introduced additional money laundering regulations. The legislation concerns identification, record keeping, and reporting of suspicious transactions for dealers in high-value goods (such as precious stones or metals, or works of art), auctioneers, real estate agents, casinos, lawyers, notaries, certified public accountants, and auditors.

During Austria's EU Presidency in the first half of 2006, the GOA, in various EU committees and bodies, facilitated the implementation of guidelines for the Financial Action Task Force's (FATF) Special Recommendation VII on wire transfers as well as the EU's Third Money Laundering Directive (Directive 2005/60/EC). The EU regulation on wire transfers entered into force on January 1, 2007, and became immediately and directly applicable in Austria. The GOA also hosted a workshop on nonprofit organizations, terrorism financing and financial sanctions.

Since 2002, the AFIU, the central repository of suspicious transaction reports, has been a section of the Austrian Interior Ministry's Bundeskriminalamt (Federal Criminal Intelligence Service). According to Interpol's General Secretariat, 40 percent of queries that Austria sends have resulted in positive leads. During the first nine months of 2006, the AFIU received 521 suspicious transaction reports from banks and fielded requests for information from Interpol, Europol, members of the Egmont Group, and other authorities. This represents an increase from the 467 suspicious transactions reported in 2005, which led to three convictions for money laundering. Criminals are often convicted for other crimes, however, with money laundering serving as additional grounds for conviction. In 2005, authorities instituted legal proceedings for money laundering in 13 cases, but data on convictions are not yet available. According to the AFIU, the increase in suspicious transaction reports in the first nine months of 2006 is due to higher sensitivity to money laundering, an improved reporting attitude, and the reporting of problems with "phishing" e-mails.

Legislation implemented in 1996 allows for asset seizure and the forfeiture of illegal proceeds. The banking sector generally cooperates with law enforcement efforts to trace funds and seize illicit assets. The distinction between civil and criminal forfeiture in Austria is different from that in the U.S. legal system. However, Austria has regulations in the Code of Criminal Procedure that are similar to civil forfeiture. In connection with money laundering, organized crime and terrorist financing, all assets are subject to seizure and forfeiture, including bank assets, other financial assets, cars, legitimate businesses, and real estate. Courts may freeze assets in the early stages of an investigation. In the first eight months of 2006, Austrian courts froze assets worth 24 million euros (approximately $30 million). In 2005, courts froze assets worth 99.2 million euros (approximately $124.0 million).

The amended Extradition and Judicial Assistance Law provides for expedited extradition, expanded judicial assistance, and acceptance of foreign investigative findings in the course of criminal investigations, as well as enforcement of foreign court decisions. Austria has strict bank secrecy regulations, though bank secrecy can be lifted in cases of suspected money laundering. Moreover,

bank secrecy does not apply in cases in which banks and other financial institutions must report suspected money laundering. Such cases are subject to instructions of the authorities (i.e., AFIU) with regard to processing such transactions.

The 2002 Criminal Code Amendment introduced the following new criminal offense categories: terrorist "grouping," terrorist criminal activities, and financing of terrorism. The Criminal Code defines "financing of terrorism" as a separate criminal offense category in the Criminal Code, punishable in its own right. Terrorism financing is also included in the list of criminal offenses subject to domestic jurisdiction and punishment, regardless of the laws where the act occurred. Furthermore, the money laundering offense is expanded to terrorist "groupings." The law also gives the judicial system the authority to identify, freeze, and seize terrorist financial assets. With regard to terrorist financing, forfeiture regulations cover funds collected or held available for terrorist financing, and permit freezing and forfeiture of all assets that are in Austria, regardless of the place of the crime and the whereabouts of the criminal.

The Austrian authorities have circulated to all financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists that the United States has designated pursuant to E.O. 13224, and EU lists. According to the Ministry of Justice and the AFIU, no accounts found in Austria ultimately have shown any links to terrorist financing. The AFIU immediately shares all reports on suspected terrorism financing with the Austrian Interior Ministry's Federal Agency for State Protection and Counterterrorism (BVT). Figures on suspected terrorism financing transaction reports in 2005 and 2006 are not yet available. There were no convictions for terrorism financing in 2005.

The GOA has undertaken important efforts that may help thwart the misuse of charitable or nonprofit entities as conduits for terrorist financing. The GOA has generally implemented the FATF's Special Recommendation on Terrorist Financing regarding nonprofit organizations. The Law on Associations (Vereinsgesetz, published in Federal Law Gazette No. I/66 of April 26, 2002), which has been in force since July 1, 2002, covers charities and all other nonprofit associations in Austria. The law regulates the establishment of associations, bylaws, organization, management, association registers, appointment of auditors, and detailed accounting requirements. On January 1, 2007, special provisions will become effective for associations whose finances exceed a certain threshold. Each association must appoint two independent auditors and must inform its members about its finances and the auditors' report. Associations with a balance sheet exceeding 3 million euros ($3.72 million) or annual donations of more than 1 million euros ($1.24 million) have to appoint independent auditors to review and certify the financial statements. Public collection of donations requires advance permission from the authorities. Since January 1, 2006, the newly established Central Register of Associations (Zentrales Vereinsregister) offers basic information on all registered associations in Austria free of charge via the Internet. The FMA recently announced intentions to employ 45 additional auditors to focus on combating money laundering, terrorist financing, as well as to better monitor offshore banking and charitable foundations.

Another law, the Law on Responsibility of Associations (Verbandsverantwortlichkeitsgesetz, published in Federal Law Gazette No.I/151 of December 23, 2005), came into force on January 1, 2006, and introduced criminal responsibility for all legal entities, general and limited commercial partnerships, registered partnerships and European Economic Interest Groupings, but not charitable or nonprofit entities. The law covers all crimes listed in the Criminal Code, including corruption, money laundering and terrorist financing.

Austria has not yet enacted legislation that provides for sharing forfeited narcotics-related assets with other governments. A bilateral U.S.-Austria agreement on sharing of forfeited assets remains under negotiation. In addition to the exchange of information with home country supervisors permitted by the EU, Austria has defined this information exchange more precisely in agreements with nine other

EU members (France, Germany, Italy, Netherlands, United Kingdom, the Czech Republic, Hungary, Slovakia, and Slovenia), as well as Bulgaria and Croatia. Austria has also given assistance to countries needing guidance in developing effective AML/CFT regimes: in March 2006, under the auspices of the EU, Austria assisted the FYROM with discussions highlighting Austria's experience, and best practices in AML, confiscation and seized assets management.

Austria is a party to the 1988 UN Drug Convention, the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. The GOA ratified the UN Convention against Corruption on January 11, 2006. Austria is a member of the EU and FATF, and a FATF mutual evaluation of Austria will take place in 2008. The AFIU is a member of the Egmont Group.

The Government of Austria has implemented a viable anti-money laundering and counterterrorist financing regime, and is generally cooperative with U.S. authorities in money laundering cases. However, certain deficiencies remain. There is a need for identification procedures for customers in non-face-to-face banking transactions. The GOA should amend its criminal code to penalize negligence in reporting money laundering and terrorist financing transactions. In spite of increases in suspicious transaction reporting and money laundering convictions in 2006, the AFIU and law enforcement require sufficient resources to adequately perform their functions. Finally, AFIU and other government personnel should be protected against damage claims because of delays in completing suspicious transactions until sufficient resources are provided to ensure timely reporting. The GOA should also ensure that it enhances inspections at its borders to protect against the cross-border transport of cash and negotiable instruments in concert with FATF Special Recommendation IX on Terrorist financing.

## Bahamas

The Commonwealth of The Bahamas is an important regional and offshore financial center. The financial services sector provides vital economic contribution to The Bahamas, accounting for approximately 15 percent of the country's gross domestic product. The U.S. dollar circulates freely in The Bahamas, and is accepted everywhere on par with the Bahamian dollar. Money laundering in The Bahamas is related to financial fraud and the proceeds of drug trafficking. Illicit proceeds from drug trafficking usually take the form of cash or are quickly converted into cash. The strengthening of anti-money laundering laws has made it increasingly difficult for most drug traffickers to deposit large sums of cash. As a result, drug traffickers store extremely large quantities of cash in security vaults at properties deemed to be safe houses. Other money laundering trends include the purchase of real estate, large vehicles and jewelry, as well as the processing of money through a complex national or international web of legitimate businesses and shell companies.

The Bahamas has two 24-hour casinos in Nassau, one in Freeport/Lucaya, and one in Great Exuma. Cruise ships that overnight in Nassau may operate casinos. Reportedly, there are over ten internet gaming sites based in The Bahamas, although internet gambling is illegal in The Bahamas. Under Bahamian law, Bahamian residents are prohibited from gambling. Freeport is home to The Bahamas' only free trade zone. There are no indications that it is used to launder money.

The Central Bank of The Bahamas is responsible for the licensing, regulation, and supervision of banks and trust companies operating in The Bahamas. The Central Bank Act 2000 (CBA) and The Banks and Trust Companies Regulatory Act 2000 (BTCRA) enhanced the supervisory powers of the Central Bank and provide the Central Bank with extensive information gathering powers, including on-site inspection of banks and enhanced cooperation between overseas regulatory authorities and the Central Bank. The BTCRA expands the licensing criteria for banks and trust companies, enhances the supervisory powers of the Inspector of Banks and Trust Companies, and enhances the role of the

Central Bank's Governor. These expanded rights include the right to deny licenses to banks or trust companies deemed unfit to transact business in The Bahamas. In 2001, the Central Bank enacted a physical presence requirement that means "managed banks" (those without a physical presence but which are represented by a registered agent such as a lawyer or another bank) must either establish a physical presence in The Bahamas (an office, separate communications links, and a resident director) or cease operations. The transition to full physical presence is complete. Some industry sources have suggested that this requirement has contributed to a decline in banks and trusts from 301 in 2003 to 250 at the end of 2005.

The International Business Companies Act 2000 and 2001 (Amendments) enacted provisions that abolish bearer shares, require international business companies (IBCs) to maintain a registered office in The Bahamas, and require a copy of the register of the names and addresses of the directors and officers and a copy of the shareholders register to be kept at the registered office. A copy of the register of directors and officers must also be filed with the Registrar General's office. Only banks and trust companies licensed under the BTCRA and financial and corporate service providers licensed under the Financial Corporate Service Providers Act (FCSPA) may provide registration, management, administration, registered agents, registered offices, nominee shareholders, and officers and directors for IBCs.

Money laundering is criminalized under the Proceeds of Crime Act 2000. The Financial Transaction Reporting Act 2000 (FTRA) establishes "know your customer" (KYC) requirements. By December 31, 2001, financial institutions were obliged to verify the identities of all their existing account holders and of customers without an account who conduct transactions over $10,000. All new accounts established in 2001 or later have to be in compliance with KYC rules before they are opened. As of October 2006, the Central Bank reported full compliance with KYC requirements. All nonverified accounts have been frozen.

The FTRA requires financial and nonfinancial institutions to report suspicious transactions to the financial intelligence unit (FIU) when the institution suspects or has reason to believe that any transaction involves the proceeds of crime. The FIU Act 2000 protects obligated entities from criminal or civil liability for reporting transactions. Financial institutions are required by law to maintain records related to financial transactions for no less than five years. Established by the FIU Act 2000, The Bahamas FIU operates as an independent administrative body under the Office of the Attorney General, and is responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs). The FIU is also responsible for publishing guidelines to advise entities of their reporting obligations. Presently, the FIU is in the process of revising its guidelines to incorporate terrorist financing reporting requirements, and is expected to publish the new guidelines in early 2007.

The FIU has the administrative power to issue an injunction to stop anyone from completing a transaction for a period of up to three days upon receipt of an STR. In 2005 there were nine cases of asset restraint as a result of suspicious transactions. From January to September 2006, the FIU received 124 STRs, of which 60 were being analyzed and 15 were forwarded to the police for investigation. If money laundering is suspected, the FIU will disseminate STRs to the Tracing and Forfeiture/Money Laundering Investigation Section (T&F/MLIS) of the Drug Enforcement Unit (DEU) of the Royal Bahamas Police Force for investigation and prosecution in collaboration with the Office of the Attorney General.

Between January 2000 and September 2006, 17 individuals were charged with money laundering by the T&F/MLIS, leading to seven convictions. Seven defendants await trail, while two defendants fled the jurisdiction prior to trial. As a matter of law, the Government of the Commonwealth of the Bahamas (GOB) seizes assets derived from international drug trade and money laundering. The banking community has cooperated with these efforts. During 2006, nearly two million dollars in cash and assets were seized or frozen. The seized items are in the custody of the GOB. Some are in the

process of confiscation while some remain uncontested. Seized assets may be shared with other jurisdictions on a case-by-case basis.

In 2004, the Anti-Terrorism Act (ATA) was enacted to implement the provisions of the UN International Convention for the Suppression of the Financing of Terrorism. In addition to formally criminalizing terrorism and making it a predicate crime for money laundering, the law provides for the seizure and confiscation of terrorist assets, reporting of suspicious transactions related to terrorist financing, and strengthening of existing mechanisms for international cooperation. To date, there have been no suspicious transactions or prosecutions for violation of the ATA.

The Bahamas is a party to the UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The Bahamas has signed, but has not yet ratified, the UN Convention against Transnational Organized Crime and the Inter-American Convention against Terrorism. The GOB has neither signed nor ratified the UN Convention against Corruption. The Bahamas is a member of the Caribbean Financial Action Task Force (CFATF) and recently underwent a Mutual Evaluation in June 2006. The FIU has been an active participant within the Egmont Group since becoming a member in 2001, and is currently one of the two regional representatives for the Americas. The Bahamas has a Mutual Legal Assistance Treaty with the United States, which entered into force in 1990, and agreements with the United Kingdom and Canada. The Attorney General's Office for International Affairs manages multilateral information exchange requests. In December 2004, the Bahamas signed an agreement for future information exchange with the U.S. Securities and Exchange Commission to ensure that requests can be completed in an efficient and timely manner. The Bahamas FIU has the ability to sign memoranda of understanding with other FIUs for the exchange of information.

The GOB has enacted substantial reforms to reduce its vulnerability to money laundering and terrorist financing. The GOB should continue to enhance its supervision of financial institutions, especially investment funds. The Bahamas should also provide adequate resources to its law enforcement, prosecutorial and judicial entities to ensure that investigations and prosecutions are satisfactorily completed and requests for international cooperation are efficiently processed.

## Bahrain

Bahrain has one of the most diversified economies in the Gulf Cooperation Council (GCC). In contrast to most of its neighbors, oil accounted for only 11.1 percent of Bahrain's gross domestic product (GDP) in 2005. Bahrain has promoted itself as an international financial center in the Gulf region. It hosts a mix of 375 diverse financial institutions, including 187 banks, of which 51 are wholesale banks (formerly referred to as off-shore banks or OBUs); 39 investment banks; and 25 commercial banks, of which 17 are foreign-owned. There are 31 representative offices of international banks. In addition there are 21 moneychangers and money brokers, and several other investment institutions, including 85 insurance companies. The vast network of Bahrain's conventional banking system—coupled with a vibrant Islamic banking sector—attracts a high volume of financial activity. With its strategic geographical location in the Middle East, close ties to neighboring Saudi Arabia, and as a transit point and communication hub along the Gulf into Southwest Asia, Bahrain may attract money laundering activities. It is thought that the greatest risk of money laundering stems from questionable foreign proceeds that transit Bahrain. Other sources of money laundering in Bahrain include hawala, trade fraud, real estate, and smuggling.

Bahrain criminalized money laundering in January 2001, with punishment of up to seven years in prison, and a fine of up to one million Bahraini dinars (approximately $2.65 million). If organized criminal affiliation, corruption, or disguise of the origin of proceeds is involved, the minimum penalty is a fine of at least 100,000 Bahraini dinars (approximately $265,000) and a prison term of not less than five years.

In August 2006, Bahrain passed Law 54/2006, which amended certain provisions of the 2001 anti-money laundering law to include banning and combating money laundering and terrorist financing. Law 54 criminalizes the undeclared transfer of money across international borders for the purpose of money laundering or supporting terrorism. Shortly after the passage of Law 54, Bahrain passed Law No. 58 of 2006 pertaining to the "Protection of the Community against Terrorist Acts." Under these laws, persons convicted of collecting or contributing funds, or otherwise providing financial support to a group or persons who practice terrorist acts, whether inside or outside Bahrain, will be subject to imprisonment for a minimum of ten years in prison up to a maximum of a life sentence. Notably, the AML law allows Bahrain to prosecute a money laundering violation regardless of whether the underlying act is a crime in Bahrain. For example, although there is no income tax system in Bahrain, someone engaging in illicit financial transactions for the purpose of evading another nation's tax system may be prosecuted for money laundering in Bahrain.

A controversial feature of the new law is a revised definition of terrorism that is based on the definition as set forth by the Organization of the Islamic Conference. Article 2 excludes from the definition of terrorism acts of struggle against invasion or foreign aggression, colonization, or foreign supremacy in the interest of freedom and the nation's liberty.

Under the original anti-money laundering law, the Bahrain Monetary Agency (BMA), the principal regulator of the financial sector, issued regulations requiring financial institutions to file suspicious transaction reports (STRs), to maintain records for a period of five years, and to provide ready access for law enforcement officials to account information. The current requirement for filing STRs stipulates no minimum thresholds. In 2005, the BMA established a secure online website, by which banks were enabled to file STRs. Immunity from criminal or civil action is given to those who report suspicious transactions. The law further provides for the confiscation of assets and allows for greater international cooperation.

In June 2001, the Policy Committee for the Prohibition and Combating of Money Laundering and Terrorist Financing was established, as an interagency committee to oversee and coordinate Bahrain's anti-money laundering efforts. The committee, which is under the chairmanship of the Deputy Governor of BMA, includes members from the Bahrain Stock Exchange, the Ministries of Finance and National Economy, Interior, Justice, Commerce, Social Development, and Foreign Affairs.

The Anti-Money Laundering Unit (AMLU) was established in 2002 as Bahrain's financial intelligence unit (FIU). The AMLU, which is housed in the Ministry of Interior, is empowered to receive reports of money laundering offenses as well as suspicious operations; conduct investigations; disseminate information to local law enforcement; share information with international counterparts; and execute decisions, orders, and decrees issued by the competent courts in offenses related to money laundering. The AMLU became a member of the Egmont Group of FIUs in July 2003.

The AMLU receives suspicious transaction reports (STRs) from banks and other financial institutions, investment houses, broker/dealers, moneychangers, insurance firms, real estate agents, gold dealers, financial intermediaries, and attorneys. Financial institutions file copies of the STRs with the BMA. Nonfinancial institutions are required under a Ministry of Industry and Commerce (MOIC) directive to also file STRs with that ministry. BMA analyzes the STRs, of which it receives copies, as part of its scrutiny of compliance by financial institutions with anti-money laundering and combating terrorist financing (AML/CFT) regulations. The BMA does not independently investigate the STRs, since responsibility for investigation rests with the AMLU. However, BMA may assist the AMLU with its investigations, particularly in cases where special banking expertise is required.

The BMA is the regulator for other nonbanking financial institutions including insurance companies, exchange houses, and capital markets. BMA inspected four insurance companies in 2005 and had conducted six more inspections by November 2006. More insurance industry inspections are

scheduled for 2007. Anti-money laundering regulations for investment firms and securities brokers were revised in April 2006.

In November 2003, the MOIC published new anti-money laundering guidelines, which govern designated nonfinancial businesses and professions (DNFBPs). The MOIC has also announced an increased focus on enforcement, noting some 300 visits to DNFBPs in 2005, including car dealers, jewelers, real estate agencies, etc. By November 2006, the MOIC had conducted an additional 274 enforcement follow-up visits. A total of 140 of these have been assigned an MOIC compliance officer as a result. The MOIC has also increased its inspection team staff from four to seven.

The MOIC system of requiring dual STR reporting to both it and the AMLU mirrors the BMA's system. Reportedly, good cooperation exists between MOIC, BMA, and AMLU, with all three agencies describing the double filing of STRs as a backup system. The AMLU and BMA's compliance staff analyze the STRs and work together on identifying weaknesses or criminal activity, but it is the AMLU that must conduct the actual investigation and forward cases of money laundering and terrorist financing to the Office of Public Prosecutor. From January through November 2006, the AMLU has received and investigated 118 STRs, 26 of which have been forwarded to the Office of Public Prosecutor for prosecution. The GOB completed its first successful money laundering prosecutions in May 2006. The prosecutions resulted in two convictions with sentences of one and three years and fines of $380 and $1,900 respectively.

Bahrain is moving ahead with plans to establish a special court to try financial crimes. The court is expected to begin hearing cases in May 2007, and Bahraini judges are undergoing special training to handle such cases.

There are 51 BMA licensed wholesale Banks, which formerly were referred to as offshore banking units (OBUs) that are branches of international commercial banks. Such new licenses allow wholesale banks to accept deposits from citizens and residents of Bahrain, and undertake transactions in Bahraini dinars. Wholesale banks are regulated and supervised in the same way as the domestic banking sector, and are subject to the same regulations, on-site examination procedures, and external audit and regulatory reporting obligations.

Bahrain's Commercial Companies Law (Legislative Decree 21 of 2001) does not permit the registration of offshore companies or international business companies (IBCs). All companies must be resident and maintain their headquarters and operations in Bahrain.

In January 2002, the BMA issued circular BC/1/2002, which implemented the Financial Action Task Force (FATF) Nine Special Recommendations on Terrorist Financing as part of the Central Bank's AML regulations. Subsequently, the BMA froze two accounts that had been designated by the UNSCR 1267 Sanctions Committee, and one account that was listed under U.S. Executive Order 13224.

Circular BC/1/2002 also states that money changers may not transfer funds for customers in another country by any means other than Bahrain's banking system. In addition, all Central Bank licensees are required to include details of the originator's information with all outbound transfers. With respect to incoming transfers, licensees are required to maintain records of all originator information and to carefully scrutinize inward transfers that do not contain the originator's information, as they are presumed to be suspicious transactions. Licensees are required to file suspicious transaction reports (STRs) if they suspect that the funds being transferred are linked to suspicious activities or terrorist financing. Licensees must also maintain records of the identity of their customers in accordance with the Central Bank's anti-money laundering regulations, as well as the exact amount of transfers. During 2004, the BMA consulted with the industry on changes to its existing AML/CFT regulations, to reflect revisions by the FATF to its Forty Recommendations plus Nine Special Recommendations. Revised

and updated BMA regulations were issued in mid- 2005. The BMA is drafting new regulations to be issued in 2007 intended to enhance existing circulars regarding requirements for money changers.

Legislative Decree No. 21 of 1989 governs the licensing of nonprofit organizations. The Ministry of Social Development (MSD) is responsible for licensing and supervising charitable organizations in Bahrain. In February 2004, as part of its efforts to strengthen the regulatory environment and fight potential terrorist financing, MSD issued a Ministerial Order regulating the collection of donated funds through charities and their eventual distribution, to help confirm the charities' humanitarian objectives. The regulations are aimed at tracking money that is entering and leaving the country. These regulations require organizations to keep records of sources and uses of financial resources, organizational structure, and membership. Charitable societies are also required to deposit their funds with banks located in Bahrain and may have only one account in one bank. The MSD has the right to inspect records of the societies to insure their compliance with the laws. Banks must report to BMA any transaction by a charitable institution that exceeds 3,000 Bahraini dinars (approximately $8,000). MSD has the right to inspect records of the societies to insure their compliance with the law.

Bahrain is a leading Islamic finance center in the region. The sector has grown considerably since the licensing of the first Islamic bank in 1979. Bahrain has 32 Islamic banks and financial institutions. Given the large share of such institutions in Bahrain's banking community, the BMA has developed a framework for regulating and supervising the Islamic banking sector, applying regulations and supervision as it does with respect to conventional banks. In March 2002, the BMA introduced a comprehensive set of regulations for Islamic banks called the Prudential Information and Regulatory Framework for Islamic Banks (PIRI). The framework was designed to monitor certain banking aspects, such as capital requirements, governance, control systems, and regulatory reporting.

In November 2004, Bahrain hosted the inaugural meeting of the Middle East and North Africa Financial Action Task Force (MENAFATF). Bahrain also serves as the headquarters for the MENAFATF Secretariat.

In October 2006, the Policy Committee for the Prohibition and Combating of Money Laundering and Terrorist Financing announced the formation of two new sub-committees: the U.N. Sub-Committee, which will head a new inter-agency framework for disseminating and reviewing international financial crimes designations; and the Legal Sub-Committee, which will coordinate the drafting of any future financial crimes legislation.

Bahrain is a party to the 1988 UN Drug Convention, the UN Convention on Transnational Organized Crime, and the UN Convention for the Suppression of the Financing of Terrorism. Bahrain has signed, but has not yet ratified, the UN Convention against Corruption.

The Government of Bahrain has demonstrated a commitment to establish a strong anti-money laundering and terrorist financing system and appears determined to engage its large financial sector in this effort. The Anti-Money Laundering Unit should maintain its efforts to obtain and solidify the necessary expertise in tracking suspicious transactions. However, there should not be an over-reliance on suspicious transaction reporting. Bahraini law enforcement and customs authorities should take a more active role in recognizing, initiating and pursuing investigations in anti-money laundering and counterterrorist financing cases. The Ministry of Social Development should expand and provide training for its staff with NGO/charities oversight responsibilities. Bahrain should become a party to the UN Convention against Corruption.

## Bangladesh

Bangladesh is not an important regional or offshore financial center.

While there is evidence of funds laundered through the official banking system, there is no indication of large-scale abuse. Money transfers outside the formal banking and foreign exchange licensing system are illegal. The principal money laundering vulnerability remains the widespread use of the underground hawala or "hundi" system to transfer money and value outside the formal banking network. The vast majority of hundi transactions in Bangladesh are used to repatriate wages from Bangladeshi workers abroad.

The Central Bank has reported a considerable increase in remittances since 2002 through official channels. The figure has more than doubled from $2 billion to the current level of $4.3 billion in fiscal year 2006 (July 1-June 30). The increase is due to competition from the government and commercial banks through improved delivery time and valued-added services, such as group life insurance. Hundi, however, will probably never be completely eradicated as it is used to avoid taxes, customs duties and currency controls. The nonconvertibility of the local currency (the taka) coupled with intense scrutiny on foreign currency transactions in formal financial institutions also contribute to the popularity of both hundi and black market money exchanges.

In Bangladesh, hundi primarily uses trade goods to provide counter valuation or a method of balancing the books in transactions. It is part of trade-based money laundering and a compensation mechanism for the significant amount of goods smuggled into Bangladesh. An estimated $1 billion dollars worth of dutiable goods are smuggled every year from India into Bangladesh. A comparatively small amount of goods are smuggled out of the country into India. Instead, hard currency and other assets flow out of Bangladesh to support the smuggling networks.

Corruption is a major area of concern in Bangladesh. For the past five years (2001-2005) Bangladesh has been ranked by Transparency International's Corruption Perception Index as the country with the highest level of perceived corruption in the world. In 2006, Bangladesh was ranked 156 out of 163 countries surveyed.

Bangladeshis are not allowed to carry cash outside of the country in excess of 3,000 taka (approximately $50). There is no limit as to how much currency can be brought into the country, but amounts over $5,000 must be declared. Customs is primarily a revenue collection agency, accounting for 40-50 percent of annual Bangladesh government income.

Since 2004, the Central Bank has conducted training for commercial banks' headquarters around the county in "know your customer" practices. Since Bangladesh does not have a national identity card and because the vast majority of Bangladeshis do not have a passport, there are difficulties in enforcing customer identification requirements. In most cases, banking records are maintained manually with little support technology, although this is slowly changing, especially in head offices. Accounting procedures used by the Central Bank may not achieve international standards in every respect. In 2004, the Central Bank issued "Guidance Notes on Prevention of Money Laundering" and designated anti-money laundering compliance programs as a "core risk" subject to the annual bank supervision process of the Central Bank. Banks are required to have an anti-money laundering compliance unit in their head office and a designated anti-money laundering compliance officer in each bank branch. The Central Bank conducts regular training programs for compliance officers based on the Guidance Notes. In December 2005, the Central Bank called all compliance officers to Dhaka for a discussion about their obligations and heightened police interest in money laundering and terrorist financing. During 2006, the Central Bank continued to work with compliance officers around the country, sending their instructors to regional workshops.

Currently, Bangladesh is working to formalize operations for a Financial Intelligence Unit (FIU). Under the 2002 Money Laundering Prevention Act (MLPA), the Anti-Money Laundering Unit (AMLU) of the Central Bank acts as a de facto FIU and has authority to freeze assets without a court order and seize them with a court order. The Central Bank has approved the purchase of hardware for

the nascent FIU, which will be coupled with link analysis software provided by the U.S. Department of Justice.

The Central Bank has received approximately 236 suspicious transaction reports since the MLPA was enacted in 2002. To date, there have been no successful prosecutions in part due to procedural problems in adjusting to inter-agency cooperation. A major setback occurred in December 2005 when the newly created Anti-Corruption Commission (ACC) advised the bank that it would not investigate these cases and returned them. The Criminal Investigation Division of the country's police force agreed to take the cases. During 2006, the bank and police hammered out a procedure to investigate cases initiated by the bank through suspicious transactions reports. With the approval of the Law Minister, dedicated government attorneys will handle the prosecutions. Officials expect prosecutions to begin in spring 2007.

The Anti-Money Laundering and Terrorist Financing Act 2005 (AMLTF), drafted to replace the MLPA from 2002, was shelved due to political issues related to upcoming national elections expected in January 2007. The draft AMLTF provided powers required for a FIU to meet most of the international recommendations set forth by the Egmont Group, including sharing information with law enforcement at home and abroad. The draft legislation also provided for the establishment of a Financial Investigation and Prosecution Office wherein law enforcement investigators and prosecutors would work as a team from the beginning of the case to trial. The 2005 draft legislation addressed asset forfeiture and provided that assets, substitute assets (without proving the relation to the crime) and instrumentalities of the crime can be forfeited. It did not, however, address the nuts and bolts of asset forfeiture, which the Central Bank asserts can be addressed administratively and via regulatory procedures. Changes following cabinet review weakened the draft by, for example, deleting provisions for the establishment of an enforcement group that would be comprised of Central Bank analysts, police and prosecutors.

The AML draft also criminalized terrorism financing. The government announced that it wanted a separate Anti-Terrorism law that would criminalize terrorist financing, stipulating that the Anti-Terrorism Act (ATA) would have to be passed before the AML. The ATA law was not sent to Parliament in 2006. A worrying development in the initial review stage of the ATA was the removal of the section providing for international cooperation.

In 2003, Bangladesh froze a nominal sum in an account of a designated entity on the UNSCR 1267 Sanctions Committee's consolidated list and identified an empty account of another entity. In 2004, following investigation of the accounts of an entity listed on the UNSCR 1267 consolidated list, the Central Bank fined two local banks for failure to comply with Central Bank regulatory directives. In 2005, the GOB became a party to the UN International Convention for the Suppression of the Financing of Terrorism and is now a party to twelve UN Conventions and protocols on Terrorism. The GOB is a party to the 1988 UN Drug Convention but is not a signatory to the Convention against Transnational Organized Crime. Bangladesh is a member of the Asia/Pacific Group on Money Laundering.

Despite some advancement, the Government of Bangladesh's anti-money laundering/terrorist financing regimes should be strengthened to comply with international standards. Bangladesh should criminalize terrorist finance. Legislation should provide for safe harbor provisions in order to protect reporting individuals, due diligence programs, and banker negligence accountability that would make individual bankers responsible under certain circumstances if their institutions launder money. Bangladesh should create a financial intelligence collection system and establish a viable Financial Intelligence Unit to analyze the intelligence. A lack of training, resources and computer technology, including computer links with the outlying districts, continue to hinder progress. Bangladesh law enforcement and customs should examine forms of trade-based money laundering. Bangladesh should further efforts to combat pervasive corruption, which is intertwined with money laundering,

smuggling, and tax evasion. Bangladesh should ratify the UN Convention against Transnational Organized Crime.

## Barbados

A transit country for illicit narcotics, Barbados remains attractive for money laundering, which primarily occurs through the formal banking system. There is also evidence of proceeds being directed to financial institutions in Barbados by criminals abroad.

As of July 30, 2006, there were six commercial banks and 14 nonbank financial institutions in Barbados. The offshore sector consists of 54 offshore banks, 4,635 international business companies (IBCs), 178 exempt insurance companies (a significant reduction from 2005), 57 qualified exempt insurance companies, nine mutual funds companies, one exempt mutual fund company, seven trust companies, and six finance companies. According to the Central Bank, it is estimated that there is approximately $32 billion worth of assets in Barbados's offshore banks. There are no free trade zones, casinos, or internet gaming sites in Barbados.

The Central Bank regulates and supervises both on and offshore banks, trust companies, and finance companies. The Ministry of Finance issues banking licenses after the Central Bank receives and reviews applications, and recommends applicants for licensing. The International Financial Services Act 2002 incorporates fully the standards established in the Basel Committee's Core Principles for Effective Banking Supervision and provides for on-site examinations of offshore banks. On-site examinations of licensees use a comprehensive methodology that seeks to assess the level of compliance with legislation and guidelines. Offshore banks must submit quarterly statements of assets and liabilities and annual balance sheets to the Central Bank. Additionally, the Central Bank conducts off-site surveillance, which consists of reviewing financial data as well as other documents submitted by financial institutions. The Central Bank revised its Anti-Money Laundering Guidelines in 2001. The revised "know your customer" guidelines provide detailed guidance to financial institutions regulated by the Central Bank.

The International Business Companies Act (1992) provides for general administration of IBCs. The Ministry of Industry and International Business vets and grants licenses to IBCs after applicants register with the Registrar of Corporate Affairs. Bearer shares are not permitted, and financial statements of IBCs are audited if total assets exceed $500,000. To enhance due diligence efforts, the 2001 International Business (Miscellaneous Provisions) Act requires more information than was previously provided for IBC license applications or renewals.

The Government of Barbados (GOB) criminalized drug money laundering in 1990 through the Proceeds of Crime Act. The Act authorizes asset confiscation and forfeiture, permits suspicious transaction disclosures to the Director of Public Prosecutions, and exempts such disclosures from civil or criminal liability. The Money Laundering (Prevention and Control) Act 1998 (MLPCA) extends the offense of money laundering beyond drug-related crimes, and criminalizes the laundering of illicit proceeds from unlawful activities that are punishable by at least one year's imprisonment. Under the MLPCA, money laundering is punishable by a maximum of 25 years in prison and a maximum fine of $1 million. The MLPCA applies to a wide range of financial institutions, including domestic and offshore banks, IBCs, and insurance companies. In 2001, the MLPCA was amended to extend to other financial institutions, including money remitters, investment services, and any other services of a financial nature. These institutions are required to identify their customers, cooperate with domestic law enforcement investigations, report and maintain records of all transactions exceeding $5,000 for a period of five years, and establish internal auditing and compliance procedures.

The Anti-Money Laundering Authority (AMLA) was created to supervise financial institutions' compliance with the MLPCA. Financial institutions must also report suspicious transactions to the

AMLA through the Barbados Financial Intelligence Unit (FIU). There are no laws that prevent disclosure of information to relevant authorities, and individuals reporting to the FIU are protected by law. The AMLA is also responsible for issuing anti-money laundering training requirements and regulations for financial institutions. However, staff constraints limit the direct supervisory capacity of the AMLA.

The FIU is housed in the Office of the Attorney General within the AMLA. The FIU was established in September 2000 and is fully operational as an independent agency. From January 1-June 30, 2006, the FIU received 41 suspicious activity reports (SARs)—half of the amount received the previous year—and referred two cases to the Commissioner of Police. The FIU reports that though there has been a decrease in SARs, the quality of SARs received has improved. The FIU forwards information to the Financial Crimes Investigation Unit of the police if it has reasonable grounds to suspect money laundering. Government entities and financial institutions are required to provide additional information to the FIU upon request by the FIU Director. The FIU also has the ability to negotiate memoranda of understanding (MOUs) with foreign counterparts.

The MLPCA only provides for criminal asset seizure and forfeiture, not civil forfeiture. In November 2001, the GOB amended its financial crimes legislation to shift the burden of proof to the accused to demonstrate that property in his or her possession or control is derived from a legitimate source. Absent such proof, the presumption is that such property was derived from the proceeds of crime. The law also enhances the GOB's ability to freeze bank accounts and to prohibit transactions from suspect accounts. Legitimate businesses and other financial institutions are subject to criminal sanctions and the termination of operating licenses. Tracing, seizing and freezing assets may be done by the FIU and the police. Freezing orders are usually granted for six months at a time after which they need to be reviewed. Frozen assets may be confiscated on application by the Director of Public Prosecutions and are paid into the National Consolidated Fund. No asset sharing law has been enacted, but bilateral treaties as well as the Mutual Assistance in Criminal Matters Act, have provisions for asset tracing, freezing and seizure between countries.

The Barbados Anti-Terrorism Act 2002, as well as provisions of the Money Laundering Financing of Terrorism (Prevention and Control) Act (MLFTA), criminalize the financing of terrorism. The MLFTA has a provision for information sharing between the Barbados Customs Department and the FIU, and is also designed to control bulk cash smuggling and the use of cash couriers. The GOB circulates the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States. To date, the GOB has found no evidence of terrorist financing. The GOB has not taken any specific initiatives focused on alternative remittance systems or the misuse of charitable and nonprofit entities.

Barbados has bilateral tax treaties that eliminate or reduce double taxation with fourteen countries including the United States. The United States and the GOB ratified amendments to their bilateral tax treaty in 2004. A mutual legal assistance treaty (MLAT) and an extradition treaty between the United States and the GOB each entered into force in 2000.

Barbados is a member of the Caribbean Financial Action Task Force (CFATF) and underwent a Mutual Evaluation in December 2006. Barbados is also a member of the Offshore Group of Banking Supervisors, the Caribbean Regional Compliance Association, and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The FIU was admitted to the Egmont Group in 2002. Barbados is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The GOB has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the Inter-American Convention against Terrorism.

Although the GOB has strengthened the anti-money laundering legislation, it must steadfastly enforce the laws and regulations it has adopted. The GOB should adopt civil forfeiture and asset sharing legislation. Barbados should be more aggressive in conducting examinations of the financial sector and maintaining strict control over vetting and licensing of offshore entities. The GOB should ensure adequate supervision of nongovernmental organizations and charities. It should also work to improve information sharing between regulatory and enforcement agencies. In addition, Barbados should continue to provide adequate resources to its law enforcement and prosecutorial personnel, to ensure Mutual Legal Assistance Treaty requests are efficiently processed.

## Belarus

Belarus is not a regional financial center. A general lack of transparency in industry and banking sectors makes it difficult to assess the level of or potential for money laundering and other financial crimes, but Belarus has many vulnerabilities, including organized crime. Due to inflation, excessively high taxes, underground markets, and the dollarization of the economy, a significant volume of foreign-currency cash transactions eludes the banking system. Shadow incomes from offshore companies, filtered through small local businesses, constitute a significant portion of foreign investment. Smuggling is prevalent. Corruption is a severe problem in Belarus, which exacerbates financial crimes enforcement and retards needed reforms.

Economic decision-making in Belarus is highly concentrated within the top levels of government and has become even more so after the President issued Decree 520 "On Improving Legal Regulation of Certain Economic Relations" in November 2005. This decree gives the president broader powers over the entire economy-including the power to manage, dispose of, and privatize all state-owned property-while taking away authority from Parliament, the National Bank of the Republic of Belarus (NBRB), and even market forces. Under the decree, legislation that contradicted the decree became void in June. On January 28, 2006 the President issued a decree granting him powers to confiscate at will any plot of land for agricultural, environmental, recreational, historical, and cultural uses. The President subsequently relinquished some of his nominal power in June by abolishing for banks the "golden share" rule that permits the government to interfere in the decision-making of any company formerly owned by the government. Moreover, the President canceled a requirement that foreign capital must account for 25 percent of the total authorized capital stock of the country's banks. However, the government imposed penalties on 107 government-owned enterprises that failed to transfer accounts from private banks to government-owned financial institutions per a 2005 presidential directive.

Since the President issued decree 114 "On free economic zones on the territory of the Republic of Belarus" in 1996, Belarus has established six free economic zones (FEZs). The president creates FEZs upon the recommendation of the Council of Ministers and can dissolve or extend the existence of a FEZ at will. The Presidential Administration, the State Control Committee (SCC), and regional and Minsk city authorities supervise the activities of companies in the FEZs. According to the SCC, applying organizations are fully vetted before they are allowed to operate in an FEZ in an effort to prevent money laundering and terrorism finance. On January 31, 2006, President Lukashenko signed degree 66, which tightened FEZ regulations on transaction reporting and security, including mandatory video surveillance systems.

Belarus' "Law on Measures to Prevent the Laundering of Illegally Acquired Proceeds" (AML Law) was amended in 2005. It establishes the legal and organization framework to prevent money laundering and terrorism financing. The measures described in the AML Law apply to all entities that conduct financial transactions in Belarus. Such entities include: bank and nonbank credit and financial institutions; stock and currency exchanges; investment funds and other professional dealers in securities; insurance and reinsurance institutions; dealers' and brokers' offices; notary offices (notaries); casinos and other gambling establishments; pawn shops; leasing and estate agents; post

offices; dealers in precious stones and metals; attorneys conducting financial transactions on behalf of clients; and other organizations conducting financial transactions.

The AML Law makes individuals and businesses, government entities, and entities without legal status criminally liable for drug and nondrug related money laundering, although the punishments for laundering money or financing terrorism are not explicitly stated in the law. However, Article 235 of the Belarusian criminal code ("legalization of illegally acquired proceeds") stipulates that money laundering crimes may be punishable by fine or prison terms of up to ten years. The law defines "illegally acquired proceeds" as money (Belarusian or foreign currency), securities or other assets, including property rights and exclusive rights to intellectual property, obtained in violation of the law. The NBRB has issued suggested anti-money laundering and counterterrorist financing (AML/CFT) regulations, including know your customer (KYC) and due diligence requirements. Although these are not legally binding, they are treated as mandatory by the institutions overseen by the NBRB.

The AML Law authorizes the following government bodies to monitor financial transactions for the purpose of preventing money laundering: the State Control Committee (Department of Financial Monitoring, or DFM); the Securities Committee; the Ministry of Finance; the Ministry of Justice; the Ministry of Communications and Information; the Ministry of Sports and Tourism; the Committee on Land Resources; the Ministry on Taxes and Duties (MTD); and other state bodies. The MTD also provides oversight and has released binding regulations on its subject institutions.

On March 17, 2006 a series of amendments to the AML Law passed by parliament in December 2005 to enhance money laundering prevention came into effect. Under the new law, individual and corporate financial transactions exceeding approximately $27,000 and $270,000, respectively, are subject to special inspection. Banks that violate the new law face fines of up to one percent of their registered capital and suspension of their licenses for up to one year. However, this is a threshold reporting requirement. A 2005 International Monetary Fund (IMF) Financial System Stability Assessment pointed out that the AML/CFT framework, including that of suspicious transaction reporting, needed to be significantly upgraded to meet FATF standards. Additionally, the new law exempts most government transactions and transactions sanctioned by the President from extraordinary inspection. Moreover, the government used the anti-money law as a pretext for preventing several pro-democracy NGOs from receiving foreign assistance.

In January 2005, the President signed a decree on the regulation of the gaming sector, making the owners of gambling businesses subject to stricter tax regulations. In addition, a provision intended to combat money laundering requires those participating in gaming activities to produce identification in order to receive a monetary winnings.

On February 9, 2006, the government abolished 1997 identification requirements for all foreign currency exchange transactions at banks. The Belarusian banking sector consists of 31 banks. Of these, 27 have foreign investors and nine banks are foreign owned. As of May 1, 2006 the capital base of Belarus' banks totaled almost $10 billion. The state-owned Belarus Bank is the largest and most influential bank in Belarus. In 2005, Belarus Bank conducted $2.7 million dollars in financial transactions with Russian clients, 28 percent more than 2004. In April, Russia's Burbank opened a $2 million credit line to Belarus Bank for trade finance on an unsecured basis. By 2006, total credit lines to Belarus Bank from foreign financial institutions amounted to $220 million. Four other state banks and one private bank comprise the majority of the remaining banking activities in the country. In addition, 12 foreign banks have representative offices in Belarus in order to facilitate business cooperation with their Belarusian clients.

In 2003, Belarus established the Department of Financial Monitoring (DFM)-the Belarusian equivalent of a Financial Intelligence Unit-within the State Control Committee and named the DFM as the primary government agency responsible for gathering, monitoring and disseminating financial intelligence. The DFM analyzes information it receives for evidence of money laundering to pass to

law enforcement officials for prosecution. The DFM also has the power to penalize those who violate money laundering laws. In April 2006, President Lukashenko signed ordinance 259, which granted the DFM the power to suspend the financial operations of any company suspected of money laundering or financing terrorism.

The DFM cooperates with its counterparts in foreign states and with international organizations to combat money laundering. In 2005, the DFM fielded 19 inquiries from other FIUs, and requested information 34 times from other FIUs. The DFM is not a member of the Egmont Group, but it has applied for membership. The DFM's counterpart FIUs from Russia and Poland are the DFM's sponsors for Egmont membership.

Financial institutions are obligated to report to the DFM transactions subject to special monitoring, including: transactions whose suspected purpose is money laundering or terrorism financing; cases where the person performing the transaction is a known terrorist or controlled by a known terrorist; cases in which the person performing the transaction is from a state that does not cooperate internationally to prevent money laundering and terrorism financing; and finally, transactions exceeding approximately $27,000 for individuals and $270,000 for businesses that involve cash, property, securities, loans or remittances. Belarusian law stipulates that a one-time transaction that exceeds predetermined amounts for individuals and businesses set by the government must be reported in accordance with the law. If the total value of transactions conducted in one month exceeds the set thresholds and there is reasonable evidence to suggest that the transactions are related, then all the transaction activity must be registered.

Financial institutions conducting transfers subject to special monitoring are required to submit information about such transfers in written form to the DFM within one business day of the reported transaction. Financial institutions should identify the individuals and businesses ordering the transaction or the person on whose behalf the transaction is being placed, disclose information about the beneficiary of a transaction, and provide the account information and document details used in the transaction, including the type of transaction, the name and location of the financial institution conducting the transfer, and the date, time and value of the transfer. The law provides a "safe harbor" for banks and other financial institutions that provide otherwise confidential transaction data to investigating authorities, provided the information is given in accordance with the procedures established by law. Under the State Control Committee (SCC), the Department of Financial Investigations, in conjunction with the Prosecutor General's Office, has the legal authority to investigate suspicious financial transactions and examine the internal rules and enforcement mechanisms of any financial institution. The DFM also has the authority to initiate its own investigations.

Failure to report and transmit the required information on financial transactions may subject a bank or other financial institution to criminal liability. The National Bank of the Republic of Belarus is the relevant monitoring agency for the majority of transactions conducted by banking and other financial institutions. According to the National Bank, information on suspicious transactions should be reported to the Bank's Department of Bank Monitoring. Although the banking code stipulates that the National Bank has primary regulatory authority over the banking sector, in practice, the Presidential Administration exerts significant influence on central and state commercial bank operations, including employment. Any member of the Board of the National Bank may be removed from office by the president with a simple notification to the National Assembly.

Terrorism is a crime in Belarus. The AML Law establishes measures to prevent terrorism finance. Belarus' law on counterterrorism also states that knowingly financing or otherwise assisting a terrorist group constitutes terrorist activity. Under the Belarusian Criminal Code, the willful provision or collection of funds in support of terrorism by nationals of Belarus or persons in its territory constitutes participation in the act of terrorism itself in the form of aiding and abetting. In December 2005, the

Belarusian Parliament amended the Criminal Code to stiffen the penalty for the financing of terrorism and thus bring Belarusian regulations into compliance with the International Convention for the Suppression of the Financing of Terrorism. The amendments explicitly define terrorist activities and terrorism finance and carry an eight to twelve year prison sentence for those found guilty of sponsoring terrorism. In February 2006, the Interior Ministry announced the establishment of a new counterterrorism department within its Main Office against Organized Crime and Corruption.

Belarusian legislation provides for broad seizure powers and for law enforcement to identify and trace assets. Seizure based on a criminal conviction is in the Criminal Code for all serious offenses, including money laundering. Seizure of assets from third parties appears to be possible but is not specifically codified. The seizure of funds or assets held in a bank requires a court decision, a decree issued by a body of inquiry or pre-trial investigation, or a decision by the tax authorities. A 2002 directive issued by the Board of Governors of the National Bank prohibits all transactions with accounts belonging to terrorists, terrorist organizations and associated persons. This directive also outlines a process for circulating to banks the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list. The National Bank is required to disseminate to banks the updates to the consolidated list and other information related to terrorist finance as it is received from the Ministry of Foreign Affairs. The directive gives banks the authority to freeze transactions in the accounts of terrorists, terrorist organizations and associated persons. Through 2006, Belarus has not identified any assets as belonging to individuals or entities included on the UNSCR 1267 Sanctions Committee's consolidated list.

Domestically, Belarus has made an effort to ensure cooperation and coordination between state bodies through the Interdepartmental Working Group; this Group has been established specifically to address these AML/CFT issues. This Working Group includes representatives of the Prosecutor's office, the National Bank, MTD, State Security Committee, Department of Financial Investigation, and the DFM. The Director of the DFM serves as the head of this Group.

Belarus has signed bilateral treaties on law enforcement cooperation with Bulgaria, India, Lithuania, the People's Republic of China, Poland, Romania, Turkey, the United Kingdom, and Vietnam. In September, 2006 Belarus signed an anti-money laundering agreement with the People's Bank of China. Belarus is also a party to five agreements on law enforcement cooperation and information sharing among CIS member states, including the Agreement on Cooperation among CIS Member States in the Fight against Crime and the Agreement on Cooperation among Ministries of Internal Affairs in the Fight against Terrorism. In 2004, Belarus joined the newly organized Eurasian Regional Group (EAG) Against Money Laundering and the Financing of Terrorism, a FATF-style regional body. The EAG has observer status in FATF. Belarus has also assumed international commitments to combat terrorism as a member of the Collective Security Treaty Organization (CSTO), which includes Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan.

Belarus is a party to the UN International Convention for the Suppression of the Financing of Terrorism. However, over the past year, Belarus has significantly expanded its economic relations with state sponsors of terrorism. In May, 2006 President Lukashenko hosted senior officials of Syria's governing Baath Party and signed several economic cooperation agreements. In October, following Foreign Minister Sergey Martynov's visit to Tehran, Belarus and Iran began formal negotiations to open Iranian banks in Minsk. In November, 2006, President Lukashenko visited Iran.

Belarus is a party to the 1988 UN Drug Convention and to the UN Convention against Transnational Organized Crime. On September 15, 2005, Belarus became a signatory to the UN International Convention for the Suppression of Acts of Nuclear Terrorism.

Belarus is a party to the UN Convention against Corruption. The lower house of Parliament ratified a bill for the Civil Law Convention on Corruption in December 2005. The bill aims to protect those who suffer from acts of corruption and makes the state or appropriate authority liable to compensate

individuals affected by a corrupt official, as well as invalidating all scandalous contract agreements. On January 31, the Belarusian State Customs Committee unveiled an anticorruption plan that included stiffer penalties for bribery and closer cooperation with law enforcement authorities. On July 20, 2006 President Lukashenko signed an anticorruption law to comply with the Council of Europe's 1999 Criminal Law Convention on Corruption, which Belarus ratified in 2004. The law expanded Belarus' existing anticorruption legislation by defining professions and individuals vulnerable to and capable of corruption to include senior government officials; members of parliament and local councils; presidential, parliamentary, and local council candidates; foreign officials; officials of private organizations that perform administrative and control functions; and volunteers assisting law enforcement agencies in maintaining public order. However, corruption remains a serious obstacle to enforcing laws dealing with financial crimes. Belarus is 151 out of 163 countries listed in Transparency International's 2006 International Corruption Perception Index.

The Government of Belarus (GOB) has taken steps to construct an anti-money laundering and counterterrorist financing regime. Belarus should increase the transparency of its business and banking sectors. It should extend the application of its current anti-money laundering legislation to cover more of the governmental transactions that are currently exempted under the law, and ensure that the regulations and guidance provided are legally binding. The GOB should implement strict regulation of its offshore industries and those operating within the FEZ areas. The GOB needs to reinstate the identification requirement for foreign currency exchange transactions. It should hone its guidance and enforcement of suspicious transaction reporting and provide adequate resources to its FIU so that it can operate effectively. The GOB must work to further improve the coordination between agencies responsible for enforcing anti-money laundering measures. The GOB also needs to take steps to ensure that the anti-money laundering framework that does exist is used in a manner consistent with the reason for which it was implemented, rather than using it in a political manner. The GOB should take serious steps to combat corruption in commerce and government.

## Belgium

The banking industry of Belgium is of medium size, with assets of over $1.9 trillion dollars in 2005. Strong legislative and oversight provisions are in place in the formal financial sector to combat money laundering and terrorist financing. Belgian officials have noted that criminals are increasing their use of the nonfinancial professions to facilitate access to the official financial sector.

Belgium criminalized money laundering through the Law of 11 January 1993, On Preventing Use of the Financial System for Purposes of Money Laundering. This law outlined the customer due diligence and reporting requirements. These are applicable to nonfinancial business and professions as well. Obligated entities include estate agents, private security firms, funds transporters, diamond merchants, notaries, bailiffs, auditors, chartered accountants, tax advisors, certified accountants, and casinos, when customers seek to execute a financial transaction in connection with their gambling. Additional laws made the requirements applicable to other sectors as well: the Law of 22 March 1993, On the Legal Status and Supervision of Credit Institutions; and the Law of 6 April 1995, On Secondary Markets, On Legal Status and Supervision of Investment Firms, On Intermediaries and Investment Advisors. Article 505 of the Penal Code sets penalties of up to five years of imprisonment for money laundering convictions. Any unlawful activity may serve as the predicate offense.

The Law of 12 January 2004 amended Belgian domestic legislation by making it applicable to attorneys, and implementing the Second European Union (EU) Directive on Money Laundering, or Council Directive 2001/97/EC On Prevention of the Use of the Financial System for Money Laundering, which broadened the scope of money laundering predicate offenses beyond drug trafficking to include the financing of terrorist acts or organizations. This Law was challenged by the Belgian bar association and taken to the Court of Arbitration, which referred the challenge to the

European Court of Justice. The bar has argued that the Second EU Directive violates the right to a fair trial by the obligated attorneys, because the reporting obligations prejudice the lawyers against fully and independently representing their clients.

In June 2005 Belgium underwent a mutual evaluation by the Financial Action Task Force (FATF). Although the report concluded that Belgium's anti-money laundering and counterterrorism financing (AML/CFT) regime is effective, the assessment team found it partially compliant or noncompliant in certain areas. These areas include: due diligence and regulation requirements for designated nonfinancial businesses and professions, licensing or registration of businesses providing money or value transfer services, allocation of adequate resources to the authorities charged with combating financial crimes, elimination of bearer bonds, development of an independent authority to freeze assets, and implementation of a system to monitor cross-border currency movements. Belgium is currently working to address these deficiencies. In 2007 Belgium must report back to FATF regarding its progress in implementing these recommendations.

A growing problem, according to government officials, is the proliferation of illegal underground banking activities. Beginning in 2004, Belgian police made a series of raids on "phone shops"-small businesses where customers can make inexpensive phone calls and access the Internet. In some phone shops, authorities uncovered money laundering operations and hawala-type banking activities. In 2006 further raids uncovered numerous counterfeit phone cards and illegal or undocumented workers in addition to evidence of money laundering activities in some locations. Since 2004, more than 130 such shops have been closed by Belgian authorities, who estimate that the Belgian state may be deprived of up to $256 million in lost tax revenue each year through tax evasion by these businesses. Authorities report that phone shops often declare bankruptcy and later reopen under new management, making it difficult for officials to trace ownership and collect tax revenues. Authorities believe that 3,000- 5,000 phone shops may be operating in Belgium. Only an estimated one-quarter of these shops are formally licensed, and Belgian authorities are considering enforcing a stricter licensing regime. Some Brussels communes have also proposed heavy taxes on these types of shops in an effort to dissuade illegitimate commerce.

Belgium's robust diamond industry presents special challenges for law enforcement. Despite some diffusion in recent years, Belgium continues to be the world's diamond-trading center. Fully 90 percent of the world's crude diamonds and 50 percent of cut diamonds pass through Belgium. Most of the "blood" or "conflict diamonds" from long-running African civil wars were processed in Antwerp. Authorities have transmitted a number of cases relating to diamonds to the public prosecutor, and they are examining the sector closely in cooperation with local police and diamond industry officials. Additionally, the Kimberley certification process (a joint government, international diamond industry, and civil society initiative designed to stem the flow of illicit diamonds) has introduced much-needed transparency into the global diamond trade. However, diamonds of questionable origin continue to appear on the Belgium market. The Government of Belgium (GOB) recognizes the particular importance of the diamond industry, as well as the potential vulnerabilities it presents to the financial sector. The GOB has distributed typologies outlining its experiences in pursuing money laundering cases involving the diamond trade, especially those involving the trafficking of African conflict diamonds.

For the purposes of money laundering and terrorist financing, Belgian financial institutions are supervised by the Belgian Banking and Finance Commission (CBFA), which also supervises exchange houses, stock brokerages, and insurance companies. The Belgian Gaming Commission oversees casinos. Belgian law mandates reporting of suspicious transactions by a wide variety of financial institutions and nonfinancial entities, including notaries, accountants, bailiffs, real estate agents, casinos, cash transporters, external tax consultants, certified accountant-tax experts, and lawyers. Lawyers in particular do not consistently comply with reporting requirements. Belgian lawyers, for example, did not report any suspicious transactions to the FIU in 2005. An association of Belgian

lawyers has appealed the law to Belgium's court of arbitration on the grounds that it violates basic principles of the independence of the lawyer and of professional secrecy. As of October 2006, a decision from the court of arbitration was still pending.

Belgian financial institutions are required to comply with "know your customer" principles, regardless of the transaction amount. Institutions must maintain records on the identities of clients engaged in transactions that are considered suspicious or that involve an amount equal to or greater than 10,000 euros (approximately $13,250). Records of suspicious transactions that are required to be reported to the FIU must be kept for at least five years.

Financial institutions are required to train their personnel in the detection and handling of suspicious transactions that could be linked to money laundering. Financial institutions or other entities with reporting requirements are also liable for illegal activities occurring under their control. Failure to comply with the anti-money laundering legislation, including failure to report, is punishable by a fine of up to $1.56 million.

Money laundering legislation imposes prohibitions on cash payments for real estate, except for an amount not exceeding 10 percent of the purchase price or approximately $18,800, whichever is lower. Cash payments over $18,800 for goods are also illegal.

Belgium had long permitted the issuance of bearer bonds ("titres au porteur"), widely used to transfer wealth between generations and to avoid taxes. In late 2005 the Belgian federal parliament adopted a law to cease the issuance of bearer bonds beginning on January 1, 2008. Bearer bonds issued before that date will still be valid, however. Bearer shares are permitted for individuals as well as for banks and companies.

Currently, Belgium has no reporting requirements on cross-border currency movements. However, in October 2005, the European Parliament and Council of the European Union issued Regulation (EC) No. 1889/2005 on controls of cash entering or leaving the Community. Belgium expects to implement this regulation by June 15, 2007, as required. Belgian customs officials and CTIF-CFI will verify cross-border currency movements, and irregularities may be forwarded to judicial authorities.

Belgium and other EU member states must implement the Third EU Money Laundering Directive by December 15, 2007. As for nonprofit organizations, the European Commission adopted a communication on November 29, 2005, that includes recommendations for EU member states and a framework for a code of conduct for the sector. Belgian officials are working to increase transparency in the nonprofit sector through better enforcement of registration and reporting procedures. Requirements for nonprofit organizations include registering, furnishing copies of their statutes and list of members, providing minutes from council meetings, and filing budget reports.

The Belgian financial intelligence unit (FIU), known as the Cellule de Traitement des Informations Financières and in Flemish as Cel voor Financiële Informatieverwerking (CTIF-CFI), was created by the Royal Decree of 11 June 1993, on the Composition, Organization, Operation and Independence of the FIU. The FIU is an autonomous and independent public administrative authority, supervised by the Ministries of Justice and Finance. Institutions and persons subject to the reporting obligations fund the FIU. Although these contributions are compulsory, the contributing entities do not exercise any formal control over the FIU. CTIF-CFI's primary mission is to receive, analyze, and disseminate all suspicious transaction reports submitted by regulated entities. Operating as a filter between obligated entities and judicial authorities, CTIF-CFI reports possible money laundering or terrorist financing transactions to the public prosecutor. The financial sector cooperates actively with CTIF-CFI to guard against illegal activity. No civil, penal, or disciplinary actions can be taken against institutions, or their employees or representatives, for reporting transactions in good faith to CTIF-CFI. Legislation also exists to protect witnesses, including bank employees, who report suspicions of money laundering or who come forward with information about money laundering crimes. Belgian officials have imposed

sanctions on institutions or individuals that knowingly permitted illegal activities to occur. CTIF-CFI also acts as the supervisory body for professions not supervised by CBFA or other authorities. CTIF-CFI has also been very active in analyzing the diamond industry and working to eliminate its potential for money laundering and terrorist financing. It has initiated several meetings with the Belgian Ministry of Economic Affairs and the High Council for Diamonds in order to clarify the obligations of diamond traders with respect to anti-money laundering and antiterrorist financing laws and how diamond traders apply this legislation.

Financial experts, including three magistrates (public prosecutors) appointed by the King compose the CTIF-CFI. A magistrate presides over the body. Terms of service are for six years and may be renewed. In addition to administrative and legal support, the investigative department consists of inspectors/analysts. There are also three liaison police officers, one customs officer, and one officer of the Belgian intelligence service to maintain contact with the various law enforcement agencies in Belgium.

From its founding in 1993 until the end of 2005, CTIF-CFI received 104,537 disclosures and opened a total of 21,959 individual case files (numerous disclosures may be linked to a single case). Of these, the FIU has transmitted 7,114 cases to the public prosecutor aggregating approximately $15.48 billion. In 2005, the FIU received 10,148 disclosures, opened 3,051 new cases, and transmitted 686 cases to the public prosecutor, up from 664 cases transmitted in 2004. Nearly 75 percent of disclosures on files transmitted to the federal prosecutor were made by credit institutions. Foreign exchange offices and foreign counterpart units accounted for an additional 18 percent of the files transmitted, with notaries, casinos, and other entities also reporting.

Since the creation of CTIF-CFI in 1993, Belgian courts and tribunals have pronounced sentences in at least 837 of the 7,114 cases transmitted to the Federal Prosecutor (some of these convictions are still under appeal). From 1993-2005, the conviction rate was 12 percent. To date, Belgian courts have convicted 1,880 individuals for money laundering on the basis of cases forwarded by the FIU. These convictions have yielded combined total sentences of 2,819 years. Whereas five years is the maximum sentence for money laundering, the length of the sentence may increase if the financial crime is compounded by another type of crime such as drug trafficking. The cumulative fines levied for money laundering total approximately $91 million. Belgian authorities have confiscated more than $788 million connected with money laundering crimes. The majority of convictions related to money laundering are based upon disclosures made by the financial institutions and others to CTIF-CFI.

As with Belgium's FIU, the federal police are required to transmit suspected money laundering cases to the public prosecutor. In 2005 the federal police referred a total of 2,241 individuals to the public prosecutor for various crimes. More than 20 percent of these (450 individual cases) involved money laundering, fraud, and corruption. Other offenses were: narcotics (28 percent); aggravated theft in homes (13 percent); stolen vehicles (12 percent); armed robbery (12 percent); and trafficking in persons (10 percent). In 2005, the federal police referred 10 individuals to the public prosecutor for suspected links to terrorism. The FATF evaluation team found that the criminal prosecution authorities have the necessary power to carry out their functions; however, in some places or at some times, the prosecutors and police seem to lack resources to properly perform their AML/CFT duties.

The federal police enjoy good cross-border cooperation with other police and investigative services in neighboring countries. Belgium does not require an international treaty as a prerequisite to lending mutual assistance in criminal cases. The federal police and the specialized services of the Central Office for the Fight against Organized Economic and Financial Crimes utilize a number of tactics to uncover money laundering operations, including investigating significant capital injections into businesses, examining suspicious real estate transactions, and conducting random searches at all international airports. In 2005, Project Cash Watch, carried out under the auspices of the federal police in Belgium's international airports and other transit venues, netted seizures of more than $2.45

million. The federal police established a special bureau to combat VAT fraud shortly after 2001, when estimates of lost revenue topped $1.4 billion. In 2005, losses to the Belgian Treasury through VAT fraud were an estimated $230 million.

According to the FATF mutual evaluation report, Belgium has created a sophisticated and comprehensive confiscation and seizure regime, including the 2003 establishment of the Central Office for Seizure and Confiscation (COSC). Belgian law allows for civil as well as criminal forfeiture of assets. A law passed in July 2006 allows for the possibility, on a reciprocal basis, of the sharing of seized assets from serious crimes, including those related to narcotics, with affected countries. The COSC operates under the auspices of the Belgian Ministry of Justice and ensures that confiscations and seizures in Belgium are carried out smoothly and efficiently in accordance with Belgian law. In Belgium, confiscations and seizures can only be carried out by a judicial order.

Belgian authorities attempt to sell confiscated items such as cars, computers, and cell phones soon after confiscation in order to minimize the loss of the market value of the goods over time. If a suspect is later found innocent, he or she receives the cash equivalent of the item(s) sold, plus accrued interest. COSC has a commercial account for the deposit of confiscated funds. As of October 2006, the fund held more than $165 million. COSC also maintains safe deposit boxes for the storage of high value items, such as jewelry. Beginning in 2005, a verification program has been in place to check the legal records of suspects who have been found innocent and are about to have confiscated proceeds returned to them. If it is discovered that the person owes taxes or has overdue fines, for example, COSC can intervene and ensure that the Belgian government is paid before proceeds are returned. Through October 2006, this program has netted $1.65 million for federal coffers.

Seizures in Belgium can be direct or indirect. Direct seizures involve the seizure of items linked directly to a crime. Noncash items are held in the clerks' offices in one of Belgium's 27 judicial districts. Indirect seizures are "seizures by equivalence," usually of homes, cars, jewels, etc., not directly linked to the crime in question. Money from seizures and from the sale of seized goods is deposited in the Belgian Treasury. According the COSC, information concerning the value of seizures is not available publicly.

In January 2004, the Belgian legislature passed domestic legislation implementing the EU Council's Framework Decision on Combating Terrorism, which criminalizes terrorist acts and material support (including financial support) for terrorist acts, allowing judicial freezes on terrorist assets. The law transposed the Second European Money Laundering Directive and implemented eight of FATF's Special Recommendations. Article 140 of the Penal Code criminalizes participation in the activity of a terrorist group, and Article 141 specifically penalizes the provision of material resources, including financial assistance, to terrorist groups; the penalty is five to ten years' imprisonment.

Under Belgium's 1993 anti-money laundering and terrorist finance law (amended in 2004), bank accounts can be frozen on a case-by-case basis if there is sufficient evidence that a money laundering crime has been committed. The FIU has the legal authority to suspend a transaction for a period of up to two working days in order to complete its analysis. If criminal evidence exists, the FIU forwards the case to the public prosecutor. In 2005, CTIF-CFI temporarily froze assets in 29 cases, representing approximately $175 million.

Under the January 2004 law, the Ministry of Justice can freeze assets related to terrorist crimes. However, the burden of proof in such cases is relatively high. In order for an act to constitute a criminal offense, authorities must demonstrate that the support was given with the knowledge that it would contribute to the commission of a crime by the terrorist group. Further, as the law does not establish a national capacity for designating foreign terrorist organizations, Belgian authorities must demonstrate in each case that the group that was lent support actually constitutes a terrorist group.

In Belgium, the Ministry of Finance can administratively freeze assets of individuals and entities associated with al-Qaeda, the Taliban and Usama Bin Laden on the United Nations 1267 Sanctions Committee's consolidated list and/or those covered by an EU asset freeze regulation. Seized assets are transferred to the Ministry of Finance. If an entity appears on the UN 1267 Sanctions Committee's consolidated list, but not on the EU list, then the GOB can pass a ministerial decree to freeze assets in order to comply with the UN requirement. Assets of entities appearing on the EU list are automatically subject to a freeze without additional legislative or executive procedures. Belgium is working on legislation to permit the administrative freeze of terrorist assets in the absence of a judicial order or UN or EU designation.

Belgium's FIU is active with its European colleagues in sharing information. CTIF-CFI has signed a memorandum of understanding with the United States that governs their collaborative work. CTIF-CFI was a founding member of the Egmont Group and headed the secretariat from 2005 to 2006. Belgium is a cooperative and reliable partner in law enforcement efforts. In 2005, Belgium collaborated with several countries on a criminal case resulting in nearly $20 million being frozen in accounts held in another European country.

Belgium is a party to the 1988 UN Drug Convention and the UN Convention for the Suppression of the Financing of Terrorism. In August 2004, the GOB ratified the UN Convention against Transnational Organized Crime. Belgium has signed, but not yet ratified, the UN Convention against Corruption. A mutual legal assistance treaty (MLAT) between Belgium and the United States has been in force since 2000, and an, an extradition treaty between the two countries has been operative since September 1997. The MLAT process is used for all information requests related to criminal cases, with careful consideration of privacy rights of parties involved. Bilateral instruments amending and supplementing these treaties, in implementation of the U.S.-EU Extradition and Mutual Legal Assistance Agreements, were signed with Belgium in December 2004.

Belgium's continuing work on implementing the FATF recommendations complements an already solid anti-money laundering regime and a clear official commitment to fighting against financial crimes, including the financing of terrorism. However, the Government of Belgium should continue to work through proposed legislation that pursues tougher and faster independent asset-freezing capability as well as the optimal disposition of seized assets. The Government of Belgium should continue its efforts to uncover, investigate, and prosecute illegal banking operations, including those connected to its diamond and real estate sectors, as well as the informal financial sector and nonbank financial institutions. Belgium should continue to enact reforms in the diamond market that will promote increased transparency. The GOB should strengthen adherence to reporting requirements by some nonfinancial entities in Belgium, such as lawyers and notaries. To be even more effective in its efforts, Belgium may need to devote more resources, including investigative personnel, to police, prosecutors and key Belgian agencies that work on money laundering, terrorist financing, and other financial crimes.

## Belize

Belize is not a major regional financial center. In an attempt to diversify Belize's economic activities, authorities have encouraged the growth of offshore financial activities and have pegged the Belizean dollar to the U.S. dollar. Belize continues to offer financial and corporate services to nonresidents. Belizean officials suspect that money laundering occurs primarily within the country's offshore financial sector. Money laundering, primarily related to narcotics trafficking and contraband smuggling, also occurs through banks operating in Belize. Criminal proceeds laundered in Belize are derived primarily from foreign criminal activities. There is no evidence to indicate that money laundering proceeds are primarily controlled by local drug-trafficking organizations, organized criminals or terrorist groups.

Offshore banks, international business companies (IBCs) and trusts are authorized to operate from within Belize, although shell banks are prohibited within the jurisdiction. The Offshore Banking Act, 1996, governs activities of Belize's offshore banks. Presently, there are eight licensed offshore banks, approximately 32,800 active registered IBCs, one licensed offshore insurance company, one mutual fund company, and 30 trust companies and agents operating in Belize. Local money exchange houses, which were suspected of money laundering, were closed effective July 11, 2005. There are also a number of undisclosed internet gaming sites operating from within the country. These gaming sites are unregulated at this time. Currently there are no offshore casinos operating from within Belize. Government of Belize (GOB) officials have reported an increase in financial crimes, such as bank fraud, cashing of forged checks, and counterfeit Belizean and United States currency. The Central Bank of Belize has engaged in public awareness activities and trainings to regulate counterfeit currency.

The International Business Companies Act of 1990 and its 1995 and 1999 amendments govern the operation of IBCs. The 1999 amendment to the Act allows IBCs to operate as banks and insurance companies. The International Financial Services Commission regulates the rest of the offshore sector. All IBCs must be registered. Although IBCs are allowed to issue bearer shares, the registered agents of such companies must know the identity of the beneficial owners of the bearer shares. GOB legislation allows for the appointment of nominee directors. The legislation for trust companies, the Belize Trust Act, 1992, is not as stringent as the legislation for other offshore financial services and does not preclude the appointment of nominee trustees.

There is one free trade zone presently operating in Belize, at the border with southern Mexico. There are also designated free trade zones in Punta Gorda, Belize City and Benque Viejo, but they are not operational. Data Pro Ltd. is designated as an Export Processing Zone (EPZ) and is regulated in accordance with the EPZ Act. Commercial free zone (CFZ) businesses are allowed to conduct business within the confines of the CFZ, provided they have been approved by the Commercial Free Zone Management Agency (CFZMA) to engage in business activities. All merchandise, articles, or other goods entering the CFZ for commercial purposes are exempted from the national customs regime. However, any trade with the national customs territory of Belize is subject to the national Customs and Excise law. The CFZMA, in collaboration with the Customs Department and the Central Bank of Belize, monitors the operations of CFZ business activities. There is no indication that the CFZ is presently being used in trade-based money laundering schemes or by financiers of terrorism.

Allegedly, there is a significant black market for smuggled goods in Belize. However, there is no evidence to indicate that the smuggled goods are significantly funded by narcotics proceeds, or evidence to indicate significant narcotic-related money laundering. The funds generated from contraband are undetermined.

The Money Laundering (Prevention) Act (MLPA), in force since 1996, criminalizes money laundering related to many serious crimes, including drug-trafficking, forgery, terrorism, blackmail, arms trafficking, kidnapping, fraud, illegal deposit taking, false accounting, counterfeiting, extortion, robbery, and theft. The minimum penalty for a money laundering offense as defined by the MLPA is three years imprisonment. Other legislation to combat money laundering include the Money Laundering Prevention Guidance Notes; the Financial Intelligence Unit Act, 2002; the Misuse of Drugs Act; The International Financial Services Practitioners Regulations (Code of Conduct), 2001 (IFSCR); Money Laundering Prevention Regulations, 1998 (MLPR); and the Offshore Banking Act, 2000, renamed the International Banking Act, 2002 (IBA). In 2006, there were no major money laundering cases to report, and the effectiveness of the anti-money laundering regime in Belize remains unclear.

The Central Bank of Belize supervises and examines financial institutions for compliance with anti-money laundering and counterterrorist financing laws and regulations. The banking regulations

governing offshore banks are different from the domestic banking regulations in terms of capital requirements. Banks are not permitted to issue bearer shares. Nevertheless, all licensed financial institutions in Belize (onshore and offshore) are governed by the same legislation and must adhere to the same anti-money laundering and counterterrorist financing requirements. To legally operate from within Belize, all offshore banks must be licensed by the Central Bank and be registered as IBCs. Before the Central Bank issues the license, the Central Bank must verify shareholders' and directors' backgrounds, ensure the adequacy of capital, and review the bank's business plan. The legislation governing the licensing of offshore banks does not permit directors to act in a nominee (anonymous) capacity.

The Central Bank issued Supporting Regulations and Guidance Notes in 1998. Licensed banks and financial institutions are required to establish due diligence ("know-your-customer") provisions, monitor their customers' activities and report any suspicious transactions to the financial intelligence unit (FIU). Belize law obligates banks and other financial institutions to maintain business transactions records for at least five years when the transactions are complex, unusual or large. Money laundering controls are also applicable to nonbank financial institutions, such as exchange houses, insurance companies, lawyers, accountants and the securities sector, which are regulated by the International Financial Services Commission. Financial institution employees are exempt from civil, criminal or administrative liability for cooperating with regulators and law enforcement authorities in investigating money laundering or other financial crimes. Belize does not have any bank secrecy legislation that prevents disclosure of client and ownership information.

The reporting of all cross-border currency movement is mandatory. All individuals entering or departing Belize with more than $10,000 in cash or negotiable instruments are required to file a declaration with the authorities at Customs, the Central Bank and the FIU.

The FIU of Belize is an independent agency presently housed at the Central Bank. Current laws do not provide for the funding of the FIU, and the FIU has to apply to the Ministry of Finance for funds. The funding allocated to the FIU for fiscal year 2006 was approximately $200,000. Due to financial constraints, the FIU is not adequately staffed and existing personnel lack sufficient training and experience. On November 5, 2005 the director of the FIU resigned, leaving the FIU with only four employees; the new FIU director did not begin until July 2006.

As of October 15, 2006, the FIU had received 34 suspicious transaction reports (STRs) from obligated entities. Of the 34 STRs filed, 13 became the subject of investigations. The Director of the Public Prosecutions Office and the Belizean Police Department are responsible for investigating all crimes. However, the FIU also has administrative, prosecutorial and investigative responsibilities for financial crimes, such as money laundering and terrorist financing. Although the FIU has access to records and databanks of other GOB entities and financial institutions, there are no formal mechanisms for the sharing of information with domestic regulatory and law enforcement agencies. The FIU is empowered to share information with FIUs in other countries. On several occasions, the FIU has cooperated with the United States' FIU and other U.S. law enforcement agencies.

Belize criminalized terrorist financing via amendments to its anti-money laundering legislation, The Money Laundering (Prevention) (Amendment) Act, 2002. GOB authorities have circulated the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 to all financial institutions in Belize. There are no indications that charitable or nonprofit entities in Belize have acted as conduits for the financing of terrorist activities. Consequently, the country has not taken any measures to prevent the misuse of charitable and nonprofit entities from aiding in the financing of terrorist activities.

Alternative remittance systems are illegal in Belize. However, Belizean authorities acknowledge the existence and use of indigenous alternative remittance systems that bypass, in whole or in part,

financial institutions. Therefore, Belizean authorities monitor such activities at the borders with Mexico and Guatemala.

Belizean law makes no distinctions between civil and criminal forfeitures. All forfeitures resulting from money laundering or terrorist financing are treated as criminal forfeitures. The banking community cooperates fully with enforcement efforts to trace funds and seize assets. The FIU and the Belize Police Department are the entities responsible for tracing, seizing and freezing assets, and the Ministry of Finance can also confiscate frozen assets. With prior court approval, Belizean authorities have the power to identify, freeze and seize assets related to terrorist financing or money laundering. Currently, the GOB's legislation does not specify the length of time assets can be frozen. There are no limitations to the kinds of property that may be seized, including any property—tangible or intangible—which may be related to a crime or is shown to be from the proceeds of a crime. This includes legitimate businesses. However, Belizean law enforcement lacks the resources necessary to trace and seize assets.

The Belize Police Department reported that during 2006, the only assets forfeited or seized were firearms and ammunition, on which no value is placed. Assets forfeited and/or seized in 2005 totaled approximately $120,000. GOB authorities are considering the enactment of a Proceeds of Crime law, which will address the seizure or forfeiture of assets of narcotics traffickers, financiers of terrorism, or organized crime. Currently, the GOB is not engaged in any bilateral or multilateral negotiations with other governments to enhance asset tracing and seizure. However, the Government of Belize actively cooperates with the efforts of foreign governments to trace or seize assets relating to financial crimes.

Belize has signed a Mutual Legal Assistance Treaty with the United States, which provides for mutual legal assistance in criminal matters. Amendments to the MLPA preclude the necessity of a Mutual Legal Assistance Treaty for exchanging information or providing judicial and legal assistance to authorities of other jurisdictions in matters pertaining to money laundering and other financial crimes. Belize is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the 1988 UN Drug Convention. The GOB has signed, but not yet ratified, the Inter-American Convention against Terrorism, and has neither signed nor ratified the UN Convention against Corruption. Belize is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Working Group to Control Money Laundering and the Caribbean Financial Action Task Force. Its FIU became a member of the Egmont Group of financial intelligence units in 2004.

The Government of Belize should increase resources to provide adequate training to those entities responsible for enforcing Belize's anti-money laundering and counterterrorist financing laws, including the financial intelligence unit and the asset forfeiture regime. Belize should take steps to address the vulnerabilities in its supervision of its offshore sector, particularly the lack of supervision of internet gaming facilities. Belize should immobilize bearer shares and mandate suspicious activity reporting for the offshore financial sector.

## Bolivia

Bolivia is not an important regional financial center, but it occupies a geographically significant position in the heart of South America. Bolivia is a major drug producing and drug-transit country. Most money laundering in Bolivia is related to public corruption, contraband smuggling, and narcotics trafficking. Bolivia's long tradition of bank secrecy and the lack of a government entity with effective oversight of nonbank financial activities facilitate the laundering of the profits of organized crime and narcotics trafficking, the evasion of taxes, and laundering of other illegally obtained earnings.

Bolivia's formal financial sector consists of approximately 13 commercial banks, six private financial funds, nine mutual funds, 23 savings and credit cooperatives, 14 insurance companies and one stock exchange, all of which are subject to the same anti-money laundering controls. The Bolivian system is highly dollarized, with close to 90 percent of deposits and loans denominated in dollars rather than bolivianos, the local currency. Free trade zones exist in the cities of El Alto, Cochabamba, Santa Cruz, Oruro, Puerto Aguirre and Desaguadero.

Several entities that move money in Bolivia remain unregulated. Hotels, currency exchange houses, illicit casinos, cash transporters, and wire transfer businesses can be used to transfer money freely into and out of Bolivia but are not subject to anti-money laundering controls. Informal exchange businesses, particularly in the department of Santa Cruz, are also used to transmit money in order to avoid law enforcement scrutiny.

Bolivia's anti-money laundering regime is based on Law 1768 of 1997. Law 1768 modifies the penal code; criminalizes money laundering related only to narcotics trafficking, organized criminal activities and public corruption; provides for a penalty of one to six years for money laundering; and defines the use of asset seizure beyond drug-related offenses. Law 1768 also created Bolivia's financial intelligence unit (FIU), the Unidad de Investigaciones Financieras (UIF), within the Office of the Superintendence of Banks and Financial Institutions. The attributions and functions of the unit are defined under Supreme Decree 24771 of July 31, 1997.

Although Law 1768 established the UIF as an administrative financial intelligence unit in 1997, the UIF did not become operational until July 1999. As Bolivia's FIU, the UIF is responsible for collecting and analyzing data on suspected money laundering and other financial crimes. Under Decree 24771, obligated entities-which include only banks, insurance companies and securities brokers-are required to identify their customers, retain records of transactions for a minimum of ten years, and report to the UIF all transactions that are considered unusual (without apparent economic justification or licit purpose) or suspicious (customer refuses to provide information or the explanation and/or documents presented are clearly inconsistent or incorrect). Under the current law, there is no requirement for obligated entities to report cash transactions above a designated threshold, nor is there a requirement that persons entering or leaving the country declare the transportation of currency over a designated threshold, as is commonplace in many countries' anti-money laundering regimes.

After analyzing suspicious transaction reports and any other relevant information it may receive, the UIF reports all detected criminal activity to the Public Ministry. The UIF also has the ability to request additional information from obligated financial institutions in order to assist the prosecutors of the Public Ministry with their investigations. The Special Group for Investigation of Economic Financial Affairs (GIAEF), created in 2002 within Bolivia's Special Counter-Narcotics Force (FELCN), is responsible for investigating narcotics-related money laundering. The UIF, the Public Ministry, the National Police and FELCN have established mechanisms for the exchange and coordination of information, including formal exchange of bank secrecy information. The UIF is also responsible for implementing anti-money laundering controls, and may request that the Superintendence of Banks sanction obligated institutions for noncompliance with reporting requirements. In 2004, the UIF began on-site inspections of obligated entities in order to review their compliance with the reporting of suspicious transactions. Given the size of Bolivia's financial sector, compliance with reporting requirements is extremely low, as the UIF receives, on average, less than 50 suspicious transaction reports per year. Seventy percent of those reports are filed by a single bank.

Corruption is a serious issue in Bolivia. According to estimates by the U.S. Agency for International Development (USAID), corruption costs Bolivians approximately $115 million per year, equal to half of the GOB's budget deficit. Traditionally, allegations against high-ranking law enforcement officials were routinely dismissed or forgotten. However, recently created anticorruption task forces have

increased the effectiveness of investigations and prosecutions, and the number of convictions related to the crime of corruption is growing.

In order to further combat corruption, the GOB promulgated Supreme Decree 28695, the Organizational Structure for the Fight against Corruption and Illicit Enrichment, on April 26, 2006. Among a number of other provisions, the decree provides for the creation of a "Financial and Property Intelligence Unit," which would replace the UIF. Decree 28695 also repealed Decree 24771, which gave the UIF its authority. However, given that the repeal of Decree 24771 would eliminate the UIF before its replacement was operational, the GOB then passed Decree 28713 on May 13, 2006, reinstating the UIF's functions and duties until January 2007 and placing the UIF under the Ministry of Finance. On November 29, 2006, the GOB passed Decree 28956, eliminating the portion of Decree 28695 that had repealed Decree 24771 and allowing the UIF to continue to operate until the Financial and Property Intelligence Unit becomes a functioning entity.

The Constitution Commission of the Bolivian Chamber of Deputies has drafted a new anti-money laundering law that would establish the Financial and Property Intelligence Unit as Bolivia's sole financial intelligence unit. However, the law does not include provisions to bring Bolivia's anti-money laundering regime into greater compliance with international standards, in spite of suggestions and input from the Financial Action Task Force for South America (GAFISUD), the International Monetary Fund (IMF), the UIF, and the Government of the United States. The draft was presented to Chamber of Deputies in early December 2006, but is not yet under consideration by the Chamber.

Although the draft law in effect provides a mission for the Financial and Property Intelligence Unit, there are concerns regarding the functions and authorities of the new entity, and the current operations of the UIF. As a result of the new decree and the plans to establish Financial and Property Intelligence Unit, the UIF has undergone two changes in leadership since April 2006 and many staff members have left, bringing the number of personnel to only five. Limitations in its reach, a lack of resources, and weaknesses in its basic legal and regulatory framework have traditionally hampered the UIF's effectiveness as a financial intelligence unit. There is no indication that the establishment of the Financial and Property Intelligence Unit will resolve these problems and allow for a more effective FIU.

There are also concerns that the new legislation will not improve the GOB's overall anti-money laundering regime, which is undermined by the lack of a legal and bureaucratic framework for money laundering investigations carried out by law enforcement officials. In order to prosecute a money laundering case, Bolivian law requires that the crime of money laundering be tied to an underlying illicit activity. At present, the list of these underlying crimes is extremely restrictive and inhibits money laundering prosecution. Although the Public Ministry is the office responsible for prosecuting money laundering offenses, it does not have a specialized unit dedicated to the prosecution of these cases. Judges trying these cases are challenged to understand their complexities. To date, there has been only one conviction involving money laundering.

There are also serious deficiencies in Bolivia's legal framework with regard to civil responsibility. Under Bolivian law, there is no protection for judges, prosecutors or police investigators who make good-faith errors while carrying out their duties. If a case is lost initially or on appeal, or if a judge rules that the charges against the accused are unfounded, the accused can request compensation for damages, and the judges, prosecutors or investigators can be subject to criminal charges for misinterpreting the law. This is particularly a problem for money laundering investigations, as the law is full of inconsistencies and contradictions, and is open to wide interpretation. For these reasons, prosecutors are often reluctant to pursue these types of investigations.

While traditional asset seizure continues to be employed by counternarcotics authorities, until recently the ultimate forfeiture of assets was problematic. Prior to 1996, Bolivian law permitted the sale of property seized in drug arrests only after the Supreme Court confirmed the conviction of a defendant.

A 1995 decree permitted the sale of seized property with the consent of the accused and in certain other limited circumstances. The Directorate General for Seized Assets (DIRCABI) is responsible for confiscating, maintaining, and disposing of the property of persons either accused or convicted of violating Bolivia's narcotics laws. DIRCABI, however, has been poorly managed for years, and has only auctioned confiscated goods sporadically. The UIF, with judicial authorization, may freeze accounts for up to 48 hours in suspected money laundering cases; this law has only been applied on one occasion.

Although terrorist acts are criminalized under the Bolivian Penal Code, the GOB currently lacks legislation that specifically addresses terrorist financing. Bolivia is a party to the UN International Convention for the Suppression of the Financing of Terrorism and has signed, but not ratified, the Organization of American States (OAS) Inter-American Convention against Terrorism. However, there are no explicit domestic laws that criminalize the financing of terrorism or grant the GOB the authority to identify, seize or freeze terrorist assets. Nevertheless, the UIF distributes the terrorist lists of the United Nations and the United States, receives and maintains information on terrorist groups, and can freeze suspicious assets under its own authority for up to 48 hours, as it has done in counternarcotics cases. A draft terrorist financing law was created by the UIF and presented to the Superintendence of Banks. However, the bill has not yet been presented to Congress. There have been no cases of terrorist financing to date.

The GOB remains active in multilateral counternarcotics and international anti-money laundering organizations. Bolivia is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group on Money Laundering and GAFISUD. Bolivia is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption and the UN Convention against Transnational Organized Crime. The GOB and the United States signed an extradition treaty in June 1995, which entered into force in November 1996.

While the Government of Bolivia's efforts to combat corruption are necessary, the GOB should take steps to ensure that any changes in its anticorruption legislation will strengthen its anti-money laundering regime. The GOB should also improve its current money laundering legislation so that it conforms to the standards of the Financial Action Task Force and GAFISUD by making money laundering an autonomous offense without requiring a connection to other illicit activities; criminalizing terrorist financing; allowing the blocking of terrorist assets; and, requiring currently unregulated sectors to be subject to anti-money laundering and counterterrorist financing controls. Bolivia should ensure that, with the creation of a new financial intelligence unit, the unit has sufficient staff and resources, as well as the authority to receive suspicious transaction reports on activities indicative of terrorist financing and reports from nonbank financial institutions. Bolivia should also continue to strengthen the relationships and cooperation between all government entities involved in the fight against money laundering and other financial crimes in order to create a more effective regime capable of preventing and combating money laundering and terrorist financing.

## Bosnia and Herzegovina

Bosnia and Herzegovina (BiH) has a cash-based economy and is not an international, regional, or offshore financial center. International observers believe the laundering of illicit proceeds from criminal activity including the proceeds from smuggling, corruption, and tax evasion is widespread. Due to its porous borders and weak enforcement capabilities, BiH is a significant market and transit point for illegal commodities including cigarettes, narcotics, firearms, counterfeit goods, lumber and fuel oils. BiH authorities have had some recent success in clamping down on money laundering through the formal banking system, which has resulted in suspect nongovernmental organizations (NGOs) increasing their use of direct cash transfers from abroad as a source of funding.

There are multiple jurisdictional levels in Bosnia and Herzegovina, including the State, the two entities (the Federation of Bosnia and Herzegovina and the Republika Srpska), and Brcko District. The Federation is further divided into ten cantons. New criminal and criminal procedure codes from the State, the two entities and Brcko District were enacted and harmonized in 2003, although the jurisdictions maintain their own enforcement bodies. Although state-level institutions are becoming more firmly grounded and are gaining increased authority, there remains a fair amount of confusion regarding jurisdictional matters between the entities and state-level institutions. Unless otherwise specified, relevant laws and institutions are at the state level.

Money laundering of all kinds is a criminal offense in all state and entity criminal codes. The new criminal procedure and criminal codes enacted in 2003 included tougher provisions against money laundering. At the state level, the Law on the Prevention of Money Laundering came into force in December 2004. The law determines the measures and responsibilities for detecting, preventing, and investigating money laundering and terrorist financing. The law also prescribes measures and responsibilities for international cooperation and establishes a financial intelligence unit (FIU) within the State Investigative and Protection Agency (SIPA). The law requires banks to submit reports on suspicious financial transactions to the state-level FIU. The Prosecutor's office must also share data on money laundering and terrorist financing offenses with the FIU.

The Law on the Prevention of Money Laundering applies to any person who "accepts, exchanges, keeps, disposes of, uses in commercial or other activity, otherwise conceals or tries to conceal money or property he knows was acquired through perpetration of criminal offence, when such a money or property is of larger value or when such an act endangers the common economic space of Bosnia and Herzegovina or has detrimental consequences to the operations or financing of institutions of Bosnia and Herzegovina." For money laundering convictions covering amounts above the equivalent of $30,000, the penalty is a term of imprisonment of between one and ten years. For lesser amounts, the penalty is a term of imprisonment of between six months and five years. SIPA and the Federation and Republika Srpska (RS) police bodies are responsible for the investigation of financial crimes. BiH has not enacted bank secrecy laws which prevent the disclosure of client and ownership information to bank supervisors and law enforcement authorities.

Banks and other financial institutions are required to know, record, and report the identity of customers engaging in significant transactions, including currency transactions above the equivalent of $18,000. Obliged entities are also required to maintain records for twelve years in order to respond to law enforcement requests. The money laundering law applies to all individuals and several nonbank financial institutions including, but not limited to, post offices, investment and mutual pension companies, stock exchanges and stock exchange agencies, insurance companies, casinos, currency exchange offices and intermediaries such as lawyers and accountants. There is, however, no formal supervision mechanism in place for nonbank financial institutions and intermediaries. It is mandatory for all banks and financial institutions to report suspicious transactions, and there is no mandated reporting threshold for reporting suspicious transactions. Banking authorities have supervision responsibility for all covered sectors. However, reportedly there is little supervision of nonbank financial institutions and intermediaries. The law also requires that customs administration authorities report cross-border transportation of cash and securities in excess of $6,000 to the FIU. The Indirect Taxation Authority (ITA), which has responsibility for customs, suffers, like other BiH state-level agencies, from a lack of resources and sufficiently trained personnel.

The banking community cooperates with law enforcement efforts to trace funds and freeze accounts. Bosnian law protects reporting individuals with respect to law enforcement cooperation. Although there is no state-level banking supervision agency, entity level banking supervision agencies oversee and examine financial institutions for compliance with anti-money laundering and counter terrorist financing laws and regulations.

The Financial Intelligence Department (FID), Bosnia-Herzegovina's FIU, is a hybrid body, performing analytical duties with some limited criminal investigative responsibilities. The FID receives, collects, records, analyzes, and forwards information related to money laundering and terrorist financing to the State Prosecutor. It also provides expert support to the Prosecutor regarding financial activities, and is responsible for international cooperation on money laundering issues. The FID has access to the records of other government entities, and formal mechanisms for inter-agency information sharing are in place. The FID is empowered to freeze accounts for five days; when its preliminary analysis is complete, it may forward the case to the Prosecutor. At that point, the freeze on the accounts may be extended. The FIU reports that it froze approximately $1,468,604 in the first nine months of 2006.

The September 2006 International Monetary Fund's Financial System Stability Assessment report praised Bosnia-Herzegovina for the progress made since the MONEYVAL 2005 mutual evaluation report. It cited in particular "the development of an effective state-level FIU." However, according to a European Commission report, fewer than half of FID's planned positions have been filled. There are also reported problems with information-sharing, coordination, and communication, as well as jurisdictional issues between the Financial Police and other State agencies.

For the first nine months of 2006, FID received 145,071 currency reports from banks and other financial institutions. Of these, 14 were identified as suspicious and nine were investigated. Of these nine investigations, two cases were dropped, four have been sent to the prosecutor's office, and three are still under investigation. Since BiH established its anti-money laundering regime, there have been nineteen convictions for money laundering. However, because of the appeals process, only one conviction has been finalized.

BiH has no asset forfeiture law, with the exception of the Persons Indicted for War Crimes (PIFWC) support laws which allow for the seizure of PIFWC assets or assets of those providing material support to them. Articles 110 and 111 of the BiH Criminal Code (along with similar laws in the harmonized entity and Brcko Criminal Codes) are the only legal provisions that might be used in place of an actual asset forfeiture law. These provisions authorize the "confiscation of material gain" (or a sum of money equivalent to the material gain if confiscation is not feasible) from illegal activity. The tools used in committing those crimes are not subject to seizure. Confiscation can only be done as part of a verdict in a criminal case, and is administered by the courts, not law enforcement agencies. The courts decide whether the articles will be "sold under the provisions applicable to judicial enforcement procedure, turned over to the criminology museum or some other institution, or destroyed. The proceeds obtained from sale of such articles shall be credited to the budget of Bosnia and Herzegovina." Prosecutors and courts do not have the administrative mechanisms in place to seize assets, maintain them in storage, dispose of them, or route the proceeds to the appropriate authorities. Property may be seized for criminal offenses for which a term of imprisonment of five years or more is prescribed. A specific relationship to the crime does not have to be proven for the assets to be seized. There is no mechanism for civil forfeiture. There are no laws for sharing seized assets with other governments. BiH authorities have the authority to identify, freeze, seize, and forfeit terrorist-finance-related and other assets. The banking agencies (Federation and RS Banking Agencies) in particular have the capability to freeze assets without undue delay.

Terrorist financing was criminalized in article 202 of the criminal procedure code. BiH is a party to the 1999 International Convention for the Suppression of the Financing of Terrorism. The entity banking agencies are cognizant of the requirements to sanction individuals and entities listed by the UNSCR 1267 Sanctions Committee's consolidated list. However, the state authorities do not circulate this list to entity authorities on a regular basis. In July 2006, BiH adopted a "Strategy against Terrorism," but SIPA needs to be strengthened to meet its designated responsibilities in the Strategy.

In 2006, after a cooperative investigation between BiH and law enforcement authorities in several European Union countries, BiH authorities initiated a prosecution at the Court of Bosnia and Herzegovina against five people suspected of terrorist crimes. And in 2004, the government disrupted the operations of Al Furqan (aka Sirat, Istikamet), Al Haramain & Al Masjed Al Aqsa Charity Foundation, and Taibah International, organizations listed by the UNSCR 1267 Committee as having direct links with al-Qaida. Authorities continue to investigate other organizations and individuals for links to terrorist financing.

Nonbank financial transfers are reportedly very difficult for BiH law enforcement and customs officials to deal with due to a lack of reporting as well as a lack of understanding of indigenous methodologies, many of which are found in the underground economy and are enabled by smuggling and the misuse of trade. Currently there are six Free Trade Zones in BiH. However, only three of the zones are active, with production based mainly on automobiles and textiles.

Bosnia and Herzegovina has no Mutual Legal Assistance Treaty with the U.S., although an extradition treaty signed by the Kingdom of Serbia in 1902 has carried over into BiH; some financial crimes are covered, but not contemporary forms of money laundering. There is no formal bilateral agreement between the United States and BiH regarding the exchange of records in connection with narcotics investigations and proceedings. Authorities have made good faith efforts to exchange information informally with officials from the United States. BiH is a party to the 1988 UN Drug Convention (by way of succession from the former Yugoslavia), the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the UN International Convention for the Suppression of the Financing of Terrorism. Unfortunately, on many occasions, BiH has not passed implementing legislation for the international conventions to which it is a signatory.

The Government of Bosnia and Herzegovina (GOBH) should continue to strengthen institutions with responsibilities for money laundering prevention, particularly those at the state level. Due to a lack of resources and bureaucratic politics, SIPA and the FIU, like many state institutions, remain under-funded and under-resourced. Efforts should be made to increase funding for its anti-money laundering and counterterrorist finance programs and enhance cooperation between concerned departments and agencies. Prosecutors, financial investigators, and tax administrators have received training on tax evasion, money laundering and other financial crimes. However, significant additional training may be necessary to ensure that they understand diverse methodologies and aggressively pursue investigations. BiH law enforcement and customs authorities should take additional steps to control the integrity of the border and limit smuggling. Efforts should be made to understand the illicit markets and their role in trade-based money laundering and alternative remittance systems. BiH should study the formation of centralized regulatory and law enforcement authorities. Specific steps should be taken to combat corruption at all levels of commerce and government.

## Brazil

Brazil is the world's fifth largest country in both size and population, and its economy is the tenth largest in the world. Due to its size and significant economy, Brazil is considered a regional financial center, although it is not an offshore financial center. Brazil is also a major drug-transit country. Brazil maintains adequate banking regulations, retains some controls on capital flows, and requires disclosure of the ownership of corporations. Brazilian authorities report that money laundering in Brazil is primarily related to domestic crime, especially drug-trafficking, corruption, organized crime, and trade in contraband, all of which generate funds that may be laundered through the banking system, real estate investment, financial asset markets, luxury goods or informal financial networks. An Inter-American Development Bank study of money laundering in the region found that Brazil's relatively strong institutions helped reduce the incidence of money laundering to below average for the region.

In 2006 the Government of Brazil (GOB) continued investigations into a series of corruption scandals of unusual scope that emerged in 2005. Parallel investigations by Brazilian Congressional committees and law enforcement authorities revealed illicit financing by several political parties of their 2002 presidential campaigns and a related scheme involving vote-buying in Congress by elements within the ruling party and the executive branch, financed by kickbacks on contracts. Two medium-sized regional banks served as conduits for illicit payments, making use of a publicity firm's bank accounts, while some payments were made into bank accounts overseas. Fourteen senators and federal deputies either resigned or were expelled from office, including the President's former Chief of Staff, due to their involvement in the scheme. Prosecutors have brought criminal charges in the case as well, which are now pending before the Supreme Court. A separate corruption case implicating multiple members of Congress involved inflated billing for ambulances purchased with public funds. Brazil's anti-money laundering mechanisms and institutions have played useful roles in the investigation of these cases.

A primary source of criminal activity and contraband is the Triborder Area (TBA) shared by Argentina, Brazil, and Paraguay. Brazilian authorities have expressed particular concern over the trafficking in arms and drugs in the TBA. Brazilian authorities note that the proceeds of domestic drug trafficking and organized crime feed a regional arms trade, operating in the TBA. In addition, a wide variety of counterfeit goods, including cigarettes, CDs, DVDs, and computer software, are smuggled across the border from Paraguay into Brazil; a significant portion of these counterfeit goods originate in Asia. The U.S. government believes the TBA to be a source of terrorist financing, although the GOB maintains that it has not seen any evidence of such. In 2006 Brazilian customs authorities continued a campaign launched in 2005 to combat contraband in the TBA given the significant loss of tax revenues that result from the contraband trade (estimated at $1.2 billion per year). The campaign has featured enhanced controls at border crossing point and frequent inspections targeting buses used by contraband couriers.

The GOB has a comprehensive anti-money laundering regulatory regime in place. Law 9.613 of 1998 criminalizes money laundering related to drug trafficking, terrorism, arms trafficking, extortion, and organized crime, and penalizes offenders with a maximum of 16 years in prison. The law expands the GOB's asset seizure and forfeiture provisions and exempts "good faith" compliance from criminal or civil prosecution. Regulations issued in 1998 require that individuals transporting more than 10,000 reais (then approximately $10,000, now approximately $4,600) in cash, checks, or traveler's checks across the Brazilian border must fill out a customs declaration that is sent to the Central Bank. Law 10.467 of 2002, which modified Law 9.613, put into effect Decree 3.678 of 2000, thereby penalizing active corruption in international commercial transactions by foreign public officials. Law 10.467 also added penalties for this offense under Chapter II of Law 9.613. Law 10.701 of 2003, which also modifies Law 9.613, establishes terrorist financing as a predicate offense for money laundering. The law also establishes crimes against foreign governments as predicate offenses, requires the Central Bank to create and maintain a registry of information on all bank account holders, and enables the Brazilian financial intelligence unit (FIU) to request from all government entities financial information on any subject suspected of involvement in criminal activity.

Law 9.613 also created Brazil's financial intelligence unit, the Conselho de Controle de Atividades Financeiras (COAF), which is housed within the Ministry of Finance. The COAF includes representatives from regulatory and law enforcement agencies, including the Central Bank and Federal Police. The COAF regulates those financial sectors not already under the jurisdiction of another supervising entity. Currently, the COAF has a staff of approximately 31, comprised of 13 analysts, two international organizations specialists, a counterterrorism specialist, two lawyers and support staff.

Since 1999, the COAF has issued a series of regulations that require customer identification, record keeping, and reporting of suspicious transactions to the COAF by obligated entities. Entities that fall under the regulation of the Central Bank, the Securities Commission (CVM), the Private Insurance Superintendence (SUSEP), and the Office of Supplemental Pension Plans (PC), file suspicious activity

reports (SARs) with their respective regulator, either in electronic or paper format. The regulatory body then electronically submits the SARs to COAF. Entities that do not fall under the regulations of the above-mentioned bodies, such as real estate brokers, money remittance businesses, factoring companies, gaming and lotteries, dealers in jewelry and precious metals, bingo, credit card companies, commodities trading, and dealers in art and antiques, are regulated by the COAF and send SARs directly to COAF, either via the Internet or using paper forms.

In addition to filing SARs, banks are also required to report cash transactions exceeding 100,000 reais (approximately $48,000) to the Central Bank. The lottery sector must notify COAF of the names and data of any winners of three or more prizes equal to or higher than 10,000 reais within a 12-month period. COAF Resolution 14 of October 23, 2006, further extended these anti-money laundering requirements to the real estate sector. Separately, the insurance regulator, SUSEP, clarified its reporting requirements for insurance companies and brokers in Circular 327 from May 29, 2006, which requires these entities to have an anti-money laundering program and report large insurance policy purchases, settlements or otherwise suspicious transactions to both SUSEP and COAF.

The COAF has direct access to the Central Bank database, so that it has immediate access to the SARs reported to the Central Bank. In 2006, it gained access to the Central Bank's new database of all current accounts in the country. COAF also has access to a wide variety of government databases, and is authorized to request additional information directly from the entities it supervises and the supervisory bodies of other obligated entities. Complete bank transaction information may be provided to government authorities, including the COAF, without a court order. Domestic authorities that register with COAF may directly access the COAF databases via a password-protected system. In 2006, the COAF received roughly 13,000 cash transaction reports and 2000 SARs per month; about 2.5 percent of the latter are referred to law enforcement authorities for investigation.

The Central Bank has established the Departamento de Combate a Ilícitos Cambiais e Financeiros (Department to Combat Exchange and Financial Crimes, or DECIF) to implement anti-money laundering policy, examine entities under the supervision of the Central Bank to ensure compliance with suspicious transaction reporting, and forward information on the suspect and the nature of the transaction to the COAF. In 2005, DECIF brought on-line a national computerized registry of all current accounts (e.g., checking accounts) in the country. A 2005 change in regulations governing foreign exchange transactions requires that banks must report identifying data on both parties for all foreign exchange transactions and money remittances, regardless of the amount of the transaction.

The GOB has institutionalized its national strategy for combating money laundering, holding its fourth annual high-level planning and evaluation session in December 2006. The strategy aims to advance six strategic goals: improve coordination of disparate federal and state level anti-money laundering efforts, utilize computerized databases and public registries to facilitate the fight against money laundering, evaluate and improve existing mechanisms to combat money laundering, increase international cooperation to fight money laundering and recover assets, promote an anti-money laundering culture, and prevent money laundering before it occurs. Given the GOB's emphasis on and need for fighting corruption, the main goal for 2006 was the introduction of requirements for banks to more closely monitor accounts belonging to politically exposed persons (PEPs) for patterns of suspicious transactions. The national anti-money laundering strategy has put in place more regular coordination and clarified the division of labor among various federal agencies involved in combating money laundering.

The GOB has reported substantial growth in the number of money laundering investigations, trials and convictions since 2003. The annual number of investigations grew from 198 in 2003 to 310 in 2004, 449 in 2005, and 625 in the first three quarters of 2006. These investigations led to 26 trials in 2003, 74 in 2004, 75 in 2005, and 41 in the first three quarters of 2006, while convictions ranged from 172 in 2003 to 87 in 2004, 183 in 2005 and 866 in 2006 to date. These numbers represent a substantial

increase from the 2000 to 2002 period, in which there was an average of 40 new investigations per year and only nine convictions (all in 2002). The GOB credits the creation of specialized money laundering courts, founded in 2003, for the increasing number of successful money laundering prosecutions. Fifteen of these courts have been established in 14 states, including two in Sao Paulo, with each court headed by a judge who receives specialized training in national money laundering legislation. A 2006 national anti-money laundering strategy goal aimed to build on the success of the specialized courts by creating complementary specialized federal police financial crimes units in the same jurisdictions. Another reason for the increased prosecutions was the large number of money laundering cases from the Banestado bank scandal of the late 1990's, which began to move to trial during the 2004-2005 period.

Brazil has a limited ability to employ advanced law enforcement techniques such as undercover operations, controlled delivery, and the use of electronic evidence and task force investigations that are critical to the successful investigation of complex crimes, such as money laundering. Generally, such techniques can be used only for information purposes, and are not admissible in court.

In 2005, the GOB drafted a bill to update its anti-money laundering legislation. If passed, this bill, which has not yet been presented to Congress, would facilitate greater law enforcement access to financial and banking records during investigations, criminalize illicit enrichment, allow administrative freezing of assets, and facilitate prosecutions of money laundering cases by amending the legal definition of money laundering and making it an autonomous offense. The draft law also allows the COAF to receive suspicious transaction reports directly from obligated entities, without their first having to pass through the supervisory bodies such as the Central Bank. The COAF would also be able to request additional information directly from the reporting entities.

Brazil has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets. The COAF and the Ministry of Justice manage these systems jointly. Police authorities and the customs and revenue services are responsible for tracing and seizing assets, and have adequate police powers and resources to perform such activities. The GOB planned to introduce in 2006 a computerized registry of all seized assets to improve tracking and disbursal. The judicial system has the authority to forfeit seized assets, and Brazilian law permits the sharing of forfeited assets with other countries.

Brazil has drafted, but not yet presented to Congress, legislation overhauling Brazil's antiterrorism legislation, including specific provisions criminalizing the financing of terrorism. Passage of this legislation would address a fundamental weakness in Brazil's legislative regime to counter money laundering and terrorism finance. Some GOB officials have declared that the 1983 National Security Act, which was passed under the military dictatorship and contains provisions criminalizing terrorism, could be used to prosecute terrorists or terrorist financiers, should the need arise. However, because of public resistance and the history of the law, it is generally not used in criminal matters. Although terrorist financing is considered to be a predicate offense for money laundering under Law 10.701 of 2003, terrorist financing is not an autonomous crime. There have been no money laundering prosecutions to date in which terrorist financing was a predicate offense, and so it remains to be seen if the financing of terrorism could be contested as an enforceable predicate offense due to the lack of legislation specifically criminalizing it. In 2005, the Ministry of Justice announced plans to require all nonprofit organizations, which the Financial Action Task Force (FATF) has designated as an area of concern with regard to the financing of terrorism, to submit annual reports for the purposes of detecting the abuse of their nonprofit status, including money laundering. These regulations would apply to nongovernmental organizations, churches and charitable organizations.

The GOB has generally responded to U.S. efforts to identify and block terrorist-related funds. Since September 11, 2001, the COAF has run inquiries on hundreds of individuals and entities, and has searched its financial records for entities and individuals on the UNSCR Sanctions Committee's

consolidated list. None of the individuals and entities on the consolidated list has been found to be operating or executing financial transactions in Brazil, and the GOB insists there is no evidence of terrorist financing in Brazil. In November 2003, the GOB extradited Assad Ahmad Barakat, designated by the United States under E.O. 13224 as a Specially Designated Global Terrorist, to Paraguay on charges of tax evasion; he was convicted in May 2004 for tax evasion (Paraguay has not criminalized terrorist financing), and sentenced to six and one-half years in prison.

On December 6, 2006, the U.S. Department of Treasury placed nine individuals and two entities in the Triborder Area that have provided financial or logistical support to Hizballah on its list of Specially Designated Nationals. The nine individuals operate in the Triborder Area and all have provided financial support and other services for Specially Designated Global Terrorist Assad Ahmad Barakat, who was previously designated by the U.S. Treasury in June 2004 for his support to Hizballah leadership. The two entities, Galeria Page and Casa Hamze, are located in Ciudad del Este, Paraguay, and have been used to generate or move terrorist funds. The GOB has publicly disagreed with the designations, stating that the United States has not provided any new information that would prove terrorist financing activity is occurring in the Triborder Area.

Brazil is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, the UN International Convention for the Suppression of the Financing of Terrorism, and the Inter-American Convention on Terrorism. Brazil is a member of the Financial Action Task Force (FATF), was a founding member of the Financial Action Task Force Against Money Laundering in South America (GAFISUD), and held the GAFISUD presidency in 2006. Brazil is also a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The COAF has been a member of the Egmont Group of financial intelligence units since 1999. In February 2001, the Mutual Legal Assistance Treaty between Brazil and the United States entered into force, and a bilateral Customs Mutual Assistance Agreement, which was signed in 2002, entered into force in 2005. Using the Customs Agreement framework, the GOB and U.S. Immigration and Customs Enforcement in 2006 established a trade transparency unit (TTU) to detect money laundering via trade transactions. The GOB also participates in the "3 Plus 1" Security Group (formerly the Counter-Terrorism Dialogue) between the United States and the Triborder Area countries.

The Government of Brazil should criminalize terrorist financing as an autonomous offense. In order to continue to successfully combat money laundering and other financial crimes, Brazil should also develop legislation to regulate the sectors in which money laundering is an emerging issue. Brazil should enact and implement legislation to provide for the effective use of advanced law enforcement techniques, in order to provide its investigators and prosecutors with more advanced tools to tackle sophisticated organizations that engage in money laundering, financial crimes, and terrorist financing. Brazil should also enforce currency controls and cross-border reporting requirements, particularly in the Triborder region. Additionally, Brazil and its financial intelligence unit, the Conselho de Controle de Actividades Financieras (COAF), must continue to fight against corruption and ensure the enforcement of existing anti-money laundering laws.

## British Virgin Islands

The British Virgin Islands (BVI) is a Caribbean overseas territory of the United Kingdom (UK). The BVI remains vulnerable to money laundering, primarily due to its financial services industry. The BVI has approximately 11 banks, 2,023 mutual funds with 448 licensed mutual fund managers/administrators, 312 local and captive insurance companies, 1,000 registered vessels, 90 licensed general trust companies, and reportedly 61,000 international business companies (IBCs)—an extraordinary diminution of some 483,000 IBCs reportedly registered in the BVI in 2004.

The Financial Services Commission (FSC) is the independent regulatory authority responsible for the licensing and supervision of regulated entities, which include banking and fiduciary businesses, investment businesses, insolvency services, insurance companies, and company management and registration businesses. Money remitters, however, are not subject to licensing or supervision. The FSC is also responsible for on-site inspections of these entities. The FSC cooperates with its foreign counterparts and law enforcement agencies. In 2000, the Information Assistance (Financial Services) Act (IAFSA) was enacted to increase the scope of cooperation between the BVI's regulators and regulators from other countries.

According to the International Business Companies Act of 1984, IBCs registered in the BVI cannot engage in business with BVI residents, provide registered offices or agent facilities for BVI-incorporated companies, or own an interest in real property located in the BVI (except for office leases). All IBCs must be registered in the BVI by a registered agent, and the IBC or the registered agent must maintain an office in the BVI. The BVI has approximately 90 registered agents that are licensed by the FSC. The process for registering banks, trust companies, and insurers is governed by legislation that requires detailed documentation, such as a business plan and vetting by the appropriate supervisor within the FSC. Registered agents must verify the identities of their clients.

The Proceeds of Criminal Conduct Act of 1997 expands predicate offenses for money laundering to all criminal conduct, and allows the BVI Court to grant confiscation orders against those convicted of an offense or who have benefited from criminal conduct. Although procedures exist for the freezing and confiscation of assets linked to criminal activity, including money laundering and terrorist financing, the procedures for the forfeiture of assets that are not directly linked to narcotics-related crimes are unclear.

The Proceeds of Criminal Conduct Act also created a financial intelligence unit (FIU). The Financial Investigation Agency Act 2003 reorganized and renamed the FIU, now called the Financial Investigation Agency (FIA). The FIA, generally referred to as the Reporting Authority, is responsible for the collection, analysis, and dissemination of financial information.

The Joint Anti-Money Laundering Coordinating Committee (JAMLCC) coordinates all anti-money laundering initiatives in BVI. The JAMLCC is a broad-based, multi-disciplinary body comprised of private and public sector representatives. The Committee has drafted Guidance Notes based on those of the UK and Guernsey. On December 29, 2000, the Anti-Money Laundering Code of Practice of 1999 (AMLCP) entered into force. The AMLCP establishes procedures to identify suspicious transactions and report them to the FIA. Obligated entities are protected from liability for reporting suspicious transactions. The AMLCP also requires covered entities to create a clearly defined reporting chain for employees to follow when reporting suspicious transactions, and to appoint a reporting officer to receive these reports. The reporting officer must conduct an initial inquiry into the suspicious transaction and report it to the authorities, if sufficient suspicion remains. Failure to report could result in criminal liability.

The United Kingdom's Terrorism (United Nations Measures) (Overseas Territories) Order 2001 and the Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002 extend to the BVI. The Afghanistan (United Nations Sanctions) (Overseas Territories) Order 2001 and the Al-Qaida and Taliban (United Nations Measures) (Overseas Territories) Order 2002 also apply to the BVI. However, the BVI has not specifically criminalized the financing of terrorism.

The BVI is a member of the Caribbean Financial Action Task Force (CFATF). The BVI is subject to the 1988 UN Drug Convention and, as a British Overseas Territory, has implemented measures in accordance with this convention and the UN Convention against Transnational Organized Crime. Application of the U.S.-UK Mutual Legal Assistance Treaty concerning the Cayman Islands was extended to the BVI in 1990. The Financial Investigation Agency is a member of the Egmont Group.

The Government of the British Virgin Islands should continue to strengthen its anti-money laundering regime by fully implementing its programs and legislation. The BVI should also extend the provisions of its anti-money laundering and counterterrorist financing to a wider range of entities, including money remitters. The BVI should establish the financing of terrorism as an autonomous offense.

## Bulgaria

Bulgaria is neither considered an important regional financial center nor an offshore financial center. Its significance in terms of money laundering stems from its geographical position, its well-developed financial sector relative to other Balkan countries, and its lax regulatory control. Although Bulgaria is a major transit point for drugs into Western Europe, it is unknown whether drug trafficking constitutes the primary generator of criminal proceeds and subsequent money laundering in Bulgaria. Financial crimes, including fraud schemes of all types, smuggling of persons and commodities, and other organized crime offenses also generate significant proceeds susceptible to money laundering. Bank and credit card fraud remains a serious problem. Tax fraud is also prevalent. The sources for money laundered in Bulgaria likely derive from both domestic and international criminal activity. Organized crime groups operate very openly in Bulgaria. There have been significant physical assaults on Bulgarian public officials as well as journalists who challenge organized crime operations. Smuggling remains a problem in Bulgaria and is sustained by ties with the financial system. While counterfeiting of currency, negotiable instruments, and identity documents has historically been a serious problem in Bulgaria, joint activities of the Bulgarian government and the U.S. Secret Service have contributed to a decline in counterfeiting in recent years. There has been no indication that Bulgarian financial institutions engage in narcotics-related currency transactions involving significant amounts of U.S. currency or otherwise affecting the United States.

Since 2003, the operation of duty free shops has been targeted by the Ministry of Finance (MOF) as part of its efforts to address the gray economy and the smuggling of excise goods. Duty free shops play a major role in cigarette smuggling in Bulgaria, as well as smuggling of alcohol, and to a lesser extent perfume and other luxury goods. Attempts by the MOF to close down shops operating in Bulgaria have been unsuccessful, in part due to political opposition within the ruling coalition. The focus of the Government of Bulgaria (GOB) has been on the duty free shops used to violate customs and tax regimes. The duty free shops may be used to facilitate other crimes, including financial crimes. Credible allegations have linked many duty free shops in Bulgaria to organized crime interests involved in fuel smuggling, forced prostitution, the illicit drug trade, and human trafficking. There is no indication, however, of links between duty free shops or free trade areas and terrorist financing. The MOF's Customs Agency and General Tax Directorate have supervisory authority over the duty free shops. According to these authorities, reported revenues and expenses by the shops have clearly included unlawful activities in addition to duty free trade. Good procedures for identifying unlawful activity are lacking. For example, MOF inspections have revealed that it is practically impossible to monitor whether customers at the numerous duty free shops have actually crossed an international border.

Article 253 of the Bulgarian Penal Code criminalizes money laundering. The 2006 amendments increase penalties (including in cases of conspiracy and abuse of office), clarify that predicate crimes committed outside Bulgaria can support a money laundering charge brought in Bulgaria, and allow prosecution on money laundering charges without first obtaining a conviction for the predicate crime. Article 253 criminalizes money laundering related to all crimes; as such, drug-trafficking is but one of many recognized predicate offenses

The Law on Measures against Money Laundering (LMML), adopted in 1998 and amended most recently in 2006, is the legislative backbone of Bulgaria's anti-money laundering regime. Bulgaria has strict and wide-ranging banking, tax, and commercial secrecy laws that limit the dissemination of

financial information absent the issuance of a court order. While the financial intelligence unit (FIU) is not bound by the secrecy provisions, they apply to all other government institutions and are often cited as an impediment to law enforcement functions. In an effort to lessen the impact of secrecy laws on law enforcement functions, in 2006 the GOB issued amendments to both the LMML and the Law on Credit Institutions. The amendments to the Law on Credit Institutions facilitated the investigation and prosecution of financial crimes by giving the Prosecutor General the right to request financial information from banks without a court order in cases involving money laundering and organized crime.

Banks and the 29 other reporting entities under the LMML are required to apply "know your customer" (KYC) standards. Since 2003, all reporting entities are required to ask for the source of funds in any transaction greater than $19,000 or foreign exchange transactions greater than $6,500. Reporting entities are also required to notify the FIA of any cash payment greater $19,000.

The LMML obligates financial institutions to a five-year record keeping requirement and provides a "safe harbor" to reporting entities. Penal Code Article 253B was enacted in 2004 to establish criminal liability for noncompliance with LMML requirements. Although case law remains weak, when it was assessed in September 2003 for purposes of EU accession, Bulgaria's anti-money laundering legislation was determined to be in full compliance with all EU standards.

The Financial Intelligence Agency (FIA) serves as Bulgaria's FIU and is located within the Ministry of Finance. The LMML guarantees the independence of the FIA director, allows the agency to perform onsite compliance inspections, and authorizes it to obtain information without a court order, share all information with law enforcement, and receive reports of suspected terrorism financing. The agency has a supervisor within the MOF who oversees the activities of the FIA. However, the supervisor is prohibited by law from issuing operational commands. The FIA remains handicapped technologically, but it is working on improving its databases to improve analytical efficiency.

The FIA is an administrative unit and does not participate in criminal investigations. In 2006, the Ministry of the Interior (MOI), the Prosecutor's Office, and the FIA established new procedures for closer cooperation when following leads contained in a suspicious transaction report (STR). The FIA forwards reports to the Prosecutor, and sends to the MOI a copy of each. The MOI is subsequently required to produce a report on the enforcement potential of the case within 30 days of receipt.

Between January and November 2006, the FIA received 310 STRs, on transactions totaling $175 million, and 134,241 currency transaction reports (CTRs). On the basis of the forwarded reports, 276 cases were opened, 74 cases were referred to the Supreme Prosecutor's Office of Cassation, and 207 cases were referred to the Ministry of Interior. The FIA forwarded 32 reports to supervisory authorities for administrative action.

A May 2006 report from the European Union (EU) regarding the status of Bulgaria's application for admission to the EU called Bulgaria's enforcement of anti-money laundering provisions an area of "serious concern," requiring "urgent action". This issue was one of several, resulting in a potential delay of entry date into the EU. In response, Bulgaria's Parliament tightened the LMML with further amendments. The 2006 LMML amendments expanded the definition of money laundering and the list of reporting entities; allowed FIA to obtain bank records without a court order; outlawed anonymous bank accounts; expanded the definition of "currency"; and required the disclosure of source for currency exported from the country. Overall, these amendments are expected to strengthen the investigative capabilities of both the FIA and law enforcement when dealing with money laundering cases. Experts view this legislation as comprehensive and in line with international standards. All financial sectors are considered susceptible to money laundering and subject to anti-money laundering regulations. Under the LMML, 30 categories of entities, including lawyers, real estate agents, auctioneers, tax consultants, and security exchange operators, are required to file suspicious transactions reports. To date, only the banking sector has substantially complied with the law's filing

requirement. Lower rates of reporting compliance by exchange bureaus, casinos, and other nonbank financial institutions can be attributed to a number of factors, including a lack of understanding of or respect for legal requirements, lack of inspection resources, and the general absence of effective regulatory control over the nonbank financial sector.

Although money laundering has been pursued in court cases, there had not been a conviction until recently. In October 2006, the courts rendered the country's first two convictions for money laundering. On October 9, the Ruse District Court sentenced a defendant to 11 months in prison and three years of probation after he admitted to receiving a 350,000 Euro (approximately $464,000) bank transfer in 2004. The FIA initiated the investigation. In another case, the Varna District Court sentenced a defendant to an eighteen-month imprisonment and a fine of 4,000 BGL (approximately $2,600) for the predicate crime of drug trafficking and distribution

There are few, if any, indications of terrorist financing connected with Bulgaria. Article 108a of the Penal Code criminalizes terrorism and terrorist financing. Article 253 of the Criminal Code qualifies terrorist acts and financing as predicate crimes under the "all crimes" approach to money laundering. In February 2003, the GOB enacted the Law on Measures Against Terrorist Financing (LMATF), which links counterterrorism measures with financial intelligence and compels all covered entities to report a suspicion of terrorism financing or pay a penalty of approximately $15,000. The law is consistent with Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing and authorizes the FIA to use its resources and financial intelligence to combat terrorism financing along with money laundering.

Under the LMATF, the GOB may freeze the assets of a suspected terrorist for 45 days. Key players in the process of asset freezing and seizing, as prescribed in existing law, include the MOI, MOF (including the FIA), Council of Ministers, Supreme Administrative Court, Sofia City Court, and the Prosecutor General. The FIA and the Bulgarian National Bank circulate the names of suspected terrorists and terrorist organizations, as found on the UNSCR 1267 Sanctions Committee's consolidated list, as well as the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224, and those designated by the relevant EU authorities. To date, no suspected terrorist assets have been identified, frozen, or seized by Bulgarian authorities. In 2005, a joint task force comprised of representatives from the FIA and the National Security Service was established to identify possible terrorist financing activities and terrorist supporters.

There are no reported initiatives underway to address alternative remittance systems. Although they may operate there, Bulgarian officials have not officially acknowledged their existence. In general, regulatory controls over non-bank financial institutions are still lacking, with some of those institutions engaging in banking activities absent any regulatory oversight. Similarly, exchange bureaus are subject to minimal regulatory oversight, and some anecdotal evidence suggests that charitable and nonprofit legal status is occasionally used to conceal money laundering. In 2006, the GOB somewhat strengthened its nonbank financial institution oversight by instituting compliance checks on casinos and exchange offices. Between January and October 2006, the FIA inspected 23 casinos and 548 exchange offices, imposing fines in 15 cases.

The Bulgarian Penal Code provides legal mechanisms for forfeiting assets (including substitute assets in money laundering cases) and instrumentalities. Both the money laundering and the terrorist financing laws include provisions for identifying, tracing, and freezing assets related to money laundering or the financing of terrorism. A new criminal asset forfeiture law, targeted at confiscation of illegally acquired property, came into effect in March 2005. The law permits forfeiture proceedings to be initiated against property valued in excess of approximately $36,000 if the owner of the property is the subject of criminal prosecution for enumerated crimes (terrorism, drug trafficking, human trafficking, money laundering, bribery, major tax fraud, and organizing, leading, or participating in a criminal group) and a reasonable assumption can be made that the property was acquired through

criminal activity. The law requires the establishment of a criminal assets identification commission that has the authority to institute criminal asset identification procedures, as well as request from the court both preliminary injunctions and ultimately the forfeiture of assets.

The United States does not have a mutual legal assistance treaty with Bulgaria. However, the 2005 ratification of the UN Convention Against Transnational Organized Crime by the U.S. established an MLAT-type relationship between the two countries, and the U.S.-EU Agreement on Mutual Legal Assistance, once ratified, will lay the basis for a more comprehensive MLAT relationship. Currently, the FIA has bilateral memoranda of understanding (MOU) regarding information exchange relating to money laundering with 29 countries. Negotiations with three more states are currently in progress. The FIA is authorized by law to exchange financial intelligence on the basis of reciprocity without the need of an MOU. Between January and October 2006, the FIA sent 285 requests for information to foreign FIUs and received 65 requests for assistance from foreign FIUs. Bulgaria has also entered into an intergovernmental agreement with Russia that promotes anti-money laundering cooperation.

Bulgaria participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The FIA is a member of the Egmont Group and participates actively in information sharing with foreign counterparts. Bulgaria is a party to the 1988 UN Drug Convention; the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the UN Convention against Transnational Organized Crime; the UN International Convention for the Suppression of the Financing of Terrorism; and the UN Convention against Corruption.

In 2005, the Bulgarian Parliament passed amendments to the 1969 law on Administrative Violations and Penalties, which establishes the liability of legal persons (companies) for crimes committed by their employees. This measure is in accordance with international standards and allows the GOB to implement its obligations under a number of international agreements, including: the OECD Anti-bribery Convention, the European Council Convention on Corruption, the UN International Convention for the Suppression of Terrorist Financing, and the UN Convention against Transnational Organized Crime. Under the amendments, Bulgaria also aligns itself with the provisions of the EU Convention on the Protection of the Communities' Financial Interests and its Protocols, a requirement for EU accession.

Although Bulgaria has enacted legislative changes consistent with international anti-money laundering standards, lax enforcement remains problematic. The GOB must take steps to improve and tighten its regulatory and reporting regime, particularly with regard to nonbank sectors. The GOB should improve the consistency of its customs reporting enforcement and should also establish procedures to identify the origin of funds used to acquire banks and businesses during privatization. The GOB needs to provide sufficient resources to the Financial Intelligence Agency so that the agency can incorporate technological improvements. The FIA should also continue to improve inter-agency cooperation in order to ensure effective implementation of Bulgaria's anti-money laundering regime and to improve prosecutorial effectiveness in money laundering cases.

## Burma

Burma, a major drug-producing country, has taken steps to strengthen its anti-money laundering regulatory regime in 2005 and 2006. The country's economy remains dominated by state-owned entities, including the military. Agriculture and extractive industries, including natural gas, mining, logging and fishing provide the major portion of national income, with heavy industry and manufacturing playing minor roles. The steps Burma has taken over the past two years have reduced vulnerability to drug money laundering in the banking sector. However, with an underdeveloped financial sector and large volume of informal trade, Burma remains a country where there is significant risk of drug money being funneled into commercial enterprises and infrastructure

investment. The government has addressed most key areas of concern identified by the international community by implementing some anti-money laundering measures, and in October 2006, the Financial Action Task Force (FATF) removed Burma from the FATF list of Non-Cooperative Countries and Territories (NCCT).

The United States maintains other sanctions on trade, investment and financial transactions with Burma under Executive Order 13047 (May 1997), Executive Order 13310 (July 2003); the Narcotics Control Trade Act, the Foreign Assistance Act, the International Financial Institutions Act, the Export-Import Bank Act, the Export Administration Act, the Customs and Trade Act, the Tariff Act (19 USC 1307), and the 2003 Burmese Freedom and Democracy Act (P.L. 108-61).

Burma enacted a "Control of Money Laundering Law" in 2002. It also established the Central Control Board of Money Laundering in 2002 and a financial intelligence unit (FIU) in 2003. It set a threshold amount for reporting cash transactions by banks and real estate firms, albeit at a fairly high level of 100 million kyat (approximately $75,000). Burma adopted a "Mutual Assistance in Criminal Matters Law" in 2004, added fraud to the list of predicate offenses, and established legal penalties for leaking information about suspicious transaction reports. The GOB's 2004 anti-money laundering measures amended regulations instituted in 2003 that set out 11 predicate offenses, including narcotics activities, human trafficking, arms trafficking, cyber-crime, and "offenses committed by acts of terrorism," among others. The 2003 regulations, expanded in 2006, require banks, customs officials and the legal and real estate sectors to file suspicious transaction reports (STRs) and impose severe penalties for noncompliance.

The GOB established a Department Against Transnational Crime in 2004. Its mandate includes anti-money laundering activities. It is staffed by police officers and support personnel from banks, customs, budget, and other relevant government departments. In response to a February 2005 FATF request, the Government of Burma submitted an anti-money laundering implementation plan and produced regular progress reports in 2005 and 2006. In 2005, the government also increased the size of the FIU to 11 permanent members, plus 20 support staff. In August 2005, the Central Bank of Myanmar issued guidelines for on-site bank inspections and required reports that review banks' compliance with AML legislation. Since then, the Central Bank has sent teams to instruct bank staff on the new guidelines and to inspect banking operations for compliance.

The United States maintains the separate countermeasures it adopted against Burma in 2004, which found the jurisdiction of Burma and two private Burmese banks, Myanmar Mayflower Bank and Asia Wealth Bank, to be "of primary money laundering concern." These countermeasures prohibited U.S. banks from establishing or maintaining correspondent or payable-through accounts in the United States for or on behalf of Myanmar Mayflower and Asia Wealth Bank and, with narrow exceptions, for all other Burmese banks. These rules were issued by the Financial Crimes Enforcement Network within the Treasury Department, pursuant to Section 311 of the 2001 USA PATRIOT Act.

Myanmar Mayflower and Asia Wealth Bank had been linked directly to narcotics trafficking organizations in Southeast Asia. In March 2005, following GOB investigations, the Central Bank of Myanmar revoked the operating licenses of Myanmar Mayflower Bank and Asia Wealth Bank, citing infractions of the Financial Institutions of Myanmar Law. The two banks no longer exist. In August 2005, the Government of Burma also revoked the license of Myanmar Universal Bank (MUB), and convicted the bank's chairman under both the Narcotics and Psychotropic Substances Law, and the Control of Money Laundering Law. Under the money laundering charge, the court sentenced him to one 10-year and one unlimited term in prison and seized his and his bank's assets.

Burma also remains under a separate 2002 U.S. Treasury Department advisory stating that U.S. financial institutions should give enhanced scrutiny to all financial transactions related to Burma. The Section 311 rules complement the 2003 Burmese Freedom and Democracy Act (renewed in July 2006) and Executive Order 13310 (July 2003), which impose additional economic sanctions on Burma

following the regime's May 2003 attack on a peaceful convoy of the country's pro-democracy opposition led by Nobel laureate Aung San Suu Kyi. The sanctions prohibit the import of most Burmese-produced goods into the United States, ban the provision of financial services to Burma by any U.S. persons, freeze assets of the ruling junta and other Burmese institutions, and expand U.S. visa restrictions to include managers of state-owned enterprises as well as senior government officials and family members associated with the regime. In August 2005, the U.S. Treasury amended and reissued the Burmese Sanctions Regulations in their entirety to implement the 2003 Executive Order that placed these sanctions on Burma.

Burma became a member of the Asia/Pacific Group on Money Laundering in January 2006, and is a party to the 1988 UN Drug Convention. Over the past several years, the Government of Burma has expanded its counternarcotics cooperation with other states. The GOB has bilateral drug control agreements with India, Bangladesh, Vietnam, Russia, Laos, the Philippines, China, and Thailand. These agreements include cooperation on drug-related money laundering issues. In July 2005, the Myanmar Central Control Board signed an MOU with Thailand's Anti-Money Laundering Office governing the exchange of information and financial intelligence. The government signed a cooperative MOU with Indonesia's FIU in November 2006.

Burma is a party to the UN Convention against Transnational Organized Crime and ratified the UN Convention on Corruption in December 2005 and the UN International Convention for the Suppression of the Financing of Terrorism in August 2006. Burma signed the ASEAN Multilateral Assistance in Criminal Matters Agreement in January 2006.

The GOB now has in place a framework to allow mutual legal assistance and cooperation with overseas jurisdictions in the investigation and prosecution of serious crimes. To fully implement a strong anti-money laundering/counterterrorist financing regime, Burma must provide the necessary resources to administrative and judicial authorities who supervise the financial sector, so they can apply and enforce the government's regulations to fight money laundering successfully. Burma must also continue to improve its enforcement of the new regulations and oversight of its banking system, and end all government policies that facilitate the investment of drug money into the legitimate economy. It also must monitor more carefully the widespread use of informal remittance or "hundi" networks, and should criminalize the funding of terrorism.

## Cambodia

Cambodia is neither an important regional financial center nor an offshore financial center. While there have been no verified reports of money laundering in Cambodia, it serves as a transit route for heroin from Burma and Laos to international drug markets such as Vietnam, mainland China, Taiwan, and Australia. Its very weak anti-money laundering regime, a cash-based economy with an active informal banking system, porous borders with attendant smuggling, casinos, and widespread official corruption also contribute to money laundering in Cambodia.

The National Bank of Cambodia (NBC) has made some strides in recent years by beginning to regulate the small official banking sector, but other nonbank financial institutions, such as casinos, remain outside its jurisdiction. While the Ministry of Interior has legal responsibility for oversight of the casinos and providing security, it exerts little supervision. In July 2006, the Council of Ministers approved draft legislation that would criminalize money laundering and the financing of terrorism and forwarded the bill to the National Assembly for ratification. However, the National Assembly had not taken action as of mid-November 2006.

Cambodia's banking sector is small but expanding, with fifteen general commercial banks, five commercial banks, and numerous microfinance institutions. However, overall lending and banking activity remains limited as most Cambodians keep their assets outside the banking system. Economists

note that while a typical country would have a bank deposit to GDP ratio of roughly 60 percent, Cambodia's ratio is only 16 percent—low even by developing economy standards. Cambodia's banking system is highly consolidated, with two banks—Canadia Bank and Foreign Trade Bank (FTB)—accounting for more than 40 percent of all bank deposits. Moreover, during the October 2005 privatization of the Foreign Trade Bank, Canadia gained a 46 percent share in FTB, further strengthening Canadia's large role in the financial services sector.

The NBC has regulatory responsibility for the banking sector. The NBC regularly audits individual banks (that have a small numbers of transactions and deposits) to ensure compliance with laws and regulations. There is a standing requirement for banks to declare transactions over 42,000,000 riel (approximately $10,000). The NBC says its audits reveal that this requirement is generally followed. While there are no reports to indicate that banking institutions themselves are knowingly engaged in money laundering, government audits would likely not be a sufficient deterrent to money laundering through most Cambodian banks. However, questions from correspondent banks about large transfers and Cambodia's relatively high 0.15 percent tax on financial transactions might discourage money laundering within the formal banking sector

A more likely route for larger scale money laundering in Cambodia is through informal banking activities or business activities. Neither the NBC nor any other Cambodian entity is responsible for identifying or regulating these informal financial networks or activities such as casinos. The vulnerability of Cambodia's financial sector is further exacerbated because of the intersection of the casino and banking interests with four companies having whole or partial shares in both banks and casinos,

With increased political stability and the gradual return of normalcy in Cambodia after decades of war and instability, bank deposits have risen by 12-15 percent per year since 2000 and the financial sector shows some signs of deepening as domestic business activity continues to increase in the handful of urban areas. Foreign direct investment, while limited, is increasing after several years of contraction.

Reportedly, there is no apparent increase in the extent of financial crime over the past year. There is a significant black market in Cambodia for smuggled goods, including drugs but reportedly no evidence that smuggling is funded primarily by drug proceeds, including the importing and local production of the methamphetamine (ATS). Most of the smuggling that takes place is intended to circumvent official duties and taxes and involves items such as fuel, alcohol and cigarettes. Some government officials and their private sector associates have a significant amount of control over the smuggling trade and its proceeds. Cambodia has a cash-based and dollar-based economy, and the smuggling trade is usually conducted in dollars. Such proceeds are rarely transferred through the banking system or other financial institutions. Instead, they are readily converted into land, housing, luxury goods or other forms of property. It is also relatively easy to hand-carry cash into and out of Cambodia.

Neither money laundering (except in connection with drug trafficking) nor terrorism financing is a specific criminal offense in Cambodia at this time. The NBC does not yet have the authority to apply anti-money laundering controls to nonbank financial institutions such as casinos or other intermediaries, such as lawyers or accountants. However, this authority is included in draft anti-money laundering legislation.

The major nonbank financial institutions in Cambodia are the casinos, where foreigners are allowed to gamble but Cambodians are not. The regulation of casinos falls under the jurisdiction of the Ministry of Interior, although the Ministry of Economy and Finance issues casino licenses. The Interior Ministry stations a few officials at each casino on a 24-hour basis. It does not appear that Interior Ministry staff at the casinos exercise any actual supervision over casino financial operations.

There are currently more than 20 licensed casinos in Cambodia, with a few more either under construction or applying for a license. Most are located along Cambodia's borders with Thailand or

Vietnam. There is one large casino in Phnom Penh that has avoided the regulation that all casinos be at least 200 kilometers from the capital city. Casino patrons placing small bets simply hand-carry their money across borders, while others use either bank transfers or junket operators. There is no effective oversight of cash movement into or out of Cambodia. Cambodian casinos have accounts with major Thai or Vietnamese banks and patrons can wire large amounts of money to one of these foreign accounts. After a quick phone call to verify the transfer, the Cambodian casino issues the appropriate amount in chips. Casinos also work with junket operators who, despite their name, only facilitate money transfers and do not serve as travel or tour operators. Players deposit money with a junket operator in Vietnam or Thailand, the casino verifies the deposit and issues chips to the player—typically up to double the amount of the deposit. After the gambling session ends, the junket operator then has 15 days to pay the casino for any losses. Because the junket operator is responsible for collecting from the patrons, casinos see little need to investigate the patron's ability to cover his/her potential debt or the source of his/her wealth.

In 1996, Cambodia criminalized money laundering related to narcotics trafficking through the Law on Drug Control. In 1999, the government also passed the Law on Banking and Financial Institutions. These two laws provide the legal basis for the NBC to regulate the financial sector. The NBC also uses the authority of these laws to issue and enforce new regulations. The most recent regulation, dated October 21, 2002, is specifically aimed at money laundering. The decree established standardized procedures for the identification of money laundering at banking and financial institutions. In October 2003, the NBC issued a circular to assist banks in identifying suspicious transactions and in fulfilling "Know Your Customer" best practices, though no suspicious transactions have yet been reported to the NBC. In addition to the NBC, the Ministries of Economy and Finance, Interior, Foreign Affairs, and Justice also are involved in anti-money laundering matters.

The 1996 and 1999 laws include provisions for customer identification, suspicious transaction reporting, and the creation of an Anti-Money Laundering Commission (AMLC) under the Prime Minister's Office. The composition and functions of the AMLC have not yet been fully promulgated by additional decrees. A Sub-Decree on the composition and duties of AMLC has been drafted but is unlikely to be passed until passage of the new anti-money laundering legislation. The NBC currently performs many of the AMLC's intended functions. The 1999 Law on Banking and Financial Institutions imposed new capital requirements on financial institutions, increasing them from $5 million to $13.5 million. Commercial banks must also maintain 20 percent of their capital on deposit with the NBC as reserves.

In 2005, Cambodia became a party to the 1988 UN Drug Convention, the UN Convention Against Transnational Organized Crime, and the UN Convention for the Suppression of the Financing of Terrorism. No existing laws currently address terrorism financing, although it is specifically addressed in the draft law on money laundering. The NBC does circulate to financial institutions the list of individuals and entities included on the UNSCR 1267 Sanction Committee's consolidated list, and reviews the banks for compliance in maintaining this list and reporting any related activity. To date, there have been no reports of designated terrorist financiers using the Cambodian banking sector. Should sanctioned individuals or entities be discovered using a financial institution in Cambodia, the NBC has the legal authority to freeze the assets but not to seize them.

In June 2004, Cambodia joined the Asia/Pacific Group on Money Laundering (APG), a Financial Action Task Force (FATF) regional body. The APG conducts mutual evaluations of members' anti-money laundering and terrorism financing efforts. An APG evaluation of Cambodia originally scheduled for 2005 has been delayed at the government's request until early 2007 to permit passage of the draft Law on the Prevention of Money Laundering and Financing of Terrorism before the evaluation. According to the draft law, a new financial intelligence unit (FIU) will be placed under the control of the NBC with a permanent secretariat working under the authority of a board composed of the senior representatives from Ministries of Economy and Finance, Justice, and Interior.

A Working Group, including the NBC and the Ministries of Economy and Finance, Interior, and Justice, the National Authority for Combating Drugs was formed on November 26, 2003 to draft anti-money laundering legislation that meets international standards. The Working Group's draft legislation and action plan to fight money laundering and the financing of terrorism envisions the following: criminalizing money laundering and the financing of terrorism (including in free trade zones); ratification of all relevant UN conventions; regulating and controlling NGOs; reducing the use of cash and encouraging the use of the formal banking system for financial transactions; enhancing the effectiveness of bank supervision; ensuring the use of national ID cards as official documents for customer identification; and regulating casinos and the gambling industry. The draft legislation also addresses preventive obligations related to customer due diligence, record keeping, internal controls, reporting of suspicious transactions, and setting up an FIU to receive, analyze and disseminate information and to supervise compliance with all relevant laws and regulations. While the draft anti-money laundering legislation was being considered, the NBC planned to issue a series of regulations that have the force of law (parkas) and that will criminalize money laundering and terrorism financing, as well as update existing financial rules and regulations. However, these prakas were not issued due to concerns that they would set stricter rules than would be included in the new legislation

Making progress on the long-awaited draft anti-money laundering legislation and becoming a party to the UN conventions on drugs, organized crime, and terrorism financing are positive steps. The Government of Cambodia should pass the draft anti-money laundering and counterterrorist financing legislation as soon as possible. Questions remain regarding the government's ability to implement and enforce the measures once they are in place. To this end, Cambodia should engage fully with the Asia/Pacific Group on Money Laundering and implement all recommendations of its upcoming mutual evaluation in order to develop a comprehensive viable anti-money laundering/counterterrorist financing regime that comports with international standards.

## Canada

With $1.5 billion in trade crossing the border each day, both the United States and Canadian governments are concerned about the criminal cross-border movements of currency, particularly the illicit proceeds of drug trafficking. Significant amounts of U.S. currency derived through illegal drug sales in the United States are subsequently laundered through the Canadian financial system each year.

The Government of Canada (GOC) enacted the Proceeds of Crime (Money Laundering) Act in 2000 to assist in the detection and deterrence of money laundering, facilitate the investigation and prosecution of money laundering, and create the financial intelligence unit (FIU). The Proceeds of Crime (Money Laundering) Act was amended in December 2001 to become the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). The list of predicate money laundering offenses was expanded to cover all indictable offenses, including terrorism and the trafficking of persons. In addition to amending the PCMLTFA, the 2001 reforms made it a crime under the Canadian Criminal Code to knowingly collect or give funds to carry out terrorism, denied or removed charitable status from those supporting terrorism and facilitated freezing and seizing their assets.

The PCMLTFA created a mandatory reporting system for suspected terrorist property, suspicious financial transactions, large cash transactions, large international electronic funds transfers, and cross-border movements of currency and monetary instruments totaling 10,000 Canadian dollars (approximately $9,000) or more. Failure to report cross-border movements of currency and monetary instruments could result in seizure of funds or penalties ranging from approximately $225 to $4,500. Failure to file a suspicious transaction report (STR) could result in up to five years' imprisonment, a fine of approximately $1.8 million, or both. The law protects those filing suspicious transaction reports

from civil and criminal prosecution. There has been no apparent decline in deposits made with Canadian financial institutions as a result of Canada's revised laws and regulations.

Canada's FIU, the Financial Transactions and Reports Analysis Center of Canada (FINTRAC), was established in July 2001. FINTRAC is an independent agency within the GOC that receives and analyzes reports from financial institutions and other financial intermediaries (such as money service businesses, casinos, accountants, and real estate agents) as mandated by the PCMLTFA, and makes disclosures to law enforcement and intelligence agencies. Guidelines explaining the PCMLTFA and its requirements were published by FINTRAC in 2002; further additions were made in 2003. The guidelines provide an overview of FINTRAC's mandate and responsibilities, and include background information about money laundering and terrorist financing, including their international scope and nature. The guidelines also provide an outline of the Canadian legislative requirements for a compliance regime, record keeping, client identification and reporting transactions.

FINTRAC currently has over 37.4 million financial transaction reports contained within its database. During 2005-2006, FINTRAC received nearly 15 million reports from reporting entities. FINTRAC produced a total of 168 case disclosures in 2005-2006, totaling approximately $4.5 billion, more than double the value of the previous year. The case disclosures represented nearly $4.3 billion in transactions of suspected money laundering, and $230 million in transactions of suspected terrorist financing activity and other threats to the security of Canada. Thirty-two domestic law enforcement agencies and 10 foreign counterparts have received disclosures from FINTRAC.

FINTRAC has the authority to negotiate information exchange agreements with foreign FIUs. It has signed over 35 memoranda of understanding (MOUs) to establish the terms and conditions to share intelligence with FIUs—including an MOU with FinCEN, the FIU of the United States—and is negotiating several other memoranda. Canada has longstanding agreements with the United States on law enforcement cooperation, including treaties on extradition and mutual legal assistance. Canada has provisions for sharing seized assets, and exercises them regularly.

The PCMLTFA enables Canadian authorities to deter, disable, identify, prosecute, convict, and punish terrorist groups. As of June 2002, STRs are required on financial transactions suspected of involving the commission of a terrorist financing offense. The PCMLTFA expanded FINTRAC's mandate to include counterterrorist financing and to allow disclosure to the Canadian Security Intelligence Service of information related to financial transactions relevant to threats to the security of Canada. The GOC has also listed and searched financial records for suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list. There are currently more than 500 individuals and entities associated with terrorist activities designated by the GOC. This designation effectively freezes their assets and prohibits fund-raising on their behalf in Canada.

In a 2004 report to Parliament, Canada's Auditor General stated that "privacy concerns restrict FINTRAC's ability to disclose intelligence to the Police, and as a result, law enforcement and security agencies usually find that the information they receive is too limited to justify launching investigations." United States law enforcement officials have echoed concerns that Canadian privacy laws and the high standard of proof required by Canadian courts inhibit the full sharing of timely and meaningful intelligence on suspicious financial transactions. Such intelligence may be critical to investigating and prosecuting international terrorist financing or major money laundering investigations. Recently, concern has focused on the inability of United States and Canadian law enforcement officers to exchange information promptly concerning suspicious sums of money found in the possession of individuals attempting to cross the United States-Canadian border. A 2005 Memorandum of Understanding on exchange of cross-border currency declarations expanded the extremely narrow disclosure policy. However, the scope of the exchange remains restrictive.

In October 2006, Bill C-25 was introduced to Parliament to amend the PCMLTFA. Bill C-25 is designed to make Canada's anti-money laundering and antiterrorist financing regime consistent with

the Financial Action Task Force (FATF) recommendations. Canada will undergo a FATF Mutual Evaluation in early 2007. The new legislation will expand the coverage of Canada's anti-money laundering and antiterrorist financing regime by bringing additional business sectors, including lawyers and dealers in precious metals and stones, under the authority of the PCMLTFA and related regulations. Bill C-25 also mandates that FINTRAC create a national registry for money service businesses and establish a system of administrative monetary penalties. The proposed measures will improve compliance with the reporting, record keeping and client identification provisions of the PCMLTFA. The Bill permits FINTRAC to include additional information in the intelligence product that FINTRAC can disclose to law enforcement and national security agencies, as recommended in the 2004 Auditor General's Report. Bill C-25 received final Parliamentary approval in December 2006

In addition to new legislation, the GOC is undertaking other initiatives to bolster its ability to combat money laundering and terrorist financing. In May 2006, the GOC announced that it had added in the 2006 budget approximately $58 million over the next two years for FINTRAC, the Royal Canadian Mounted Police (RCMP), and the Department of Justice. The new funding will increase the number of RCMP officers working in the antiterrorist financing and anti-money laundering units; increase the capabilities of the Canada Border Services Agency (CBSA) to detect unreported currency at airports and border crossings; enable Canada's Department of Justice to handle the expanding litigation workload that will result from increasing the enforcement resources of other GOC agencies; and ensure that FINTRAC can better analyze transactions reports and monitor compliance of unregulated financial sectors such as money remitters.

Canada is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the 1988 UN Drug Convention, and the UN Convention against Transnational Organized Crime. The GOC has also ratified the Organization of American States (OAS) Inter-American Convention on Mutual Assistance in Criminal Matters, the Inter-American Convention against Terrorism, and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. The GOC has signed, but not yet ratified, the UN Convention against Corruption.

Canada is a member of the Financial Action Task Force and assumed the FATF Presidency for a one-year term beginning in July 2006. Canada became a member of the Asia/Pacific Group on Money Laundering (APG) in July 2006. Canada also belongs to the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. FINTRAC became a member of the Egmont Group in 2002. In June 2006, Toronto was selected as the permanent location of the Secretariat of the Egmont Group. The GOC will contribute approximately $4.5 million over the next five years to help establish the Secretariat

Canada has demonstrated a strong commitment to combat money laundering and terrorist financing both domestically and internationally. In 2006, the GOC made strides in enhancing its anti-money laundering regime and reducing its vulnerability to money laundering and terrorist financing, and should continue to expand these efforts in 2007. The GOC should consider taking the necessary steps to permit FINTRAC to disclose timely and meaningful information to Canadian law enforcement agencies on suspicious financial transactions. Were the GOC to do so, both Canada and the United States might see a significant decrease in the illegal cross-border movement of cash and narcotics, as well as a significant increase in successful prosecutions and convictions.

## Cayman Islands

The Cayman Islands, a United Kingdom (UK) Caribbean overseas territory, continues to make strides in strengthening its anti-money laundering program. However, the islands remain vulnerable to money laundering due to their significant offshore sector. The Cayman Islands is home to a well-developed offshore financial center that provides a wide range of services, including banking, structured finance,

investment funds, various types of trusts, and company formation and management. At the end of 2006, The Cayman Islands Monetary Authority (CIMA) reported over 450 banks and trust companies, 8,143 funds, 740 captive insurance companies, and 62,572 exempt companies licensed or registered in the Cayman Islands.

The CIMA is responsible for the licensing, regulation and supervision of the Cayman Islands' financial industry, which includes banks, trust companies, investment funds, fund administrators, insurance companies, insurance managers, money service businesses, and corporate service providers. The CIMA received independence to issue and revoke licenses and enforce regulations through the Monetary Authority Law 2003. Supervision of licensees is carried out through on-site and off-site examinations, which include monitoring for anti-money laundering and counter financing terrorism compliance. A 2001 amendment to The Companies Law institutes a custodial system in order to immobilize bearer shares. There are no shell banks in the Cayman Islands. The CIMA has a statutory function under the Monetary Authority Law to provide assistance to overseas regulatory authorities, and is able to share information with such authorities with or without a memorandum of understanding (MOU). In June 2005, the CIMA signed an MOU with the U.S. Securities and Exchange Commission (SEC). The CIMA also has several other MOUs with regulatory counterparts in a number of countries, including Brazil, Canada, Jamaica and Panama.

Money laundering regulations entered into force in late 2000 that specify employee training, record-keeping, and "know your customer" (KYC) identification requirements for financial institutions and certain financial services providers. The regulations specifically cover individuals who establish a new business relationship, engage in one-time transactions over 15,000 Cayman Islands dollars (approximately $18,000), or who may be engaging in money laundering.

The Misuse of Drugs Law criminalized narcotics-related money laundering. The Proceeds of Criminal Conduct Law (PCCL) criminalized money laundering related to all other serious crimes. The PCCL provides for the offense of money laundering where a person or business has engaged in criminal conduct or has benefited from criminal conduct; tax offenses are not included. The PCCL requires mandatory reporting of suspicious transactions, and makes failure to report a suspicious transaction a criminal offense that could result in fines or imprisonment. There is no threshold amount for the reporting of suspicious activity. A suspicious activity report (SAR) must be reported once it is known or suspected that a transaction may be related to money laundering or terrorism financing.

Established under PCCL (Amendment) Law 2003, the Financial Reporting Authority (FRA) replaces the former financial intelligence unit of the Cayman Islands. The FRA began operations on January 12, 2004. FRA staff consists of a director, a legal advisor, a senior accountant, a senior analyst, a junior analyst, and an administrative officer. The FRA is a separate civilian authority governed by the Anti-Money Laundering Steering Group (AMLSG), which is chaired by the Attorney General. Other members of the AMLSG include the Financial Secretary, the Managing Director of the Cayman Islands Monetary Authority, the Commissioner of Police, the Solicitor General, and the Collector of Customs. The FRA is responsible for, among other things, receiving, analyzing, and disseminating disclosures of financial information regarding proceeds or suspected proceeds, including those relating to the financing of terrorism. From June 2005 to June 2006, the FRA developed 221 new cases, which consisted of suspicious activity reports received from reporting entities as well as information requests from foreign FIUs.

The Cayman Islands is subject to the United Kingdom Terrorism (United Nations Measure) (Overseas Territories) Order 2001. The Cayman Islands criminalized terrorist financing through the passage of the Terrorism Bill 2003, which extends criminal liability to the use of money or property for the purposes of terrorism. It also contains a specific provision on money laundering related to terrorist financing. However, the United Kingdom has yet to extend the application of the International Convention for the Suppression of the Financing of Terrorism to the Cayman Islands.

In 1986, the United States and the United Kingdom signed a Treaty concerning the Cayman Islands relating to Mutual Legal Assistance in Criminal Matters. By a 1994 exchange of notes, Article 16 of that treaty has been deemed to authorize asset sharing between the United States and the Cayman Islands. The Cayman Islands is a member of the Caribbean Financial Action Task Force (CFATF), and the FRA is a member of the Egmont Group.

The Cayman Islands should continue its efforts to implement its anti-money laundering regime.

## Chile

Chile's large and well-developed banking and financial sector stands out as one of the strongest in the region. With rapidly increasing trade and currency flows, the government is actively seeking to turn Chile into a global financial center. Some Chilean officials believe these increased flows do not, at the same time, create a significant money laundering threat. However, the combination of Chile's irregular regulatory oversight and favorable financial reputation might make it attractive to criminal organizations and other potential money launderers, particularly in the northern free trade zone and in the money exchange house sector. Money laundering in Chile appears to be primarily narcotics-related.

Money laundering in Chile is criminalized under Law 19.366 of January 1995, Law 19.913 of December 2003, and Law 20.119 of August 2006. Prior to the approval of Law 19.913, Chile's anti-money laundering program was based solely on Law 19.366, which criminalized only narcotics-related money laundering activities. The law required only voluntary reporting of suspicious or unusual financial transactions by banks and offered no "safe harbor" provisions protecting banks from civil liability. As a result, the rate of reporting of such transactions was extremely low. Law 19.366 gave only the Council for the Defense of the State (Consejo de Defensa del Estado, or CDE) authority to conduct narcotics-related money laundering investigations. The Department for the Control of Illicit Drugs within the CDE functioned as Chile's financial intelligence unit (FIU) until a new FIU with broader powers (the Unidad de Análisis Financiero, or UAF) was created under Law 19.913. The new UAF is part of the Ministry of Finance.

Law 19.913 went into effect on December 18, 2003. Under Law 19.913, predicate offenses for money laundering are expanded to include (in addition to narcotics trafficking) terrorism in any form (financing terrorist acts or groups), illegal arms trafficking, fraud, corruption, child prostitution and pornography, and adult prostitution.

Law 19.913 requires mandatory reporting of suspicious transactions by banks and financial institutions, financial leasing companies, general funds-managing companies and investment funds-managing companies, the Foreign Investment Committee, money exchange firms and other entities authorized to receive foreign currencies, firms that carry out factoring operations, credit card issuers and operators, securities companies, money transfer and transportation companies, stock exchanges, stock exchange brokers, securities agents, insurance companies, mutual funds managing companies, forwards and options markets operators, tax-free zones' legal representatives, casinos, gambling houses and horse tracks, customs general agents, auction houses, realtors and companies engaged in the land development business, notaries and registrars. However, the law does not specify the parameters for determining suspicious activity. Each entity independently decides what constitutes irregularities in financial transactions. Under Law 20.119, which went into effect on August 31, 2006, pension funds and sports clubs are now also subject to reporting requirements.

In addition to reporting suspicious transactions, Law 19.913 also requires that obligated entities maintain registries of cash transactions that exceed 450 unidades de fomento (UF) (approximately $12,000). All cash transaction reports (CTRs) contained in the internal registries must be sent to the UAF at least once a year, or more frequently at the request of the UAF. The Chilean tax service

(Servicio de Impuestos Internos) issued a regulation, Resolution 120, requiring all banks, exchange houses and money remitters to report all transactions exceeding $10,000 sent to or received from foreign countries. The physical transportation of funds exceeding UF 450 into or out of Chile must be reported to Customs, which then files a report with the UAF. These reports are sent to the UAF on a daily basis. However, Customs and other law enforcement agencies are not legally empowered to seize or otherwise stop the movement of funds, and the entry or exit of these funds is not subject to taxation.

On August 31, 2006, Law 20.119 went into effect. This law restores several powers of the UAF that had been previously removed from the original draft of Law 19.913 by Chile's constitutional tribunal, including the UAF's ability to impose sanctions for noncompliance. Law 19.913 did not grant any government or supervisory entity the authority to impose penalties for partial or noncompliance, resulting in only voluntary-not compulsory-reporting of suspicious or unusual financial transactions. Additionally, while the UAF could previously only exact information from institutions which had already submitted suspicious transaction reports (STRs), it can now demand information to pursue leads received through any official avenue, be it an STR, a cash transaction report (CTR), cross border report, or a request for information from a foreign FIU. The UAF may also now access any government information (police, taxes, etc.) not covered by secrecy or privacy laws. Article 154, paragraph 1 of the Chilean General Banking Law establishes bank secrecy on all types of bank deposits, and prohibits the institution from providing background information related to such operations to any individual except the person making the deposit, or to a third party expressly authorized by the client. Records covered by secrecy protection can now be obtained by the UAF with permission from a judge, usually obtained within 48 hours. One deficiency of Law 19.913 that was not corrected with the passage of Law 20.119, however, is the lack of a definition of "suspicious activity" in the reporting requirements for nonbank and nonfinancial institutions.

The UAF began operating in April 2004, and began receiving STRs from reporting entities in May 2004. In 2005 the UAF received an average of 13 STRs per month. The average number per month increased to 19 in 2006. The average breakdown per month was 14.6 STRs from banks, 1.6 from exchange houses, 1.8 from money transfer and courier services, and 1 from other obliged institutions. By October 1, 2006, the UAF had received 170 STRs, 131 of which were from banks. STRs from nonbank institutions comprise about 23 percent of the total STRs received by October 2006.

Cash transaction reports are also requested regularly by the UAF. In May 2005 money exchange houses were instructed by the UAF to submit CTRs every three months. In September 2005, banks were instructed to submit CTRs every three months. In March 2006 the rest of the obliged institutions were instructed to submit CTRs every 3 months, though some specific institutions without a high amount of cash transactions (e.g. notaries) may submit every 6 months. In all cases, institutions must report CTRs dating from May 2004, when the obligation to record cash transactions over 450 UF went into effect. The UAF received approximately 1000 CTRs in 2006.

The UAF has two STR forms—one for banks, and the other for nonbanking institutions. As of November 2006 it became possible to submit STRs and CTRs through the Internet. Suspicious transaction reports from financial institutions can also be received electronically, via a system known as SINACOFI (Sistema Nacional de Comunicaciones Financieras) that is used by banks to distribute encrypted information among themselves and the Superintendence of Banks.

Banks in Chile are supervised formally by the Superintendence of Banks and Financial Institutions (SBIF) and informally by the Association of Banks and Financial Institutions. Banks are obliged to abide by "know-your-customer" standards and other money laundering controls for checking accounts. However, savings accounts are not subject to the same compliance standards. Only a limited number of banks rigorously apply money laundering controls to noncurrent accounts. Stock brokerages, securities firms and insurance companies are under the supervision and regulation of the Superintendence of Securities and Insurance. The Superintendence of Securities and Insurance is an

autonomous corporate agency affiliated to the Chilean Government through the Ministry of Finance, and enforces compliance with all laws, regulations, by-laws and other provisions governing the operation of securities, stock exchange and insurance companies in Chile.

In March 2006, the SBIF developed new rules establishing the norms and standards for banks and financial institutions (including leasing companies, securities companies and agents, factoring companies, insurance companies, stock brokerages, general funds-managing companies, and investment fund-managing companies) to prevent money laundering and terrorism financing. These rules also require financial institutions to keep records with updated background information on their clients throughout the period of their commercial relationship. Additionally, Chilean law requires that banks and financial institutions maintain records for a minimum of five years on any case reported to the UAF.

One weakness in Chile's efforts to combat money laundering is that nonbank financial institutions, such as money exchange houses and cash couriers, currently do not fall under the supervision of any regulatory body for compliance with anti-money laundering and counterterrorist financing standards. In Santiago alone there are approximately 55 exchange houses, many of which do not record or share with other exchange houses any information about their customers. Discerning suspicious activity is more difficult without due diligence on clients or good record-keeping. An attempt to self-regulate was undertaken by six exchange houses that formed the Chamber of Exchange Houses and Couriers in 1999, and registered with the Ministry of Economy. However, the Association dissolved in October 2006. Exchange houses as well as cash courier companies are also requested by Law 19,913 to report any suspicious transaction and any cash transaction over UF 450 to the UAF. The lack of supervision, definition of "suspicious activity," and a harmonized system to keep record of daily transactions diminishes useful reporting to the UAF, and undermines the effectiveness of the system. This sector appears particularly vulnerable to abuse by money launderers.

Chile's gaming industry falls under the supervision of the Superintendence of Casinos, which is in charge of drafting regulations about casino facilities, and the administration, operation and proper development of the industry. There are currently seven casinos located throughout the country. The SCJ has oversight powers over the industry but no law enforcement or regulatory authority. Under Law 19.995, the Superintendence of Casinos granted authorization for 10 casinos to operate in Chile after participating in an international and domestic bidding process to assign 17 permits during 2005 and 2006. Seven of these permits are still under a revision process; it is expected that their permits will be issued by December 2006. In total, 22 casinos, including the 7 already in operation, will be fully operating by 2008 under the oversight authority of the Superintendence of Casinos. There is currently no legal framework for supervising the money moving through the gaming industry. However, Article 3 of Law 19.913 requires casinos to report to the UAF any transaction in cash for over UF 450 (approximately $12,000) and any suspicious operation, to present them with balance sheets, to provide financial reports, to keep historical accounting records, and to designate a compliance official to relate to the UAF. Currently the Superintendence of Casinos has focused on analyzing the integrity of the bidding companies. They have investigated these companies with the support of domestic and international police and financial institutions.

When the UAF determines that an account or a case requires further investigation, it passes the information to the Public Ministry (the public prosecutor's office). The Public Ministry has been responsible for receiving and investigating all cases from the UAF since June 2005 (prior to June 2005, all cases deemed by the UAF to require further investigation were sent to the Consejo de Defensa del Estado or CDE). Of the 170 STRs received as of October 1, 2006, the UAF sent 27 of to the Public Ministry for further investigation. Under Law 20.119, the Public Ministry has the ability to request that a judge issue an order to freeze assets under investigation, and can also, with the authorization of a judge, lift bank secrecy provisions to gain account information if the account is

directly related to an ongoing case. The Public Ministry has up to two years to complete an investigation and begin prosecution.

The Chilean investigative police (PICH) work in conjunction with the Public Ministry on money laundering investigations. The PICH investigators appear to be very competent and well-trained, but complain about insufficient access to information. Chilean law prohibits the UAF from giving information directly to law enforcement, and allows the sharing of information only with the Public Ministry and foreign FIUs. Currently PICH and other law enforcement must request financial information from the Public Ministry, which in turn requests it from the UAF. The police and prosecutors have expressed concern about the lack of timely access to information.

No money laundering cases have been prosecuted to date in Chile. The first such case is scheduled to go to trial in July 2007. The case was brought to the attention of the Chilean authorities when local press ran articles about a Chilean arrested in Germany for drug trafficking. The articles also detailed the suspect's business dealings in Chile, which led to the decision to investigate the case in Chile as well. Through cooperation with the German government, the Government of Chile (GOC) discovered the suspect's brother had been laundering money in Chile tied with the drug trafficking in Germany. The Public Ministry and PICH continue to cooperate with U.S. and regional law enforcement in money laundering investigations.

Two free trade zones exist in Chile, in Punta Arenas and Iquique. The Iquique free trade zone, the larger of the two, also has an extension in Arica, near Chile's border with Peru. The physical borders of the free trade zone are porous and largely uncontrolled. There are indications that money laundering schemes are rampant in the Iquique-Arica free trade zone. Chilean resources to combat this issue are extremely limited. Police investigative efforts suggest possible criminal links between Iquique and the Triborder Area (Brazil, Paraguay and Argentina), involving both terrorist financing and money laundering. In December 2006, the U.S. Department of Treasury designated nine individuals and two businesses in the Triborder Area that have provided financial and logistical support to Hizballah; one of those individuals, Hatim Ahmad Barakat, had traveled to Chile to collect funds intended for Hizballah, and was reported to be a significant shareholder in at least two businesses in Iquique. Hatim Barakat has been in prison in Paraguay since 2004.

Terrorist financing in Chile is criminalized under Law 18.314 and Law. 19.906. Law 19.906 went into effect in November 2003 and modifies Law 18.314, in order to sanction more efficiently terrorist financing in conformity with the UN International Convention for the Suppression of the Financing of Terrorism. Under Law 19.906, financing a terrorist act and the provision (directly or indirectly) of funds to a terrorist organization are punishable by five to ten years in prison. The Superintendence of Banks circulates the UNSCR 1267 Sanctions Committee's consolidated list to banks and financial institutions.

No terrorist assets belonging to individuals or groups named on the list have been identified to date in Chile. If assets were found, the legal process that would be followed to freeze and seize them is still unclear. Law 19.913 contains provisions which allow prosecutors to request that assets be frozen, based on a suspected connection to criminal activity. Government officials have stated that Chilean law is currently sufficient to effectively freeze and seize terrorist assets. However, the new provisions for freezing assets are based on provisions in the drug law, which at times have been interpreted narrowly by the courts. While assets have been frozen during two drug investigations, it is unclear how the new system would operate for a terrorist financing case. The Ministry of National Property currently oversees forfeited assets, and proceeds from the sale of forfeited assets are passed directly to CONACE, the National Drug Control Commission, to fund drug abuse prevention and rehabilitation programs. Under the present law, forfeiture is possible for real property and financial assets. Civil forfeiture is not permitted.

Chile is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the Inter-American Convention on Terrorism. On September 13, 2006, the GOC ratified the UN Convention against Corruption. Chile is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the South American Financial Action Task Force on Money Laundering (GAFISUD). GAFISUD conducted a mutual evaluation of Chile's efforts to combat money laundering in September 2006. The CDE became a member of the Egmont Group of financial intelligence units in 1997, and the UAF was vetted by the Egmont Group in October 2004 to replace the CDE. The UAF was nominated in 2006 to serve as the representative for the Americas on the Egmont Committee. The UAF has signed memoranda of understanding (MOUs) for the exchange of financial information with the United States FIU and FIUS of 25 other jurisdictions. Chile is also in the process of establishing MOUs with Belgium, British Virgin Islands, Gibraltar, Holland, Italy, Luxembourg, St. Kits and Nevis, United Kingdom, and Venezuela.

In the establishment of the UAF, the Government of Chile has created an FIU that meets the Egmont Group's definition of a financial intelligence unit. Chile took a major step in addressing some limitations of the UAF in the passage of Law 20.119. The new law should strengthen the ability of the UAF to aggressively track potential money laundering, but is too new at this point to determine if that has yet occurred. There continues to be no government oversight or standardization of most nonbank financial institutions, and anecdotal evidence that money laundering is occurring in money exchange houses makes this lack of oversight an issue of greater concern. The laws and institutions in Chile which combat money laundering are relatively new, and the system is still developing. The Public Ministry, the investigative police (PICH), and the uniformed national police (Carabineros) are trying to find effective ways to work together, but there are complaints of limited access to information and inter-agency conflict. Chile should take all necessary steps to ensure sufficient government oversight of nonfinancial institutions, aggressive action on the part of the UAF and other key agencies, and inter-agency cooperation, so that Chile is capable of effectively combating money laundering and terrorist financing.

## China, People's Republic of

Money laundering remains a major concern as China restructures its economy. A more sophisticated and globally connected financial system in one of the world's fastest growing economies will offer significantly more opportunities for money laundering activity. Most money laundering cases currently under investigation involve funds obtained from corruption and bribery. Narcotics trafficking, smuggling, alien smuggling, counterfeiting, fraud and other financial crimes remain major sources of laundered funds. Proceeds of tax evasion, recycled through offshore companies, often return to China disguised as foreign investment, and as such, receive tax benefits. Continuing speculation following the July 2005 adjustment of the renminbi (RMB) exchange rate system also fueled illicit capital flows into China throughout 2006. Hong Kong-registered companies figure prominently in schemes to transfer corruption proceeds and in tax evasion recycling schemes. The International Monetary Fund estimated that money laundering in China may total as much as $24 billion annually.

On October 31, 2006, the National People's Congress passed a new Anti-Money Laundering Law, which came into effect January 1, 2007. This new law broadens the scope of existing anti-money laundering regulations to include any institution involved in money laundering. It mandates that financial and some nonfinancial institutions maintain records on accounts and transactions, and that they report large and suspicious transactions. The law more firmly establishes the Central Bank's authority over national anti-money laundering efforts, but does not clearly define "nonfinancial institutions" for this purpose. The law also increases the number of predicate offenses for money

laundering, to include fraud, bribery, and embezzlement. China has taken steps to enhance its anti-money laundering regime. After conducting studies on how to strengthen the system, the People's Bank of China (PBC) and the State Administration of Foreign Exchange (SAFE) promulgated a series of anti-money laundering regulatory measures for financial institutions. These include: Regulations on Real Name System for Individual Savings Accounts, Rules on Bank Account Management, Rules on Management of Foreign Exchange Accounts, Circular on Management of Large Cash Payments, and Rules on Registration and Recording of Large Cash Payments.

Additional regulations were announced in 2006 aimed at further strengthening China's anti-money laundering efforts. In December, 2006, China's central bank issued two new regulations—"Rules for Anti-Money Laundering by Financial Institutions", which will come into effect January 1, 2007, and "Administrative Rules for Reporting of Large-Value and Suspicious Transactions by Financial Institutions", which will come into effect March 1, 2007. Together, these regulations revise earlier PBC regulations implemented in March, 2004. The new regulations will require all financial institutions—including securities, trust companies and futures dealers—to report large and suspicious transactions. Any cash deposit or withdrawal of over RMB 200,000 or foreign-currency withdrawal of $10,000 in one business day must be reported within five days if electronically or within 10 days in writing to the PBC. Money transfers between companies exceeding RMB 2 million or US$200,000 in one day or between an individual and a company greater than RMB 500,000 or US$100,000 must also be reported. The regulations are slated for implementation between January and March of 2007.

These regulations enhance a prior March 2004 PBC regulation entitled "Regulations on Anti-Money Laundering for Financial Institutions," which strengthens the regulatory framework under which Chinese banks and financial institutions must treat potentially illicit financial activity. The regulation effectively requires Chinese financial institutions to take responsibility for suspicious transactions, instructing them to create their own anti-money laundering mechanisms. Banks in particular were required to report suspicious foreign exchange transactions—but not all transactions, as in the new regulations—of more than $10,000 per person in a single transaction or cumulatively per day in cash, or noncash foreign exchange transactions of $100,000 per individual or $500,000 per entity either in a single transaction or cumulatively per day. Under the regulation, banks were further required to submit monthly reports to the PBC outlining suspicious activity and to retain transaction records for five years. Banks which failed to report on time can be fined up to the equivalent of approximately $3,600. Under the December 2006 regulations, financial institutions that fail to meet reporting requirements in a timely manner can have their licenses or business operations suspended.

On April 12, 2006, the PBC proposed a series of measures aimed at curbing money laundering in the insurance, banking and securities sectors. The proposed regulations, which were circulated for comment until May 8 2006, would require institutions to report all "block transactions"-defined as transactions worth more than 50,000 RMB (approximately $6,241) or $10,000 per day-to the PBC's anti-money laundering center for review. The proposal would also define the following as "block transactions": noncash transactions of more than 200,000 RMB or $100,000 per day and transactions between institutional accounts amounting to more than 1 million RMB or $500,000 per day. However, the current status of these proposed regulations is unclear.

The new Anti-Money Laundering Law passed in 2006 builds on China's 1997 Criminal Code. The 2006 law amended Article 191 of the Criminal Code to criminalize money laundering for seven predicate offenses, expanded from the original three predicate offenses, which were narcotics trafficking, organized crime, and smuggling. In 2001, Article 191 was amended to add terrorism as a fourth predicate offense. Article 191, however, still does not encompass all of the twenty designated categories of offenses identified by the Financial Action Task Force (FATF), even after passage of the 2006 law. Additionally, the 2006 law amended Article 312 to make it an offense to launder the proceeds of any crime through a variety of means. Article 312 criminalizes complicity in concealing

the proceeds of criminal activity. Article 174 criminalizes the establishment of an unauthorized financial institution.

While official scrutiny of cross-border transactions is improving, the Chinese Government is also moving to loosen capital-account restrictions. For example, as of January 1, 2005, travelers can take up to 20,000 RMB (approximately $2,500) or, in foreign currency, up to $5,000, into or out of the country on each trip, up from 3,000 RMB (approximately $360) previously. New provisions allowing the use of RMB in Hong Kong have also created new loopholes for money laundering activity. Authorities are also allowing greater use of domestic, RMB-denominated, credit cards overseas. Such cards can now be used in Hong Kong, Macau, Singapore, Thailand, and South Korea. To address online fraud, the PBC tightened regulations governing electronic payments. In 2005, the Central Bank announced new rules that consumers could not make online purchases of more than RMB 1,000 (approximately $124) in any single transaction or more than 5,000 RMB (approximately $620) in a single day. Enterprises are limited to electronic payments of no more than 50,000 RMB (approximately $6,200) in a single day.

In 2003, the Chinese Government established a new banking regulator, the China Banking Regulatory Commission (CBRC), which assumed substantial authority over the regulation of the banking system. The CBRC has been authorized to supervise and regulate banks, asset management companies, trust and investment companies, and other deposit-taking institutions, with the aim of ensuring the soundness of the banking industry. One of its regulatory objectives is to combat financial crimes. However, primary authority for anti-money laundering efforts remains with the PBC, the country's Central Bank, while enforcement is handled by the Ministry of Public Security.

In 2004, the PBC established a central national Financial Intelligence Unit (FIU), the China Anti-Money Laundering Monitoring and Analysis Center, whose function is to collect, analyze and disseminate suspicious transaction reports and currency transaction reports. This move was an important accomplishment of the Anti-Money Laundering Strategy Team tasked with developing the legal and regulatory framework for countering money laundering in the banking sector. According to the China Anti-Money Laundering Monitoring and Analysis Center, 683 suspicious money laundering cases had been reported to the police by the end of 2005. They involved 137.8 billion yuan ($17.2 billion) and over one billion U.S. dollars.

In September 2002, SAFE adopted a new system to supervise foreign exchange accounts more efficiently. The new system allowed for immediate electronic supervision of transactions, collection of statistical data, and reporting and analysis of transactions. A separate Anti-Money Laundering Bureau was established at the PBC in late 2003 to coordinate all anti-money laundering efforts in the PBC and among other agencies, and to supervise the creation of the new FIU.

In spite of China's efforts, institutional obstacles and rivalries between financial and law-enforcement authorities continue to hamper Chinese anti-money laundering work and other financial law enforcement. Continuing efforts by some Chinese officials to strengthen the relatively weak legal framework under which money laundering offenses are currently prosecuted in the Chinese criminal code have yet to bear fruit. Anti-money laundering efforts are hampered by the prevalence of counterfeit identity documents and cash transactions conducted by underground banks, which in some regions reportedly account for over one-third of lending activities. China has increased efforts in recent years to crack down on such underground lending institutions. In December, 2006, authorities in Shanghai announced they were investigating the country's largest-ever money laundering case, totaling about five billion yuan ($633 million). The case involves underground banks, according to Chinese media reports.

To remedy information deficiencies, the PBC launched a national credit-information system in early 2005. The system officially began operation in January 2006. Although still very limited, this system will allow banks to have access to information on individuals as well as on corporate entities. PBC

rules obligate financial institutions to perform customer identification, due diligence and record keeping. SAFE implemented a new regulation on March 1, 2004 requiring nonresidents, including those from Hong Kong, Macau, Taiwan, and Chinese passport holders residing outside mainland China, to verify their real names when opening bank accounts with more than $5,000.

China supports international efforts to counter the financing of terrorism. Terrorist financing is now a criminal offense in China, and the government has the authority to identify, freeze, and seize terrorist financial assets. Subsequent to the September 11, 2001, terrorist attacks in the United States, Chinese authorities began to actively participate in U.S. and international efforts to identify, track, and intercept terrorist finances, specifically through implementation of United Nations Security Council counterterrorist financing resolutions.

China's concerns with terrorist financing are generally regional, focused mainly on the western Xinjiang Uighur Autonomous Region. Chinese law enforcement authorities have noted that China's cash-based economy, combined with its robust cross-border trade, has led to many difficult-to-track large cash transactions. There is concern that groups may be exploiting such cash transactions in an attempt to bypass China's financial enforcement agencies. While China is proficient in tracing formal foreign currency transactions, the large size of the informal economy-estimated by the Chinese Government at about 10 percent of the formal economy, but quite possibly larger-makes monitoring of China's cash-based economy very difficult.

China is a party to the 1988 UN Drug Convention, and the UN Convention against Transnational Organized Crime. China became as party to UN Convention against Corruption, and to the UN International Convention for the Suppression of the Financing of Terrorism in 2006.

China has signed mutual legal assistance treaties with 24 countries. The United States and China signed a mutual legal assistance agreement (MLAA) in June 2000, the first major bilateral law enforcement agreement between the countries. The MLAA entered into force in March 2001 and provides a basis for exchanging records in connection with narcotics and other criminal investigations and proceedings. The United States and China cooperate and discuss money laundering and other enforcement issues under the auspices of the U.S.-China Joint Liaison Group's (JLG) subgroup on law enforcement cooperation. JLG meetings are held annually in either Washington, D.C., or Beijing. In addition, the United States and China have established a Working Group on Counterterrorism that meets on a regular basis. The PRC has established similar working groups with other countries as well.

In late 2004, China joined the Eurasian Group (EAG), a Financial Action Task Force (FATF)-style regional group which includes Russia, Belarus, China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. In January 2005, China became an observer to the FATF and seeks to become a full member of the FATF. The FATF conducted a mutual evaluation of China in November, 2006.

In 2005, China's CBRC signed a memorandum of understanding with the Philippine Central Bank, Bangko Sentral ng Pilipinas, to share information on suspected money laundering activity. China's financial intelligence unit, the China Anti-Money Laundering Monitoring and Analysis Center, also signed its first MOU with a foreign counterpart at the end of 2005, with South Korea's FIU, allowing the two to exchange information related to money laundering, terrorist financing and other criminal financial activity.

The Chinese Government should continue to build upon the substantive actions taken in recent years to develop a viable anti-money laundering/terrorist financing regime consistent with international standards. Important steps will include expanding its list of predicate crimes to include all serious crimes and continuing to develop a regulatory and law enforcement environment designed to prevent and deter money laundering. China should ensure that the FIU is an independent, centralized body with adequate collection, analysis and disseminating authority, including the ability to share with foreign analogs and law enforcement, and that a system of suspicious transaction reporting (STR) is

adequately implemented. It will be important for China's FIU to join the Egmont Group of Financial Intelligence Units as soon as possible to ensure it has access to vital financial information on possible illicit transactions occurring in other jurisdictions. China should provide for criminal penalties for noncompliance with requirements that financial institutions perform customer identification, due diligence, and record keeping. China should also ensure effective implementation of the many regulatory changes it has put in place over the past three years in seeking to build a highly functional anti-money laundering regime.

## Colombia

The Government of Colombia (GOC) is a regional leader in the fight against money laundering. Comprehensive anti-money laundering regulations have allowed the government to refine and improve its ability to combat financial crimes and money laundering. Nevertheless, the laundering of drug money from Colombia's lucrative cocaine and heroin trade continues to penetrate its economy and affect its financial institutions. Although progress has been made in recent years, a complex legal system and limited resources for anti-money laundering programs have constrained the effectiveness of the GOC's efforts. Laundering illicit funds is related to a number of criminal activities (narcotics trafficking, commercial smuggling for tax and import duty evasion, kidnapping for profit, and arms trafficking and terrorism connected to violent paramilitary groups and guerrilla organizations), and is carried out, to a large extent, by officially recognized terrorist organizations. The GOC and U.S. law enforcement agencies are closely monitoring transactions that could disguise terrorist finance activities. The U.S. and Colombia exchange information and cooperation based on Colombia's 1994 ratification of the United Nations Convention against Illicit Trafficking in Narcotics and Psychotropic Substances. This convention extends into most money laundering activities that are the result of Colombia's drug trade.

Colombia's economy is robust and diverse and is fueled by significant export sectors that ship goods such as palm oil, textiles and apparel, flowers, and coffee to the U.S. and beyond. While Colombia is not a regional financial center, the banking sector is mature and well regulated. An increase in financial crimes not related to money laundering or terrorist financing, such as bank fraud, has not been widely seen in Colombia. However, criminal elements have used the banking sector to launder money, under the guise of licit transactions. Money laundering has occurred via trade and the nonbank financial system, especially related to transactions that support the informal or underground economy. Colombian money is also laundered through offshore centers, generally relating to transactions involving drug-related proceeds.

Money launderers in Colombia employ a wide variety of techniques. Money launderers frequently use such alternative laundering methods as the Black Market Peso Exchange and contraband trade to launder the proceeds of illicit funds. Colombia's financial intelligence unit, the Unidad de Información y Análisis Financiero (Financial Information and Analysis Unit, or UIAF) has identified more than ten techniques alone for laundering money via contraband trade. In 2005, the GOC asserted that illicit funds were being laundered by imports of under-valued Chinese manufactured goods via Panama's Colon Free Trade Zone, and implemented specific controls on Panamanian re-exports to Colombia. Panama countered with a complaint to the World Trade Organization (WTO), and eventually the controls were dropped in October 2006. Colombian industry reaction to the decision was negative, reflecting in part the realities of increasing Chinese competition, but as well the very negative impact that laundering via contraband trade has on legitimate businesses.

Colombia also appears to be a significant destination and transit location for bulk shipment of narcotics-related U.S. currency. Local currency exchangers convert narcotics dollars to Colombian pesos and then ship the U.S. currency to Central America and elsewhere for deposit as legitimate exchange house funds that are then reconverted to pesos and repatriated by wire to Colombia. Other

methods include the use of debit cards to draw on financial institutions outside of Colombia and the transfer of funds out of and then back into Colombia by wire through different exchange houses to create the appearance of a legal business or personal transaction. Colombian authorities have also noted increased body smuggling (carrying currency on a person) of U.S. and other foreign currencies and an increase in the number of shell companies operating in Colombia. Pre-paid debit cards, internet banking, and the dollarization of the economy of neighboring Ecuador represent some of the growing challenges to money laundering enforcement in Colombia.

Casinos in Colombia lack adequate regulation and transparency. Free trade zones in some areas of the country present opportunities for smugglers to take advantage of lax customs regulations, or the corruption of low-level officials to move products into the informal economy. Although corruption of government officials remains a problem, it has not been reported as widespread. The GOC has taken steps to ensure the integrity of its most sensitive institutions and senior government officials.

Colombia has broadly criminalized money laundering. In 1995, Colombia established the "legalization and concealment" of criminal assets as a separate criminal offense. Also, in 1997 and 2001, Colombia criminalized the laundering of the proceeds of extortion, illicit enrichment, rebellion, narcotics trafficking, arms trafficking, crimes against the financial system or public administration, and criminal conspiracy. Penalties under the criminal code range from two to six years with possibilities for aggravating enhancements of up to three-quarters of the sentence. Persons who acquire proceeds from drug trafficking are subject to a potential sentence of six to fifteen years, while illicit enrichment convictions carry a sentence of six to ten years. Failure to report money laundering offenses to authorities is itself an offense punishable under the criminal code, with penalties increased in 2002 to imprisonment of two to five years.

Established in 1999 within the Ministry of Finance and Public Credit, the UIAF is widely viewed as a hemispheric leader in efforts to combat money laundering and supplies considerable expertise in organizational design and operations to other financial intelligence units (FIUs) in Central and South America. The UIAF currently has approximately 45 personnel, and a new director took over leadership of the unit in August 2006.

The UIAF has broad authority to access and analyze financial information from public and private entities in Colombia. Obligated entities, which include banks, stock exchanges and brokers, mutual funds, investment funds, export and import intermediaries, credit unions, wire remitters, exchange houses, public agencies and entities that fall under the supervision of the Superintendence of Notaries, are required to report suspicious transaction to the UIAF, and are barred from informing their clients of their reports. Most obligated entities are also required to establish "know-your-customer" provisions. With the exception of exchange houses, obligated entities must report to the UIAF cash transactions over $5,000. Through December 2004, the UIAF had also required exchange houses provide bulk data for all transactions above US$ 700. A change in January 2005 extended this requirement to all financial institutions for bulk data on transfers, remittances and currency transactions, and lowered the threshold transaction value to US$ 200. This considerably broadened the data which UIAF examines, enhancing their analytical coverage.

Financial institutions are required by law to maintain records of account holders and financial transactions for five years. Secrecy laws have not been an impediment to bank cooperation with law enforcement officials, since under Colombian law there is a legal exemption to client confidentiality when a financial institution suspects money laundering activity. Colombia's banks have strict compliance procedures, and work closely with the GOC, other foreign governments and private consultants to ensure system integrity. General negligence laws and criminal fraud provisions ensure the financial sector complies with its responsibilities while protecting consumer rights. Obligated entities are supervised by the Superintendence of Finance, which was created in November 2005 by combining the former Superintendence of Banks and the former Superintendence of Securities into a

single organization. The fusion was generally welcomed as providing more consistent and comprehensive oversight of the financial industry.

Following UIAF's inception in 1999, the number of STRs grew rapidly as financial institutions strived to comply with the reporting requirement, peaking at 13,488 STRs in 2002. The UIAF analysts noted, however, that the quality of reports was lacking, and subsequently began an outreach program to educate reporting institutions on what type of financial activity merited an STR. The quantity of STRs fell to 9,074 in 2005, but UIAF is generally pleased that the overall quality of reporting has improved. Currently, 20 percent of STRs are deemed by UIAF to merit further investigation by their analysis unit, and between five and seven percent of cases are forwarded to an enforcement division for further action. In 2006, 6,120 STRs were filed through the month of October. The prosecutor's office reported 87 successful convictions for money laundering in 2005, and 66 convictions between January and October 2006.

In June 2006, the UIAF inaugurated a new centralized data network connecting 17 governmental entities as well as the banker's association (Asobancaria). The network allows these entities to exchange information online and share their databases in a secure manner, and should facilitate greater cooperation among government agencies in preventing money laundering and other financial crimes. The pilot phase of the project had been made possible by USG financial contributions.

Given past concerns about bulk cash smuggling, in October 2005, the GOC made it illegal to transport more than the equivalent of US$ 10,000 in cash across Colombian borders, inbound or outbound. Such transactions must now be handled through the formal financial system, which is subject to the UIAF reporting requirements. Colombia has criminalized cross-border cash smuggling and defines it as money laundering. In spite of improvements, customs officials are inadequately equipped to detect cross-border currency smuggling. Workers rotate frequently producing inadequately trained staff. In addition, the individual customs officials are held liable for any inspected article that they damage, causing hesitation in conducting thorough inspections. Reportedly, corruption is also a problem, and it has been noted that customs officials lack the proper technical equipment necessary to do their job. The GOC has been slow to make needed changes in this area.

Colombian law provides for both conviction-based and nonconviction based in rem forfeiture, giving it some of the most expansive forfeiture legislation in Latin America. A general criminal forfeiture provision for intentional crimes has existed in Colombian Penal Law since the 1930s. Since then, Colombia has adopted more specific criminal forfeiture provisions in other statutes, including Law 30 of 1986 and Law 333 of 1996; however, procedural and other difficulties led to only limited forfeiture successes, with substantial assets tied up in proceedings for years. In 2002, the GOC enacted Law 793, which repeals Law 333 and establishes new procedures that eliminate interlocutory appeals that prolonged and impeded forfeiture proceedings in the past, imposes strict time limits on proceedings, places obligations on claimants to demonstrate their legitimate interest in property, requires expedited consideration of forfeiture actions by judicial authorities, and establishes a fund for the administration of seized and forfeited assets. The amount of time for challenges was shortened and the focus was moved from the accused to the seized item (cash, jewelry, boat, etc.), placing more burdens on the accused to prove the item was acquired with legitimately obtained resources. Law 785 of 2002 also strengthened the GOC's ability to administer seized and forfeited assets. This statute provides clear authority for the National Drug Directorate (DNE) to conduct interlocutory sales of seized assets and contract with entities for the management of assets. Notably, Law 785 also permits provisional use of seized assets prior to a final forfeiture order, including assets seized prior to the enactment of the new law.

Laws 793 and 785 have helped streamline the asset forfeiture process, resulting in a tenfold increase in sentences. Yet problems remain: concerns about personal liability have discouraged official action in some cases, exceptions in proceedings can still cause cases to drag on for years, and the pace of final

decisions remains slow compared to new seizures. Prosecutors also have limited discretion on assets seizures, and must seize all assets associated with a case, including those of minimal value or those which clearly risk loss under state administration, such as livestock.

In 2006, the Colombian media criticized DNE's asset management, citing losses to the GOC from poor maintenance or even loss of assets under their administration. Prior to the fourth quarter of 2006, only a very limited number of assets were disposed of or transferred to government entities, due to the huge task of managing the assets. At the end of 2006, DNE was managing 75,000 assets, some 75 percent of which were seized before 2002. With limited resources and only 45 staff dedicated to asset management, the DNE must rely on outside contractors to store or manage assets. The GOC has established priorities for the proceeds of disposed assets; however, DNE's management task will only be reduced when the pace of judicial decisions and disposals exceeds new seizures.

The Colombian government has been aggressively pursuing the seizure of assets obtained by drug traffickers through their illicit activities. For the last three years the Sensitive Investigations Unit (SIU) of the Colombian National Police (CNP), in conjunction with U.S. law enforcement and the Colombian Fiscalia (prosecutor's office) have been investigating the Cali and North Valle cartels' business empires under the Rodriguez Orejuela brothers and the Grajales family, respectively. The Cali and Norte Valle cartels, as well as their leaders and associated businesses, are on the U.S. Department of the Treasury Office of Foreign Asset Control (OFAC) list of Specially Designated Narcotics Traffickers (SDNTs), pursuant to Executive Order 12978. Colombian and U.S. law enforcement agencies have cooperated in a series of investigations designed to identify and seize assets either purchased by money gained through illegal drug activity or assets used to launder drug proceeds. These joint actions to apply economic sanctions have gravely affected the Colombian drug cartels' abilities to use many of the financial assets they derived from their narcotics trafficking activities and have assisted the Colombian government in creating cases in order to seize narcotics related assets. Recent seizures include those of the Drogas La Rebaja drug store chain owned by the Rodriguez Orejuela brothers in 2004, and the Grajales' agricultural companies and Casa Estrella department stores in June 2005 and August 2006 respectively.

In September 2006, 28 family members of the Rodriguez-Orejuelas brothers entered into a plea agreement with the United States. Under the terms of the agreement, the family members agreed to forfeit their right, title, and interest in all Rodriguez-Orejuela business entities and other assets worldwide, as well as all assets of any nature in the United States, up to a maximum of $ 2.1 billion in value. Approximately $ 260 million in assets related to this judgment have been identified in Colombia.

Bilateral cooperation between the GOC and the USG remains strong and active. In 2006, several major investigations by DEA and the sensitive investigation unit (SIU) of the Department of Administrative Security (DAS) resulted in arrests and seizures of major money laundering organizations operating between the countries. These include Operation Common Denominator, which led to the arrests of money launderers that utilized the black market peso exchange to launder drug proceeds from the U.S. and Europe, and the seizure of over 17 million euros and 2,000 kilograms of cocaine in Spain; Operation Hoyo Verde, which resulted in 88 arrests for money laundering in the United States, Curacao, the Dominican Republic, Puerto Rico, the Netherlands and Colombia, and the seizure of $ 8.6 million in cash, $ 5.8 million in assets and 100 kilograms of cocaine; and Operation Plata Sucia, which led to 28 money laundering arrests in Colombia, New York and Florida, and the seizure of over $5 million in currency, 65 kilograms of heroin and 60 kilograms of cocaine. Extradition requests to the United States are pending in many of the arrests.

In January 2007, the Colombian National Police in cooperation with the DEA recovered approximately $80 million in primarily U.S. currency and gold on raids on houses used to stash drug

proceeds. Reportedly, the total value is probably the most ever seized by law enforcement in a single operation anywhere in the world.

The U.S. Department of Homeland Security's Immigration and Customs Enforcement (ICE) division has also worked closely with Colombian authorities. In 2002, ICE supported the CNP establishment of a financial investigative unit within the organization's intelligence and investigations unit (DIJIN). ICE also helped Colombia establish a Trade Transparency Unit (TTU) to analyze trade data for customs fraud and money laundering. The TTU analysis showed a direct financial relationship between the narcotics cartels and the Revolutionary Armed Forces of Colombia (FARC), the primary armed guerilla group also designated as an international terrorist organization

Significant strides have been made in the past year to close a loophole in Colombian law to make terrorist financing an autonomous crime. A law was approved by the Colombian Congress (Project 208) which amended the penal code to define and criminalize direct and indirect financing of terrorism, of both national and international terrorist groups. In accordance with the Financial Action Task Force of South America (GAFISUD) and Egmont Group recommendations, the UIAF will receive STRs regarding terrorist financing. The new law will allow the UIAF to freeze terrorists' assets immediately after their designation. In addition, banks will now be held responsible for their client base. Banks will be required to immediately inform the UIAF of any accounts held by newly designated terrorists. Banks will also have to screen new clients against the current list of designated terrorists before the banks are allowed to provide prospective clients with services. Previously, banks were not legally required to comply with either of these regulations, but many had complied regardless. The bill was passed by the Colombian Senate in September 2006, and by the Colombian House of Representatives in December 2006. Presidential approval is expected in 2007.

Colombian law is unclear on the government's authority to block assets of individuals and entities on the UN 1267 Sanctions Committee consolidated list. The government circulates the list widely among financial sector participants, and banks are able to close accounts but not seize assets. Banks also monitor other lists, such as OFAC's publication of Specially Designated Terrorists. Charities and nongovernmental organizations (NGOs) are regulated to ensure compliance with Colombian law and to guard against their involvement in terrorist activity. This regulation consists of several layers of scrutiny, including the regulation of incorporation and the tracing of suspicious financial flows through the collection of intelligence or STR reporting. Reportedly, the GOC acknowledges that monitoring NGOs and charities is an issue that needs continued work and vigilance.

Colombia is a member of GAFISUD and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Money Laundering Experts Working Group, which it chaired in 2005. The UIAF is a member of the Egmont Group, and has signed memoranda of understanding with 27 FIUs around the world. Colombia is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. The GOC has signed, but not ratified, the Inter-American Convention against Terrorism. Colombia formally ratified the UN Convention against Corruption in October 2006.

In 2006, the Government of Colombia has seen additional progress in the development of its financial intelligence unit, regulatory framework and interagency cooperation within the government. The passage of a formal terrorist finance law within the year is another development in fighting terrorism and financial crime. International cooperation with the U.S. and other countries has led to several high-profile seizures and prosecutions. However, weaknesses remain. The growth in contraband trade to launder illicit drug proceeds will require even greater interagency cooperation within the GOC, including coordination between the UIAF and DIAN, the tax and customs authority. Congestion in the court system, procedural impediments and corruption are also problems. Limited resources for prosecutors, investigators, and the judiciary hamper their ability to close cases and dispose of seized assets. Streamlined procedures for the liquidation and sale of seized assets under state management

could help provide funds available for Colombia's anti-money laundering and counterterrorist financing regime.

## Comoros

The Union of the Comoros (Comoros) consists of three islands: Grande Comore, Anjouan and Moheli. An ongoing struggle for influence continues between the Union and island presidents. Comoros is not a principal financial center for the region. An anti-money laundering (AML) law, which addresses many of the primary AML issues of concern, was passed by Presidential Decree in 2004. However, Comoran authorities lack the capacity to effectively implement and enforce the legislation, especially on the island of Anjouan. In May 2006, Muslim cleric Ahmed Abdallah Mohamed Sambi was elected President in the first peaceful change of power in Comoros' post-independence history. He won the election with 58 percent of the vote after campaigning on promises to fight corruption and unemployment. The presidency of the union rotates between the three islands. The former incumbent, Azali Assoumani, represented Grand Comore; Sambi is from Anjouan. The three islands in the Comoros continue to retain much of their autonomy, particularly with respect to their security services, economies, and banking sectors.

The 2004 federal-level AML law is based on the French model. The main features of the law are that it: requires financial and related records to be maintained for five years; permits assets generated or related to money laundering activities to be frozen, seized and forfeited; requires residents to declare all currency or financial instruments upon arrival and departure, and nonresidents to declare all financial instruments upon arrival and all financial instruments above Comoran francs 500,000 (approximately $1,250) on departure; permits provision and receipt of mutual legal assistance with another jurisdiction where a reciprocity agreement is in existence and confidentiality of financial records is respected; requires nonbank financial institutions to meet the same customer identification standards and reporting requirements as banks; requires banks, casinos and money exchangers to report unusual and suspicious transactions (by amount or origin) to the Central Bank and prohibits cash transactions over Comorian francs 5 million (approximately $12,500); and, criminalizes the provision of material support to terrorists and terrorist organizations. Although there is a suspicious activity filing requirement in the Union's AML law, there does not appear to be an independent financial intelligence unit in either Anjouan or the Union. As of February 2006, no suspicious transaction reports had been filed with the Comorian Central Bank in Grand Comore as required under the existing Union law, and the branch of the Central Bank located in Anjouan had no knowledge of the shell bank entities that have been licensed by Anjouan's Offshore Finance Authority, which apparently operates independently from the Union's Central Bank and has licenced some 300 offshore banks, many of which appear to be shell banks.

Foreign remittances from Comorans abroad in France, Mayotte (claimed by France) and elsewhere remain the most important influx of funds for most Comorons. Until recently most remittances came via informal channels, but in 2006 Western Union established a presence to capture part of this market.

Union authorities have limited ability to implement AML laws in Anjouan and Moheli. Similarly, the island governments of Anjouan and Moheli may have limited control over AML matters. Although Moheli has its own AML law in effect (the Anti-Money Laundering Act of 2002), the law itself has some serious shortcomings and authorities lack the resources and expertise to enforce its provisions. For example, there is no absolute requirement to report large cash transactions. Comprehensive information on Anjouan's laws and regulations is difficult to obtain, but it appears Anjouan does have an AML law (the Money Laundering Prevention Act, Government Notice 008 of 2005) but reportedly the law applies to Anjouan and not to the offshore entities it licenses. Little is known about: (i) the procedures that have been established to review and approve offshore licenses issued before the

enactment of the AML law; (ii) the procedures that have been established to review and approve ongoing bank license applications and to supervise and monitor institutions for compliance with Anjouan laws; and, (iii) the efforts and resources available to implement these procedures and enforce compliance.

Union President Azali made efforts during his time as President to bring AML enforcement under Union government jurisdiction. In May 2005, he issued a note to the Ministry of Finance, the islands' presidents, and the Public Prosecution Department urging these institutions to take action with regard to any illegal offshore banking practices. The note indicated that all banking and financial institutions operating within the jurisdiction of the Union of the Comoros, whether offshore or onshore, must abide by the provisions of legislation No. 80-7 of May 3, 1980. According to article 7 of this legislation, a bank or any other financial institution cannot operate in the Union of the Comoros without prior authorization from the Union Finance Minister upon recommendation from the Comoros Central Bank. Thus, offshore banks operating in the autonomous islands of the Union of the Comoros without prior authorization from the Finance Minister contravene the May 3, 1980 legislation. Consequently, Azali's note directed the ministries and other government institutions responsible for banking and financial matters to take (or to see to it that the necessary measures are taken) to put an end to this "blatant illegality which is prejudicial to the Union of the Comoros." Also in May 2005, President Azali told the USG that the Comoran government is prepared to bring to justice the beneficiaries of illegal offshore licenses and sought the assistance and support of the USG in this endeavor. Since taking office, President Sambi has sought to have corrupt former officials prosecuted. A grossly inadequate budget, dysfunctional ministries, and a nonfunctioning judiciary limit Sambi. Throughout 2006 there were reports that Sambi's authority in Anjouan is limited. There are reports that high-ranking Comoran officials tolerate and possibly benefit from money laundering. The lack of political will is exacerbated by the lack of capacity.

While the Comoros is not a principal financial center for the region, Moheli and Anjouan may have attempted or may be attempting to develop an offshore financial services sector as a means to finance government expenditures. The Anjouan island government's claim that unrelated companies are presenting themselves as licensed by the government of Anjouan makes authoritative information on Anjouan's offshore sector difficult to establish. Both Moheli, pursuant to the International Bank Act of 2001, and Anjouan, pursuant to the Regulation of Banks and Comparable Establishments of 1999, license off-shore banks. Together, the islands have licensed more than 100 banks. Applicants for banking licenses in either jurisdiction are not required to appear in person to obtain their licenses. In Anjouan, only two documents (a copy of the applicant's passport and a certificate from a local police department certifying the lack of a criminal record) are required to obtain an offshore license and fax copies of these documents are acceptable. Even if additional information was to be required, it is doubtful that either jurisdiction has the ability or resources to authenticate and verify the information. Neither jurisdiction is capable, in terms of expertise or resources, of effectively regulating an offshore banking center. Anjouan, and probably Moheli as well, has delegated much of its authority to operate and regulate the offshore business to private, non-Comoran domiciled parties. In November 2004 and again in December 2005, Anjouan island government officials denied island government involvement in the offshore sector. They said the Union of the Comoros Central Bank was the only authority for the offshore banking sector in the country and insisted the Anjouan island government had not established its own central bank. They admitted that several years earlier the government of Anjouan considered starting an offshore banking sector, but they had not pursued it. Substantial concern remains that Anjouan, and possibly Moheli, allows shell banking activity.

There are reports that France, which as the former colonial power maintains substantial influence and activity in Comoros, has bypassed the Union and island governments in order to, where possible, prosecute suspects in money laundering or shell banks under French law. Although Comoros lacks homegrown narcotics, the islands are used as a transit site for drugs coming mainly from Madagascar.

In view of international concern about drug trafficking, in 1993 France began providing technical expertise in this field to Comoros.

In addition to offshore banks, both Moheli, pursuant to the International Companies Act of 2001, and Anjouan, pursuant to Ordinance Number 1 of 1 March 1999, license insurance companies, internet casinos, and international business companies (IBC's). Moheli claims to have licensed over 1200 IBC's. Bearer shares of IBC's are permitted under Moheli law. Anjouan also forms trusts, and registers aircraft and ships (without requiring an inspection of the aircraft or ship in Anjouan).

Comoros is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism.

Comoros has become the 12th member of the free-trade area of the Common Market for Eastern and Southern Africa (Comesa). The U.S. Export-Import Bank (ExIm Bank) has added Comoros to its Short-Term Insurance Pilot Program for Africa (STIPP), while renewing the program for three years, beginning March 31, 2006.

The Government of the Union of the Comoros (GOC) should harmonize anti-money legislation for the three islands that comprise the federal entity. The legislation should adhere to world standards. A unified financial intelligence unit should be established and the unregulated offshore financial sectors in Moheli and Anjouan should either be regulated by federal authorities or be shut down. In either case, bearer shares should be prohibited. The list of individuals and entities that are included on the United Nations 1267 Sanctions Committee's consolidated list should be circulated to banks in the Comoros. The deficiencies in the anti-money laundering/terrorist financing regimes in the Comoros and the inability to implement existing legislation make it vulnerable to traditional money laundering and to the financing of terrorism. Comoros should make every effort to comport to international standards.

## Cook Islands

The Cook Islands is a self-governing parliamentary democracy in free association with New Zealand and a member of the British Commonwealth. Cook Islanders are citizens of New Zealand. The Cook Islands' offshore sector makes it vulnerable to money laundering. The sector offers banking, insurance, international trusts, and formation of international business companies and trusts. However, due to recent legislative and regulatory changes, the Cook Islands complies with current international standards.

The domestic banking system is comprised of branches of two major Australian banks and the local Bank of the Cook Islands (BCI). Domestic banks are primarily involved in traditional deposit taking and lending. The BCI operates as a stand-alone institution competing against the two Australian banks and is no longer engaged in development lending. Legislation allows for development lending to be undertaken in the future by a separate company not subject to supervision by the Financial Supervisory Commission (FSC). In addition, nonperforming loans made by the Cook Islands Development Bank have been transferred to another affiliated company. In addition to the three domestic banks, the Cook Islands financial sector also consists of four international banks, six trustee companies, and six offshore and three domestic insurance companies.

The Cook Islands has an offshore financial sector that licenses international banks and offshore insurance companies and registers international business companies (IBCs). The offshore sector also consists of company services and trusts, including asset protection trusts (APTs). APTs protect the assets of individuals from civil judgments in their home countries and often contain a "flee clause." Under a "flee clause," if a foreign law enforcement agency makes an inquiry regarding the trust, the trust will be transferred automatically to another offshore center. According to officials of the

Government of the Cook Islands (GOCI), the "flee clause" is used to transfer APTs in times of emergency, such as a natural disaster.

The Cook Islands was placed on the Financial Action Task Force (FATF) list of Non-Cooperative Countries and Territories (NCCT) since 2000. After the GOCI addressed deficiencies in its anti-money laundering regime by enacting legislative reforms, the FATF removed the Cook Islands from its NCCT list in February 2005. The FATF conducted a year-long monitoring program, which concluded in June 2006, to closely monitor the islands.

The Banking Act 2003 and the Financial Supervisory Commission Act (FSCA) 2003 established a new framework for licensing and prudential supervision of domestic and offshore financial institutions in the Cook Islands. The legislation requires international offshore banks to have a physical presence in the Cook Islands, transparent financial statements, and adequate records prepared in accordance with consistent accounting systems. The physical presence requirement is intended to prohibit shell banks. All banks are subject to a vigorous and comprehensive regulatory process, including on-site examinations and supervision of activities.

The FSCA established the Financial Supervisory Commission as the licensed financial sector's sole regulator. The FSC is empowered to license, regulate, and supervise the business of banking. It serves as the administrator of the legislation that regulates the offshore financial sector. The FSC can license international banks and offshore insurance companies and register international companies. It also supervises trust and company service providers. Its policy is to respond to requests from overseas counterparts to the utmost extent possible. The FSC has taken a broad interpretation of the concept of "counterpart" and does not need to establish general equivalence of function before being able to cooperate.

Licensing requirements, as set out in the legislation, are comprehensive. The Banking Act 2003 and a Prudential Statement on Licensing issued in February 2004 contain detailed licensing criteria for both locally incorporated and foreign banks, including "fit and proper" criteria for shareholders and officers, satisfactory risk management, accounting and management control systems, and minimum capital requirements. The Banking Act 2003 defines banking business, prohibits the unauthorized use of the word "bank" in a company name, and requires prior approval for changes in significant shareholding.

By enacting the Financial Transactions Reporting Act (FTRA) 2003 and additional legislation and amendments in 2003 and 2004, Cook Islands authorities strengthened its anti-money laundering and counterterrorist financing (AML/CTF) legal and institutional framework. Reviews are underway to consider how the AML/CTF legislation affects other domestic laws. The Financial Supervisory Commission (FSC), regulator of the licensed financial sector, drafted new insurance legislation in 2006. It is anticipated that the draft legislation will be passed in 2007. The legislation will regulate the small domestic insurance sector and update supervision of the offshore insurance sector. Insurance intermediaries will also be regulated under the proposed legislation.

The FTRA imposes certain reporting obligations on 26 different types of institutions, including banks, offshore banking businesses, offshore insurance businesses, casinos, gambling services, insurers, financial advisors, solicitors/attorneys, accountants, financial regulators, lotteries and money remitters. The Minister of Finance can extend the reporting obligation to other businesses when required. Reporting institutions are required to retain all records related to the opening of accounts and financial transactions for a minimum of six years. The records must include sufficient documentary evidence to verify the customer's identity. In addition, reporting institutions are required to develop and apply internal policies, procedures, and controls to combat money laundering and to develop audit functions to evaluate such policies, procedures, and controls. Reporting institutions must comply with any guidelines and training requirements issued under the FTRA, as amended, and must provide internal

training on all anti-money laundering matters. The FTRA provides for administrative and financial sanctions on institutions for noncompliance.

The FTRA requires the FSC to assess the compliance by licensed financial institutions with customer due diligence and record keeping requirements. Resulting reports and documentation from annual inspections are provided to the Cook Islands Financial Intelligence Unit (CIFIU). The CIFIU is also responsible for assessing compliance by nonlicensed institutions.

The CIFIU is the central unit responsible for processing disclosures of financial information in accordance with anti-money laundering and antiterrorist financing legislation. It became fully operational with the assistance of a Government of New Zealand technical advisor. The FTRA grants supervisory authority to the CIFIU, allowing it to cooperate with other regulators and supervisors, require reporting institutions to supplement reports, and obtain information from any law enforcement agency and supervisory body.

Obligated institutions are required to report any attempted or completed large currency transactions and suspicious transactions to the CIFIU. The currency reporting requirements apply to all currency transactions of NZ$10,000 (approximately $6870) and above, electronic funds transfers of NZ$10,000 and above, and transfers of currency in excess of NZ$10,000 into and out of the Cook Islands. Failure to declare such transactions could incur penalties. The CIFIU is required to destroy a suspicious transaction report if there has been no activity or information related to the report or to a person named in the report for six years. The CIFIU does not have an investigative mandate. If it determines that a money laundering offense, serious offense or terrorist financing offense has been or is being committed, it must refer the matter to law enforcement for investigation. The Minister of Finance, who is responsible for administrative oversight, appoints the head of the CIFIU.

The CIFIU is participating in the Pacific FIU database project (PFIUDP) provided by AUSTRAC, the Australian FIU. The CIFIU received a prototype of the database and is now testing the reporting and analysis capacity. The Pacific FIU Database Project includes other jurisdictions that will receive versions of the same database framework.

Since June 2004 the Cook Islands had made further progress in implementing its AML/CFT regime. The head of the CIFIU chairs the Coordinating Committee of Agencies and Ministries, which promotes, formalizes and maintains coordination among relevant government agencies; assists the GOCI in the formulation of policies related to AML/CFT issues; and enables government agencies to share information and training resources gathered from their regional and international networks. The AML/CFT consultative group of stakeholders facilitates consultation between government and the private sector, and ensures all financial sector players are involved in the decision making and problem solving process regarding AML/CFT regulations and reporting. The CIFIU is also a member of the Anti-Corruption Committee, along with the Office of the Prime Minister, Police, Crown Law, Audit Office, and the Financial Secretary.

The Terrorism Suppression Act 2004, based on the model law drafted by an expert group established under the auspices of the Pacific Islands Forum Secretariat, criminalizes the commission and financing of terrorism. The United Nations (Security Council Resolutions) Act 2003 allows the Cook Islands, by way of regulations, to give effect to the Security Council resolutions concerning international peace and security.

The GOCI is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. The Cook Islands is an active member of the Asia/Pacific Group on Money Laundering (APG), an associate member organization of the FATF. The CIFIU became a member of the Egmont Group in June 2004, has bilateral agreements allowing the exchange of financial intelligence with Australia, and is negotiating a memorandum of understanding (MOU) with Thailand. The Cook

Islands plans to become a member of the Offshore Group of Banking Supervisors (OGBS), once it has qualified by undergoing further evaluation. The GOCI is also an active member of the Association of Financial Supervisors of Pacific Countries and draws on the resources of this association and Pacific Financial Technical Assistance Centre for capacity building for FSC staff. The Cook Islands has received nine requests for mutual legal assistance since the Mutual Assistance in Criminal Matters Act came into force in 2003. Five have been answered, and four are pending. The Cook Islands has not received any extradition requests from foreign countries, but successfully extradited one person from New Zealand.

The Cook Islands should continue to implement legislation designed to strengthen its nascent AML/CTF institutions. The Government of the Cook Islands should maintain vigilant regulation of its offshore financial sector, including its asset protection trusts, to ensure that its offshore sector comports with international standards.

## Costa Rica

Costa Rica is not a major financial center but remains vulnerable to money laundering and other financial crimes. This is due in part to narcotics trafficking in the region, particularly of South American cocaine, and the presence in Costa Rica of Internet gaming companies. Costa Rica has a black market for smuggled goods, but the goal of most of this activity seems to be tax evasion rather than laundering of narcotics proceeds. Reforms in 2002 to the Costa Rican counternarcotics law expand the scope of anti-money laundering regulations, but also create an invitation to launder funds by eliminating the government's licensing and supervision of casinos, jewelers, realtors, attorneys, and other nonbank financial institutions. No actions were taken to close this loophole in 2006. Gambling is legal in Costa Rica, and there is no requirement that the currency used in Internet gaming operations be transferred to Costa Rica. Currently, over 250 sports-book companies have registered to operate in Costa Rica. Two of the largest companies shut down their operations during 2006 when top executives were arrested in the United States.

In 2002, the Government of Costa Rica (GOCR) enacted Law 8204. Law 8204 criminalizes the laundering of proceeds from all serious crimes, which are defined as crimes carrying a sentence of four years or more. Law 8204 also obligates financial institutions and other businesses (such as money exchangers) to identify their clients, report currency transactions over $10,000 and suspicious transactions to the financial intelligence unit (FIU), keep financial records for at least five years, and identify the beneficial owners of accounts and funds involved in transactions. While Law 8204, in theory, applies to the movement of all capital, current regulations are strictly interpreted so that the law applies only to those entities that are involved in the transfer of funds as a primary business purpose. Therefore, the law does not cover such entities as casinos, dealers in gems or Internet gambling operations, as their primary business is not the transfer of funds.

The formal banking industry in Costa Rica is tightly regulated. However, the offshore banking sector, which offers banking, corporate and trust formation services, remains an area of concern. Foreign-domiciled "offshore" banks can only conduct transactions under a service contract with a domestic bank, and they do not engage directly in financial operations in Costa Rica. Costa Rican authorities acknowledge that they are unable to adequately assess risk. Costa Rican financial institutions are regulated by the Office of the Superintendent of Financial Institutions (SUGEF).

Currently, six offshore banks maintain correspondent operations in Costa Rica: three from The Bahamas and three from Panama. The GOCR has supervision agreements with its counterparts in Panama and The Bahamas, permitting the review of correspondent banking operations. These counterpart regulatory authorities occasionally interpret the agreements in ways that limit review by Costa Rican officials. In 2005, the GOCR's Attorney General ruled that the SUGEF lacks authority to regulate offshore operations due to an apparent contradiction between the 1995 Organic Law of the

Costa Rican Central Bank and Law 8204. Draft legislation to correct the contradiction and reassert the SUGEF's regulatory power is under review in the Legislative Assembly. However, the Legislative Assembly took no action on this draft legislation in 2006.

All persons carrying cash are required to declare any amount over $10,000 to Costa Rican officials at ports of entry. During 2006, officials seized over $5.2 million in narcotics-related assets, much of it in undeclared cash. By comparison, in 2005 the GOCR seized $850,000 in assets. Seized assets are processed by the Costa Rican Drug Institute (ICD) and if forfeited, are divided among drug treatment agencies (60 percent), law enforcement agencies (30 percent), and the ICD (10 percent).

Eighteen free trade zones operate within Costa Rica, primarily producing electronics, integrated circuits, textiles and medicines for re-export. The zones are under the supervision of "PROCOMER" a federal export-promotion entity. Costa Rican authorities report no indications of trade-based money laundering schemes in the zones. PROCOMER strictly enforces control over the zones, but its measures are aimed primarily at preventing tax evasion.

Costa Rica's FIU, the Unidad de Análisis Financiero (UAF), became operational in 1998 and was admitted into the Egmont Group in 1999. Established within the ICD, the UAF analyzes suspicious activity reports for potential referral to prosecutors. It has no regulatory responsibilities. The UAF has access to the records and databases of financial institutions and other government entities, but must obtain a court order if the information collected is to be used as evidence in court. The banking industry cooperates with authorities and routinely reports suspicious activities. In spite of its broad access to government information and high levels of cooperation with the financial sector, the UAF remains ill-equipped and under-funded to provide information needed by investigators. Nevertheless, in 2006, the UAF increased the quality of its analysis and forwarded more thoroughly analyzed cases to prosecutors. Three money laundering cases that began judicial proceedings in 2005 were successfully prosecuted in 2006.

Although the GOCR has ratified the major UN counterterrorism conventions, terrorism and its financing are not crimes in Costa Rica. Costa Rican authorities have received and circulated to all financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. However, these authorities cannot block, seize, or freeze property without prior judicial approval. Thus, Costa Rica lacks the ability to expeditiously freeze assets connected to terrorism. No assets related to designated individuals or entities were identified in Costa Rica in 2006.

In 2002, a government task force drafted a comprehensive counterterrorism law with specific terrorist financing provisions. The draft law, when passed, would expand existing conspiracy laws to include the financing of terrorism and enhance existing narcotics laws by incorporating the prevention of terrorist financing into the mandate of the ICD. In 2004, the Legislative Assembly also considered a separate draft terrorism law but took no action. In 2006, the Assembly's Narcotics Committee continued to study the two proposals, but no further progress has been made.

Costa Rica is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. The GOCR has signed, but not yet ratified, the UN Convention against Corruption. The GOCR has also signed the Organization of American States (OAS) Inter-American Convention on Mutual Assistance in Criminal Matters, and has ratified the Inter-American Convention against Terrorism. Costa Rica is a member of the Caribbean Financial Action Task Force (CFATF) and the Money Laundering Experts Working Group of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD). The UAF is a member of the Egmont Group.

Even though Costa Rica has convicted a handful of individuals for money laundering in 2005 and 2006, further efforts are required to bring Costa Rica into compliance with international anti-money laundering and counterterrorist financing standards. The GOCR should pass legislation that clarifies contradictions regarding the supervision of its offshore banking sector, and should extend its anti-money laundering legislation and regulations to cover the Internet gaming sector, gem dealers, attorneys, casinos and other nonbank financial institutions. Costa Rica should also criminalize terrorism and terrorist financing, and ensure that its financial intelligence unit and other GOCR authorities are adequately equipped to combat financial crime.

## Côte d'Ivoire

Cote d'Ivoire is an important West African regional financial hub. Money laundering and terrorist financing in Cote d'Ivoire are not primarily related to narcotics proceeds. Criminal proceeds that are laundered are reportedly derived from regional criminal activity, such as the smuggling of consumer goods and agricultural products. Most of the smuggling networks are organized chiefly by nationals from Nigeria and the Democratic Republic of the Congo. Due to the ongoing political and economic turmoil in Cote d'Ivoire, respect for the rule of law continues to deteriorate. As a result, Ivorian and some Liberian nationals are becoming more and more involved in criminal activities and the subsequent laundering of funds. Cote d'Ivoire is ranked 153 out of 163 countries in Transparency International's 2006 Corruption Perception Index.

The outbreak of the rebellion in 2002 increased the amount of smuggling of goods across the northern borders, especially of textiles and cigarette products. There have also been reports of an increase in the processing and smuggling of small quantities of diamonds from mines located in the north. Ivorian law enforcement authorities have no control over the northern half of the country, and therefore they cannot judge what relationship, if any, the funding for smuggled goods might have to narcotics proceeds or other illicit proceeds. Smuggling of sugar, cotton, cocoa, cars, and pirated DVDs occurs in the government-controlled south and is motivated by a desire to avoid the payment of taxes. According to the Office of the Customs Financial Enquiries, the cross-border trade of diamond and cocoa over Cote d'Ivoire's porous borders generates contraband funds that are laundered into the banking system via informal moneychangers. Criminal enterprises use both the formal and informal financial sector to launder funds. Cash is moved both via the formal banking sector and by cash couriers. Cash earned by immigrant or migrant workers generally flows out of Cote d'Ivoire, going to extended families outside the region. Informal money couriers and money transfer organizations similar to hawaladars move funds both domestically and within the sub-region. Currently, domestic informal cash transfer systems are not regulated. Informal remittance transfers from outside Cote d'Ivoire violate West African Central Bank (BCEAO) money transfer regulations. Because of the division of the country, a lack of security, and the lack of a widespread banking system, transportation companies have also stepped in to provide courier services. The standard fee for these services is approximately ten percent. In addition to transferring funds, criminal enterprises launder illicit funds by investing in real estate and consumer goods such as used cars in an effort to conceal the source of funding.

Hizbollah is present in Cote d'Ivoire, and it conducts fundraising activities, mostly among the large Lebanese expatriate community. The Ivorian government has taken no legal action to prevent the misuse of charitable and or other nonprofit entities that can be used as conduits for the financing of terrorism. Reportedly, the Ministry of Interior Security is addressing this problem.

There are no free trade zones in Cote d'Ivoire. In August 2004, the Ivorian government adopted a plan for the creation of a free trade zone for information technology and for biotechnology. This project is dormant. Another free trade zone project, which was planned for the port of San Pedro, also remains dormant.

The Economic and Financial police have noticed an increase in financial crimes related to credit card theft and foreign bank account fraud, which includes wire transfers of large sums of money primarily involving British and American account holders who are the victims of Internet based advanced fee scams. The Ministry of Finance remains concerned by the high levels of tax fraud, particularly VAT tax fraud, by merchants. The country has the largest bank network in the region with seventeen banks and two nonbank financial institutions. Of that number, there are eight foreign-owned banks and two foreign-owned financial institutions in operation. French banking accounts for more than 60 percent of banking activity. The law requires a capitalization of the CFA equivalent of $2 million for banks and $600,000 for financial institutions. Banks provide traditional banking services such as lending, savings and checking accounts and money transfers, while financial institutions offer leasing, payroll and billing services, and project financing for small businesses. The political crisis has disrupted banking operations.

The Ivorian banking law, enacted in 1990, prevents disclosure of client and ownership information, but it does allow the banks to provide information to judicial authorities, such as investigative magistrates. The law also permits the use of client and ownership information as evidence in legal proceedings or during criminal investigations. The Tax and Economic police can request information from the banks.

Until recently, the penal code criminalized only money laundering related to drug-trafficking, fraud, and arms trafficking. On November 29, 2005, the Ivorian National Assembly adopted the West African Economic and Monetary Union's (WAEMU) model law on money laundering, making money laundering per se a criminal offense. Money laundering is defined as the intention to conceal the criminal origins of illicit funds. The new law was adopted on December 2, 2005, and became effective on August 9, 2006.

The new law focuses on the prevention of money laundering and also expands the definition of money laundering to include the laundering of funds from all serious crimes. The law does not set a minimum threshold. It includes standard "know your customer" requirements for banks and other financial institutions. It establishes procedures, which require these institutions to assist in the detection of money laundering through suspicious transaction reporting, and it creates an Ivorian Financial Intelligence Unit (FIU). It also provides a legal basis for international cooperation. The new law includes both penal and civil penalties. The law permits the freezing and seizure of assets, which includes instruments and proceeds of crime, including business assets and bank accounts that are used as conduits for money laundering. Substitute assets cannot be seized if there is no relationship with the offense. Legitimate businesses can be seized if used to launder money or support terrorist or other illegal activities.

Under the new money laundering law, Cote d'Ivoire is required to create and fund an FIU named the "Cellule Nationale de Traitement des Informations Financieres" (CENTIF). The CENTIF will report to the Finance Ministry. On a reciprocal basis, with the permission of the Ministry of Finance, the CENTIF may share information with the FIUs in member states of WAEMU or with those of non-WAEMU countries, as long as those institutions keep the information confidential.

The FIU will take the lead in tracking money laundering, but it will continue to work with previously established investigative units such as the "Centre de Recherche Financiere" (CRF) at the Department of Customs and the Agence Nationale de Strategie et d'Intelligence" (ANSI) at the presidency. The CRF and the ANSI will still continue their missions, which include fiscal and customs fraud and counterfeiting. The Ivorian Economic and Financial police, the criminal police unit (Police Judiciaire), the Department of Territorial Surveillance (Ivorian intelligence service), the CRF and ANSI all are responsible for investigating financial crimes, including money laundering and terrorist financing. However, in addition to a lack of resources for training, there is a perceived lack of political will to permit investigative independence.

The Ministry of Finance, the BCEO, and the West African Banking Commission, headquartered in Cote d'Ivoire, supervise and examine Ivorian compliance with anti-money laundering/counterterrorist financing laws and regulations. All Ivorian financial institutions are now required to begin to maintain customer identification and transaction records for ten years. For example, all bank deposits over approximately CFA 5,000,000 (approximately $10,000) made in BCEAO member countries must be reported to the BCEAO, along with customer identification information. Law enforcement authorities can access these records to investigate financial crimes upon the request of a public prosecutor. In 2005, there were no arrests or prosecutions for money laundering or terrorist financing.

The new legislation imposes a ten year retention requirement on financial institutions to retain records of all "significant transactions," which are transactions with a minimum value of CFA 50,000,000 (approximately $100,000) for known customers. For occasional customers, the floor value for "significant transactions" is CFA 5,000,000.

The new money laundering controls will apply to nonbank financial institutions such as exchange houses, stock brokerage firms, insurance companies, casinos, cash couriers, national lotteries, nongovernment organizations, travel agencies, art dealers, gem dealers, accountants, attorneys, and real estate agents. The law also imposes certain customer identification and record maintenance requirements on casinos and exchange houses. The tax office (Ministry of Finance) supervises these entities. All Ivorian financial institutions, businesses, and professionals and nonbank institutions under the scope of the new money laundering law are required to report suspicious transactions. The Ivorian banking code protects reporting individuals. Their identities are not divulged with respect to cooperation with law enforcement authorities.

Cote d'Ivoire monitors and limits the international transport of currency and monetary instruments under WAEMU administrative regulation R/09/98/CM/WAEMU. There is no separate domestic law or regulation. When traveling from Cote d'Ivoire to another WAEMU country, Ivorian and expatriate residents must declare the amount of currency being carried out of the country. When traveling from Cote d'Ivoire to a destination other than another WAEMU country, Ivorian and expatriate residents are prohibited from carrying an amount of currency greater than the equivalent of 500,000 CFA francs (approximately $1,000) for tourists, and two million CFA francs (approximately $4,000) for business operators, without prior approval from the Department of External Finance of the Ministry of Economy and Finance. If additional amounts are approved, they must be in the form of travelers' checks.

Although Cote d'Ivoire's new money laundering law encompasses the laundering of funds from all serious crimes, terrorism and terrorist financing are not considered "serious crimes" for the purposes of this law. Cote d'Ivoire does not have a specific law that criminalizes terrorist financing, as required under UNSC resolution 1373. Until the passage of the new law, the GOCI relied on several WAEMU directives on terrorist financing, which provided a legal basis for administrative action by the Ivorian government to implement the asset freeze provisions of UNSCR 1373. The BCEAO and Ivorian government report that they promptly circulate to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's Consolidated List and those on the list of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224. A U.S. financial institution present in Cote d'Ivoire confirms the receipt of notices issued by government authorities. No assets related to terrorist entities or individuals have been discovered, frozen or seized.

Cote d'Ivoire participates in the ECOWAS-Intergovernmental Group for Action Against Money Laundering (GIABA) based in Dakar, which sits as an observer to the Financial Action Task Force (FATF). In July 2006, the United Nations Office on Drugs and Crime (UNODC) sponsored a meeting on money laundering in cooperation with the GIABA. The Ivorian government has neither adopted laws nor promulgated regulations that specifically allow for the exchange of records with United

States on money laundering and terrorist financing. However, under the new money laundering law, after obtaining the approval of the Finance Ministry, the CENTIF could share information related to money laundering records with U.S. or other countries on a reciprocal basis and under an agreement of confidentiality between the two governments.

Cote d'Ivoire has demonstrated a willingness to cooperate with the USG in investigating financial or other crimes. For example, in one case from 2004, an American citizen was being defrauded by an individual posing as a GOCI Customs Official requesting demurrage fees for a shipment of goods. With a short window of opportunity for action, the U.S. Embassy notified the Economic Police, who then instructed the Bank Examiner to monitor the suspect's account. The next morning, the Economic Police arrested a Nigerian who came in to retrieve the funds. Armed with a search warrant, the police searched the suspect's house, gathered evidence of a boiler-room operation, and arrested three other Nigerians. The funds ($15,000) were successfully wired back to the victim.

Cote d'Ivoire hosted a workshop and conference regarding money laundering and fraud prevention, both in March 2006. Abidjan also hosted the Eleventh Conference of Customs Director Generals for West and Central Africa on information exchange as a critical part of the fight against customs and fiscal fraud. Also in March 2006, Cote d'Ivoire held, in collaboration with the United Nations Development Program (UNDP), a workshop releasing the results of the 2004 training seminar on financial delinquency, money laundering and terrorism financing.

Cote d'Ivoire is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. Cote d'Ivoire has signed, but not yet ratified, the UN Convention against Transnational Organized Crime.

The Government of the Cote d'Ivoire should implement its new anti-money laundering law, including the funding and establishing of an FIU. It should criminalize terrorist financing. Cote d'Ivoire law enforcement and customs should examine forms of trade-based money laundering and informal value transfer systems. Authorities should take steps to halt the spread of corruption that permeates both commerce and government and facilitates the underground economy and money laundering. Cote d'Ivoire should ratify the UN Convention against Transnational Organized Crime.

## Cyprus

Cyprus has been divided since the Turkish military intervention of 1974, following an unsuccessful coup d'etat directed from Greece. Since then, the southern part of the country has been under the control of the Republic of Cyprus. The northern part is run by a Turkish Cypriot administration that in 1983 proclaimed itself the "Turkish Republic of Northern Cyprus (TRNC)," recognized only by Turkey. The U.S. Government recognizes only the Republic of Cyprus (ROC). This report refers to the Government-controlled area unless otherwise specified.

Cyprus is a major regional financial center with a robust financial services industry that includes an offshore sector. As with other such centers, Cyprus remains vulnerable to international money laundering activities. Fraud and other financial crimes, and narcotics trafficking are the major sources of illicit proceeds laundered in Cyprus. Casinos and internet gaming sites are not permitted, although sports betting halls are allowed.

A number of factors facilitated the development of Cyprus' offshore financial sector in Cyprus: the island's central location; a preferential tax regime, double tax treaties with 40 countries (including the United States, several European Union (EU) nations, and former Soviet Union nations); a labor force particularly well trained in legal and accounting skills; a sophisticated telecommunications infrastructure; and, relatively liberal immigration and visa requirements. Since the offshore financial sector was established in 1975, more than 54,000 offshore international business companies have been registered. Reportedly, there are approximately 14,000 international business companies (IBCs)

currently registered. An International Banking Unit (IBU) is a Cypriot limited liability company or a branch of a foreign bank, which has obtained a banking license from the Central Bank. An Offshore Financial Services Company (OFSC) engages in dealing, buying, selling, subscribing to or underwriting investments; managing investments belonging to other persons; giving investment advice to actual or potential investors; and establishing collective investment schemes. The Central Bank vetting process for offshore companies also ensures that prospective OFSCs are linked to existing investment or financial services companies in well-regulated countries.

In recent years, Cyprus has introduced tax and legislative changes effectively abolishing all legal and substantive distinctions between domestic and offshore companies. All Cypriot companies are now taxed at a uniform rate of 10 percent, irrespective of the permanent residence of their owners or whether they do business internationally or in Cyprus. A transition period allowing preferential tax treatment to offshore companies that existed prior to 2002 expired on January 1, 2006. Additionally, the prohibition from doing business domestically has been lifted and companies formerly classified as offshore are now free to engage in business locally. Bearer shares have been abolished. It is not clear whether the beneficial owners of the more than 50,000 international business companies formally registered in the offshore sector are now known to the Cyprus authorities.

Cyprus continues to revise its anti-money laundering (AML) framework to meet evolving international standards. In 1996, it passed the Prevention and Suppression of Money Laundering Activities Law, which mandated the establishment of the Cypriot financial intelligence unit (FIU). This law criminalizes all money laundering, provides for the confiscation of proceeds from serious crimes, and codifies the actions that banks, nonbank financial institutions, and obligated nonfinancial businesses must take, including those related to customer identification. The anti-money laundering law authorizes criminal (but not civil) seizure and forfeiture of assets. Subsequent amendments to the 1996 law broadened its scope by replacing the separate list of predicate offenses with a definition of predicate offense to be any criminal offense punishable by a prison term exceeding one year, by addressing government corruption, by providing for the sharing of assets with other governments and by facilitating the exchange of financial information with other FIUs.

Amendments passed in 2003 and 2004 authorize the FIU to instruct banks to delay or prevent execution of customers' payment orders; extend due diligence and reporting requirements to auditors, tax advisors, accountants, and, in certain cases, attorneys, real estate agents, and dealers in precious stones and gems; and permit administrative fines of up to 2,863 Cypriot pounds (approximately $6,390). The amendments also increase bank due diligence obligations concerning suspicious transactions and customer identification requirements, subject to supervisory exceptions for specified financial institutions in countries with equivalent requirements.

Also in 2003, Cyprus enacted legislation regulating capital and bullion movements and foreign currency transactions. The law requires all persons entering or leaving Cyprus to declare all currency, Cypriot or foreign, or gold bullion worth approximately $15,500 (approximately 6,730 Cypriot pounds) or more. This sum is subject to revision by the Central Bank. This law replaced the exchange control restrictions under the Exchange Control Law, which expired in May 2004.

Four authorities regulate and supervise financial institutions in Cyprus: the Central Bank of Cyprus, responsible for supervising locally incorporated banks as well as subsidiaries and branches of foreign banks; the Cooperative Societies Supervision and Development Authority (CSSDA), supervising cooperative credit institutions; the Superintendent for Insurance Control; and the Cyprus Securities and Exchange Commission. Designated nonfinancial businesses and professions (DNFBPs) are regulated by three entities: the Council of the Bar Association supervises attorneys; the Institute of Certified Public Accountants supervises accountants; and the FIU supervises real estate agents and dealers in precious metals and stones. The supervisory authorities may impose administrative

sanctions if the legal entities or persons they supervise fail to meet their obligations as prescribed in Cyprus' anti-money laundering laws and regulations.

Cyprus currently hosts a total of 40 banks. Fourteen of these are incorporated locally. Eleven of the fourteen banks are commercial banks and three are specialized financial institutions. Of the commercial banks, six are foreign-owned, and two are branches of foreign banks. The remaining 26 banks are foreign-incorporated and conduct their operations almost exclusively outside of Cyprus. At the end of August 2006, the cumulative assets of domestic banks were $53.9 billion, while the cumulative assets of subsidiaries and branches of the foreign-incorporated banks were $22.8 billion.

As of May 2004, when Cyprus joined the EU, banks licensed by competent authorities in EU countries could establish branches in Cyprus or provide banking services on a cross-border basis without obtaining a license from the Central Bank of Cyprus, under the EU's "single passport" principle. By the end of 2006, four foreign banks were operating a branch in Cyprus under the EU's "single passport" arrangement.

Cyprus hosts six licensed money-transfer companies, 40 international independent financial advisers, six international trustee services and 200 feeder funds. There are also 47 investment firms, two management firms handling "undertakings for collective investment in transferable securities" (UCITS), 43 licensed insurance companies, 238 licensed real estate agents, 1,858 registered accountants, 1,631 practicing lawyers and around 350 credit institutions. These 350-plus credit societies and cooperative savings banks retain 32 percent of total deposits.

In October 2006, the IMF released a detailed assessment of the "Observance of Standards and Codes for Banking Supervision, Insurance Supervision and Securities Regulation." Among other issues, the report noted that the SEC was legally unable to cooperate with foreign regulators if the SEC did not have an independent interest in the matter being investigated and that the SEC was experiencing difficulty obtaining information regarding the beneficial owners of Cypriot-registered companies. The SEC is working to resolve both of these issues. The report also noted that commitments emerging from EU accession had "placed stress on the skills and resources" of the staff of the CSSDA and the Insurance Superintendent and recommended additional training.

In recent years the Central Bank has introduced many new regulations aimed at strengthening anti-money laundering vigilance in the banking sector. Among other requirements, banks must (1) ascertain the identities of the natural persons who are the "principal/ultimate" beneficial owners of corporate or trust accounts; (2) obtain as quickly as possible identification data on the natural persons who are the "principal/ultimate" beneficial owners when certain events occur, including: an unusual or significant transaction or change in account activity; a material change in the business name, officers, directors and trustees, or business activities of commercial account holders; or a material change in the customer relationship, such as establishment of new accounts or services or a change in the authorized signatories; (3) adhere to the October 2001 paper of the Basel Committee on Banking Supervision on "Customer Due Diligence for Banks"; and (4) pay special attention to business relationships and transactions involving persons from jurisdictions identified by the Financial Action Task Force (FATF) as noncooperative. This list is updated regularly in line with the changes effected to the list of noncooperative countries and territories by the FATF.

All banks must report to the Central Bank, on a monthly basis, individual cash deposits exceeding 10,000 Cypriot pounds (approximately $22,000 in local currency) or approximately $10,000 in foreign currency. Bank employees are required to report all suspicious transactions to the bank's compliance officer, who determines whether to forward a report to the Cypriot FIU for investigation. Banks retain reports not forwarded to the FIU, and these are audited by the Central Bank as part of its regular on-site examinations. Banks must file monthly reports with the Central Bank indicating the total number of suspicious transaction reports (STRs) submitted to the compliance officer and the number forwarded by the compliance officer to the FIU. By law, bank officials may be held personally liable if

their institutions launder money. Cypriot law partially protects reporting individuals with respect to their cooperation with law enforcement but does not clearly absolve a reporting institution or its personnel from complete criminal or civil liability. Banks must retain transaction records for five years.

In November 2004, the Central Bank issued a revised money laundering guidance note that places several significant new obligations on banks, including requirements to develop a customer acceptance policy; renew customers' identification data on a regular basis; construct customers' business profiles; install computerized risk management systems in order to verify whether a customer constitutes a "politically exposed person"; provide full details on any customer sending an electronic transfer in excess of $1,000; and implement (by June 5, 2005) adequate management information systems for on-line monitoring of customers' accounts and transactions. Cypriot banks have responded by adopting dedicated electronic risk management systems, which they typically use to target transactions to and from high-risk countries. Cyprus' Exchange Control Law expired on May 1, 2004, ending Central Bank review of foreign investment applications for non-EU residents. Individuals wishing to invest on the island now apply through the Ministry of Finance. The Ministry also supervises collective investment schemes.

The Central Bank also requires compliance officers to file an annual report outlining measures taken to prevent money laundering and to comply with its guidance notes and relevant laws. In addition, the Central Bank is legally empowered to conduct unannounced inspections of bank compliance records. In July 2002, the U.S. Internal Revenue Service (IRS) officially approved Cyprus' "know-your-customer" rules, which form the basic part of Cyprus' anti-money laundering system. As a result of the above approval, banks in Cyprus that may be acquiring United States securities on behalf of their customers are eligible to enter into a "withholding agreement" with the IRS and become qualified intermediaries.

Established as the Cypriot FIU in 1997, the Unit for Combating Money Laundering (MOKAS) is responsible for receiving and analyzing STRs and for conducting money laundering or financial fraud investigations. At the time of the MONEYVAL mutual evaluation report submission, in February 2006, MOKAS had a multidisciplinary staff of 14. In June 2006, MOKAS hired an additional six financial investigators. A representative of the Attorney General's Office heads the unit. MOKAS cooperates closely with FinCEN and other U.S. Government agencies in money laundering investigations. All banks and nonbank financial institutions, insurance companies, the stock exchange, cooperative banks, lawyers, accountants, and other financial intermediaries must report suspicious transactions to MOKAS. Sustained efforts by the Central Bank and MOKAS to strengthen reporting have resulted in an increase in the number of STRs being filed from 25 in 2000 to 179 in 2006. During 2006, MOKAS received 208 information requests from foreign FIUs, other foreign authorities, and INTERPOL. MOKAS evaluates evidence generated by its member organizations and other sources to determine if an investigation is necessary. Money laundering is an autonomous crime. The MONEYVAL team noted at its on-site visit that there appeared to be 14 money laundering cases in the courts. Only three of the 14 known cases resulted from the STR process.

MOKAS has the power to suspend financial transactions for an unspecified period of time as an administrative measure. MOKAS also has the power to apply for freezing or restraint orders affecting any kind of property at a very preliminary stage of an investigation. In 2005, for the first time, MOKAS issued several warning notices, based on its own analysis, identifying possible trends in criminal financial activity. These notices have already produced results, including the closure of dormant bank accounts. MOKAS conducts anti-money laundering training for Cypriot police officers, bankers, accountants, and other financial professionals. Training for bankers is conducted in conjunction with the Central Bank of Cyprus.

During 2006, MOKAS opened 410 cases and closed 160. There were twelve prosecutions for money laundering, which have resulted in seven convictions since 2000: three in 2001, four in 2004, and one each in 2002, 2005 and 2006. During the same period, it issued 28 Information Disclosure Orders (typically involving judiciary proceedings in courts abroad), 13 administrative orders for postponement of transactions, and 4 freezing orders, including two foreign restraint orders, resulting in the freezing of 2.23 million euros (approximately $2.9 million) in bank accounts and three vehicles. Additionally, during 2006, MOKAS issued one confiscation order for a total amount of 1.33 million euros (approximately $1.73 million). A number of other cases are pending.

On November 30, 2001, Cyprus became a party to the UN International Convention for the Suppression of the Financing of Terrorism. Terrorism financing is criminalized by sections 4 and 8 of the Ratification Law 29 (III) of 2001. The implementing legislation amended the AML law to criminalize the collection of funds in the knowledge that these would be used by terrorists or terrorist groups for violent acts. The parliament passed an amendment to the implementing legislation in July 2005 eliminating a loophole that had inadvertently excused Cypriot nationals operating in Cyprus from prosecution for terrorism finance offenses. However, as noted in the 2006 MONEYVAL mutual evaluation report, Cyprus has yet to criminalize the general collection of funds in the knowledge that they would be used by terrorists or terrorist groups for any purpose (i.e. not just for violent acts) as required by FATF Special Recommendation II. In November 2004, MOKAS designated two employees to be responsible for terrorist finance issues. MOKAS routinely asks banks to check their records for any transactions by any person or organization designated by foreign FIUs or the U.S. Treasury Department as a terrorist or a terrorist organization.

Under a standing instruction, the Central Bank automatically issues a "search and freeze" order for accounts matching the name of any entity or group designated by the UN 1267 Sanctions Committee or the EU Clearinghouse as a terrorist of terrorist organization. If a financial institution were to find any matching accounts, it would be required to immediately freeze the accounts and inform the Central Bank. As of January 2007, no bank had reported holding a matching account. When FIUs or governments such as the USG -- not the UN or the EU Clearinghouse -- designate and circulate the names of suspected terrorists, MOKAS has the authority to block funds and contacts commercial banks directly to investigate. None of these checks have revealed anything suspicious to date. The lawyers' and accountants' associations cooperate closely with the Central Bank. Cyprus cooperates with the United States to investigate terrorist financing. MOKAS reports that no terrorist assets have been found in Cyprus to date and thus there have been no terrorist finance prosecutions or freezing of terrorist assets. However, authorities reported that in 2006 there had been one investigation for terrorism financing involving four persons.

Reportedly, there is no evidence that alternative remittance systems such as hawala or black market exchanges are operating in Cyprus on a significant scale. Cyprus believes that its existing legal structure is adequate to address money laundering through such alternative systems. Cyprus licenses charitable organizations, which must file with the government copies of their organizing documents and annual statements of account. Reportedly, the majority of charities registered in Cyprus are domestic organizations.

Cyprus is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Cyprus is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and the Offshore Group of Banking Supervisors. MOKAS is a member of the Egmont Group and has signed memoranda of understanding (MOUs) with 17 FIUs, although Cypriot law allows MOKAS to share information with other FIUs without benefit of an MOU. A mutual legal assistance treaty between Cyprus and the United States entered into force September 18, 2002.

Cyprus underwent a MONEYVAL mutual evaluation in April 2005, the results of which were published in a report adopted at the MONEYVAL Plenary meeting in February 2006. The report found Cyprus to be fully compliant in 17 areas, largely compliant in 22, and partially compliant in 10 of the Financial Action Task Force's (FATF) Forty Recommendations and Nine Special Recommendations on terrorism finance. There were no criteria for which Cyprus was found to be noncompliant. The assessment team also put forward a detailed recommended action plan designed to further improve its anti-money laundering system.

Cyprus has put in place a comprehensive anti-money laundering regime. It should continue to take steps to tighten implementation of its laws. In particular, it should enhance regulation of corporate service providers, including trust and incorporation companies, lawyers, accountants, and other designated nonfinancial businesses and professions. Now that Cyprus is abolishing its offshore financial services, it should withdraw from the Offshore Group of Banking Supervisors to dispel any confusion that its continued membership might engender. It should enact provisions that allow for civil forfeiture of assets. It should also continue to work on improving the collection and centralization of statistical data in relation to money laundering investigations, prosecutions and convictions. Cyprus should criminalize the collection of funds with the knowledge that they will be used by terrorists or terrorist groups for any purpose -- not only to commit violent acts. Cyprus should also take steps to implement the recommendations of the recent MONEYVAL and IMF evaluations, including ensuring the staffing level at MOKAS is sufficient for MOKAS to fulfill its mandate.

**Area Administered by Turkish Cypriots.** The Turkish Cypriot community continues to lack the legal and institutional framework necessary to provide effective protection against the risks of money laundering. It is thought that the 19 essentially unregulated and primarily Turkish-mainland owned casinos and the 15 offshore banks are the primary vehicles through which money laundering occurs. Casino licenses are fairly easy to obtain, and background checks on applicants are minimal. A significant portion of the funds generated by these casinos reportedly change hands in Turkey without ever entering the Turkish Cypriot banking system, and there are few safeguards to prevent the large-scale transfer of cash to Turkey. Another area of concern is the approximately five hundred "finance institutions" operating in the area that extend credit and give loans. Although they must register with the "Office of the Registrar of Companies," they are unregulated. Some of these companies are owned by banks and others by auto dealers. In 2005 and 2006, there was a large increase in the number of sport betting halls, which are licensed by the "Office of the Prime Minister." There are currently seven companies operating in this sector, with a total of 85 outlets. Four of the companies also accept bets over the internet. Turkish Cypriot authorities deported one prominent Turkish organized crime figure, Yasar Oz, following a December 19 shootout at the Grand Ruby Casino that left two dead. As a result of this incident, the Turkish Cypriot authorities arrested seven individuals, closed the Grand Ruby and Denizkizi Casinos and deported much of their staff. Nevertheless, several other casinos are still believed to have significant links to organized crime groups in Turkey.

The fact that the “TRNC” is recognized only by Turkey limits the ability of Turkish Cypriot authorities to receive training or funding from international organizations with experience in combating money laundering. The Turkish Cypriot community is not part of any regional FATF-style organization and thus is not subject to any peer evaluations.

The offshore banking sector remains a concern. In August 2004, the U.S. Department of the Treasury's FinCEN issued a notice of proposed rulemaking to impose a special measure against First Merchant Bank OSH Ltd in the area administered by Turkish Cypriots as a financial institution of primary money laundering concern. Pursuant to Section 311 of the USA PATRIOT Act, FinCEN found First Merchant Bank to be of primary money laundering concern based on a number of factors, including: (1) it is licensed as an offshore bank in the “TRNC,” a jurisdiction with inadequate anti-money laundering controls, particularly those applicable to its offshore sector; (2) it is involved in the marketing and sale of fraudulent financial products and services; (3) it has been used as a conduit for

the laundering of fraudulently obtained funds; and (4) the individuals who own, control, and operate First Merchant Bank have links with organized crime and apparently have used First Merchant Bank to launder criminal proceeds. As a result of the finding and in consultation with federal regulators and the Departments of Justice and State, FinCEN proposed imposition of the special measure that would prohibit the opening or maintaining of correspondent or payable-through accounts by any U.S. domestic financial institution or domestic financial agency for, or on behalf of, First Merchant Bank OSH Ltd. On December 4, 2006, the Turkish Cypriot administration ordered First Merchant Bank to cease its operations due to violations of the Turkish Cypriot "Offshore Banking Law." The bank is now only permitted to perform activities associated with closing the Bank such as the payment and collection of outstanding debts.

Turkish Cypriot authorities have begun taking limited steps to address these risks. Nevertheless, it appears that the Turkish Cypriot leadership lacks the political will necessary to push through reforms needed to introduce effective oversight of its limited and relatively isolated financial sector. In 1999, an anti-money laundering law (AMLL) for the area administered by Turkish Cypriots went into effect with the stated aim of reducing the number of cash transactions in the “TRNC” as well as improving the tracking of any transactions above $10,000. Banks are required to report to the "Central Bank" any electronic transfers of funds in excess of $100,000. Such reports must include information identifying the person transferring the money, the source of the money, and its destination. Banks, nonbank financial institutions, and foreign exchange dealers must report all currency transactions over $20,000 and suspicious transactions in any amount. Banks must follow a know-your-customer policy and require customer identification. Banks must also submit suspicious transaction reports (STRs) to a five-member “Anti-Money Laundering Committee (AMLC)” which decides whether to refer suspicious cases to the “police” and the “attorney general's office” for further investigation. The five-member committee is composed of representatives of the “police”, “customs”, the “Central Bank”, and the “Ministry of Finance”. However, the AMLL has never been fully implemented or enforced.

In 2005, the “AMLC”, which had been largely dormant for several years, began meeting on a regular basis and encouraging banks to meet their obligations to file STRs. The committee has reportedly referred several cases of possible money laundering to law enforcement for further investigation, but no cases have been brought to court and no individuals have been charged. There have been no successful prosecutions of individuals for money laundering, although one foreign bank owner suspected of having ties to organized crime was successfully extradited. There are significant concerns that law enforcement and judicial authorities lack the technical skills needed to investigate and prosecute financial crimes.

Although the 1999 AMLL prohibits individuals entering or leaving the area administered by Turkish Cypriots from transporting more than $10,000 in currency without prior “Central Bank” authorization, “Central Bank” officials note that this law is difficult to enforce, given the large volume of travelers to and from Turkey. In 2003, Turkish Cypriot authorities relaxed restrictions that limited travel across the UN-patrolled buffer zone. There is also a relatively large British population in the area administered by Turkish Cypriots and a significant number of British tourists. As a result, an informal currency exchange market has developed.

The “Ministries of Finance, Economy and Tourism” are drafting several new anti-money laundering laws that they claim will, among other things, establish an FIU and provide for better regulation of casinos, currency exchange houses, and both onshore and offshore banks. Turkish Cypriot authorities have committed to ensuring that the new legislation meets international standards. However, it is unclear if or when the new legislation will be adopted, and if it is adopted, whether it will ever be fully implemented and enforced. Work on the new bills has been ongoing for more than two years.

There are currently 23 domestic banks in the area administered by Turkish Cypriots. Internet banking is available. The offshore sector consists of 16 banks and approximately 50 companies. The offshore

banks may not conduct business with residents of the area administered by Turkish Cypriots and may not deal in cash. The offshore entities are audited by the "Central Bank" and are required to submit a yearly report on their activities. However, the "Central Bank" has no regulatory authority over the offshore banks and can neither grant nor revoke licenses. Instead, the "Ministry of Finance" performs this function. Since 2000, the Turkish Cypriot authorities have registered one new offshore bank. A new law has come into effect that restricts the granting of new bank licenses to only those banks with licensees in an OECD country or a country with "friendly relations" with the "TRNC."

The 1999 Turkish Cypriot AMLL provided better banking regulations than were previously in force, but as an AML tool it is far from adequate, and without ongoing enforcement, cannot meet its objectives. A major weakness continues to be the many casinos, where a lack of resources and expertise leave that area, essentially unregulated and therefore especially vulnerable to money laundering abuse. The largely unregulated finance institutions, currency exchange houses, and offshore banking sector are also of concern. The Turkish Cypriot authorities should move quickly to enact a new anti-money laundering law, establish a strong, functioning financial intelligence unit, and adopt and implement a strong regulatory environment for all obliged institutions, in particular casinos, money exchange houses, and entities in the offshore sector. Turkish Cypriot authorities should take steps to enhance the expertise of members of the enforcement, regulatory, and financial communities with an objective of better regulatory guidance, the more efficient STR reporting, better analysis of reports, and enhanced use of legal tools available for prosecutions.

## Czech Republic

The Czech Republic's central location in Europe and its relatively new status as a functional market economy have left it vulnerable to money laundering. While various forms of organized crime (narcotics trafficking, trafficking in persons, fraud, counterfeit goods, embezzlement and smuggling) remain the primary source of laundered assets in the country, Czech officials and media outlets have voiced increasing concern about the ability of extremist groups and terrorists to launder or remit money within the country. Domestic and foreign organized crime groups target Czech financial institutions for laundering activity, most commonly by means of financial transfers through the Czech Republic. Banks, currency exchanges, casinos and other gaming establishments, investment companies, and real estate agencies have all been used to launder criminal proceeds. Currency exchanges in the capital and border regions are also considered to be a major problem.

The Czech Republic first criminalized money laundering in September 1995 through additions to its Criminal Code. Although the Criminal Code does not explicitly mention money laundering, its provisions apply to financial transactions involving the proceeds of all serious crimes. A July 2002 amendment to the Criminal Code introduce a new independent offense called "Legalization of Proceeds from Crime." This offense has a wider scope than previous provisions in that it enables prosecution for laundering one's own illegal proceeds (as opposed to those of other parties). The 2002 amendment also stipulated punishments of five to eight years imprisonment for the legalization of proceeds from all serious criminal activity and also called for the forfeiture of assets associated with money laundering.

The Czech anti-money laundering legislation (Act No. 61/1996, Measures Against Legalization of Proceeds from Criminal Activity) became effective in July 1996. A 2000 amendment to the money laundering law requires a wide range of financial institutions to report all suspicious transactions to the Czech Republic's financial intelligence unit (FIU), known as the Financial Analytical Unit (FAU) of the Ministry of Finance. In September 2004, the latest amendments to the money laundering law came into force. The amendments introduced several major changes to the Czech Republic's money laundering laws and harmonized the nation's legislation with the requirements of the Council Directive 2001/97/EC on prevention of the use of the financial system for money laundering (European Union's Second Money Laundering Directive). As a result, the list of covered institutions

now includes attorneys, casinos, realtors, notaries, accountants, tax auditors, and entrepreneurs engaging in transactions exceeding 15,000 euros (approximately $19,440).

The Ministry of Interior is currently drafting legislation implementing the European Union's Third Money Laundering Directive. In connection with this effort, the Czech National Bank is preparing an amendment to the foreign currency law that would introduce new regulations and licensing requirements for currency exchanges. Moreover, new legislation on the "Application of International Sanctions" came into force in April 2006. Under the new law, the FAU has the authority to fine institutions not reporting accounts or other assets belonging to individuals, organizations or countries on which international sanctions have been imposed or those not fulfilling other obligations set by international regulations. Earlier laws restricting financial cooperation with the Taliban (2000) and Iraq (2005) were replaced with the new law.

The Czech Republic had been criticized in the past for allowing anonymous passbook accounts to exist within the banking system. Legislation adopted in 2000 prohibits new anonymous passbook accounts. In 2002, the Act on Banks was amended to abolish all existing bearer passbooks by December 31, 2002, and by June 2003 approximately 400 million euros had been converted to nonbearer passbooks. While account holders can still withdraw money from the accounts for the next decade, the accounts do not earn interest and cannot accept deposits. In 2003, the Czech National Bank introduced new "know your customer" measures, based on the recommendations of both the Financial Action Task Force (FATF) and the Basel Committee, and created an on-site inspection team. New due diligence provisions became effective in January 2003.

Czech authorities require that financial institutions maintain transaction records for a period of ten years. Reporting requirements also apply to persons or entities seeking to enter the Czech Republic. Under the provisions of the anti-money laundering act, anyone seeking to enter or leave the Czech Republic with more than 15,000 Euros in cash, traveler's checks, or other monetary instruments must declare this to customs officials, who are required to forward this information to the FAU. Similar reporting requirements apply to anyone seeking to mail the same amount in cash into or out of the country. In practice, however, the effectiveness of these procedures is difficult to assess. With the accession of the Czech Republic to the EU in 2004, nearly all customs stations on the borders were closed. Although the customs station at the Prague Airport remains operational, detecting the smuggling or transport of large sums of currency by highway is difficult. Reportedly, Chinese and Vietnamese residing locally in the Czech Republic are the most active in cash smuggling across the border.

Since 2000, financial institutions have been required to report all suspicious transactions to the FAU. As the Czech FIU, the FAU has the statutory authority to enforce money laundering and terrorist finance laws. The 2004 amendments to the Anti-Money Laundering Act extended the anti-money laundering/counterterrorist financing responsibilities of the FAU. As a result, the FAU is now authorized to share all information with the Czech Intelligence Service (BIS) and Czech National Security Bureau (NBU) in addition to its ongoing cooperation with the police and customs. It is hoped that this type of information sharing will improve the timeliness and nature of exchanges between the different agencies within the Czech government.

The FAU is an administrative FIU without law enforcement authority and can only investigate accounts for which designated entities have filed suspicious transaction reports. The FAU has the power to ask the banking sector to check a specific individual or organization's account. Since April 2006, they are also able to fine financial institutions for not reporting on accounts or other assets belonging to individuals, organizations, or countries on which international sanctions have been imposed. The FAU has neither the mandate nor the capacity to initiate or conduct criminal investigations. Investigative responsibilities lie with the Financial Police or other Czech National Police body.

There are two law enforcement agencies working closely together on the investigation of money laundering cases. The Financial Police (also known as the Illegal Proceeds and Tax Crime Unit) is the main law enforcement counterpart to the FAU and is also responsible for investigating cases of terrorism financing. The Unit for Combating Corruption and Financial Criminality (UOKFK) has primary responsibility for all financial crime and corruption cases.

Although the FAU conducts investigations based on suspicious transaction reports filed by financial institutions, these examinations only cover a relatively small segment of total financial activity within the Czech Republic. Moreover, the FAU's primary responsibility has been, and remains, identifying cases of tax evasion, which is an endemic problem in the Czech Republic. Recently, the FAU has focused on the growing problem of embezzlement of European Structural Funds and has already seized 220 million crowns (approximately $10 million) of suspected embezzled funds. The law facilitates the seizure and forfeiture of bank accounts. A financial institution that reports a suspicious transaction has the authority to freeze the suspect account for up to 24 hours. However, for investigative purposes, this time limit can be extended to 72 hours in order to give the FAU sufficient time to investigate whether or not there is evidence of criminal activity. Currently, the FAU is authorized to freeze accounts for 72 hours. If sufficient evidence of criminal activity exists, the case is forwarded to the Financial Police, which have another three days to gather the necessary evidence. If the Financial Police are able to gather enough evidence to start prosecution procedures, then the account can stay frozen for the duration of the investigation and prosecution. If, within the 72-hour time limit, the Financial Police fail to gather sufficient evidence to convince a judge to begin prosecution, the frozen funds must be released. These time limits do not apply to accounts owned by individuals or organizations on the UN 1267 Sanctions Committee's consolidated list of suspected terrorists and terrorist organizations. The FAU also has the ability to freeze assets associated with suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list.

While the institutional capacity to detect, investigate, and prosecute money laundering and financial offenses has unquestionably increased in recent years, both the FAU and the Financial Police face staffing challenges. Despite recommendations from both the FATF and the Council of Europe's FATF-style regional body (MONEYVAL) regarding the need for FAU staff increases, the government lowered its funding and personnel authorizations in 2005. The FAU still remains a relatively small organization, given the scope of its responsibilities. The Financial Police could soon face similar challenges due to changes in the police retirement plan and a perceived lack of political support for independent police work. Reportedly, many senior officers are leaving the police force or to considering early retirement. The departure of senior officials would have devastating effects and would hinder not only the Financial Police, but the organized crime unit, anticorruption unit, and other critical police organizations as well. Most troubling is the proposed dissolution of the Financial Police into other police units. The creation of the Financial Police was based on EU recommendations and these changes would possibly lead to a loss of EU funding and would negatively impact police morale. Observers believe this action would have a serious negative effect on the government's ability to investigate and prosecute money laundering and terrorist finance cases.

Despite these staffing challenges, an increase in the government's political will and attention to the problems of money laundering and financial crimes has slightly improved the results of law enforcement and prosecutorial efforts. Prior to 2004, the Czech Republic had not successfully prosecuted a money laundering case. However, in 2004 the Ministry of Justice achieved its first four convictions against individuals attempting to legalize the proceeds from crime. Unfortunately, sentences were very low and consisted of probation. In 2005, 23 alleged offenders were prosecuted and three were convicted. In the first six months of 2006, courts increased convictions to 5 individuals. However; only 6 people were prosecuted during the same time period, a marked decrease from the previous year. Sentences were again low including suspended sentences or fines. An ongoing issue in

criminal prosecutions is that law enforcement must prove that the assets in question were derived from criminal activity. The accused is not obligated to prove that the property or assets were acquired legitimately.

The number of suspicious transaction reports transmitted to the FAU in 2005 grew slightly after a significant jump in 2004. The number of inquiries evaluated and forwarded to law enforcement doubled in 2005. This trend is interpreted as evidence of the active participation of obliged entities in the anti-money laundering regime and police suspicion of financial activities of groups and individuals suspected of some cooperation with terrorism groups. There were 3,267 suspicious transactions reported in 2004, and 3,404 in 2005. From January through September 2006, there were 2,043 reports of suspicious transactions. The number of reports forwarded to the police in 2004 by the FAU was 103. This number rose significantly in 2005 to 208. From January through September 2006, the number of reports forwarded to the police was 102. Every case that was passed to law enforcement was investigated. In 2005, the FAU received 130 assistance requests from abroad and sent 69 requests abroad. During the first nine months of 2006, the FAU received 84 requests and sent out 69 requests. From January to October 2006, the Financial Police's Department of Criminal Proceeds and Money Laundering investigated 76 cases and seized assets valued at 1.42 billion crowns (approximately $64.6 million). This figure is a significant increase over 2005, when the Department investigated 99 cases and seized assets valued at roughly 931 million crowns (approximately $42.3 million) and a monumental upsurge when compared to 2004 when the Department investigated 139 cases and seized assets only valued around 2 million crowns (approximately $91,000). Regarding drug cases, the Department participated in 12 cases in 2005 investigated by the Czech National Drug Headquarters, and seized assets valued at 48 million crowns (approximately $2 million) including three cars. Although the National Drug Headquarters continues close cooperation with the Czech Financial Police, during the first half of 2006, the amount of successfully seized assets from two cases decreased significantly to 1.34 million crowns (approximately $61,000).

In October 2005, the Czech Parliament ratified the UN International Convention for the Suppression of the Financing of Terrorism. This was a major step in that it marked both the implementation of the recommendations from international bodies and the completion of the statutory and organizational reforms required to effectively confront this issue. The Czech Government approved the National Action Plan of the Fight against Terrorism for 2005-2007 in November 2005. This document covers topics ranging from police work and cooperation to protection of security interests, enhancement of security standards, and customs issues. One of the major priorities contained in the plan continues to be the fight against terrorist financing.

In November 2004, the Czech Government amended the Criminal Code and enacted new definitions for terrorist attacks and terrorist financing. A penalty of up to 15 years imprisonment can be imposed on those who support terrorists financially, materially or by other means. Also, in addition to reporting all suspicious transactions possibly linked to money laundering, obliged institutions are now required to report all transactions suspected of being tied to terrorist financing. Multilateral bodies generally agree that the Czech Republic currently possesses an adequate regulatory basis with which to combat money laundering and terrorist financing.

In general, Czech authorities have been reliable partners in the battle against terrorist financing. Although the terrorist finance threat in the Czech Republic is generally modest, there is reason to believe that there has recently been an increased possibility of terrorist support activities in the country, and officials have publicly discussed the discovery of small hawala networks remitting funds from the Czech Republic to other parts of the world. The Czech Republic has specific laws criminalizing terrorist financing and legislation permitting rapid implementation of UN and EU financial sanctions, including action against accounts held by suspected terrorists or terrorist organizations. A governmental body called the Clearinghouse, instituted in 2002, was established to streamline the collection of information from institutions in order to enhance cooperation and response

to a terrorist threat. The Clearinghouse meets only in necessary cases. The FAU is currently distributing lists of designated terrorists to relevant financial and governmental bodies. Czech authorities have been cooperative in the global effort to identify suspect terrorist accounts. An amendment to the anti-money laundering law in 2000 requires financial institutions to freeze assets that belong to suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committees consolidated list. To date, two suspect accounts have been identified in Czech financial institutions based on the information provided by the United States. The accounts have been frozen and contain $500,000.

Although Czech law authorizes officials to use asset forfeiture, it is a relatively new tool and that is not widely used. It was introduced into the criminal system in 2002 and allows judges, prosecutors, or the police (with the prosecutor's assent) to freeze an account or assets if evidence indicates that the contents were used, or will be used, to commit a crime, or if the contents are proceeds of criminal activity. In urgent cases, the police can freeze the account without the previous consent of the prosecutor, but within 48 hours have to inform the prosecutor, who then confirms the freeze or releases the funds. An amendment to the 2004 Law on the Administration of Asset Forfeiture in Criminal Procedure implemented provisions and responsibilities overseeing the administration and storage of seized property and appoints the police as responsible for the administration of seized assets as well.

A recent amendment of Czech Criminal Procedure Code and Penal Code came into force in July 2006, bringing several positive changes to asset forfeiture and seizure. The law, as newly amended, now allows for the freezing and confiscation of the value of any asset (including immovable assets) and is not limited to property. These provisions allow the police and prosecutors to effectively seize assets gained in illicit activity previously shielded by family members. The law allows for the seizure of substitute asset values as well as asset values not belonging to the criminal and appoints the police as responsible for administration of seized assets.

The Czech Republic has signed memoranda of understanding (MOUs) on information exchange with 22 countries, including new agreements with Australia and Canada. The Czech Republic also has a formalized agreement with Europol since 2002. The FAU is a member of the Egmont Group, and is also authorized to cooperate and share information with all of its international counterparts, including those not part of the Egmont Group. The Czech Republic actively participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). Cooperation and information exchange with international counterparts or other international organizations has a foundation in Czech law.

The Czech Republic is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. The Czech Republic is also a party to the World Customs Organization's Convention on Mutual Administrative Assistance for the Prevention, Investigation and Repression of Customs Offenses as well as the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

The United States and the Czech Republic have a Mutual Legal Assistance Treaty (MLAT), which entered into force on May 7, 2000, as well as an extradition treaty that has been in effect since 1925. In May 2006, the United States and the Czech Republic signed a supplemental extradition treaty and a supplemental MLAT to implement the U.S.-EU Agreements on these subjects; but these instruments have not yet been ratified.

The Czech Republic has made progress in its efforts to strengthen its money laundering regime, as demonstrated by its ratification in 2005 of the UN International Convention on the Suppression of the Financing of Terrorism and its expanded capacity to enforce existing money laundering regulations despite the threat of future personnel shortages. However, further improvement is still needed. The

Czech Republic has to date made only incremental and limited progress in its law enforcement efforts. Prosecutions are still infrequent and penalties have been far too light to serve as an effective deterrent. Standards of proof remain extremely high and assets forfeiture has not yet become a standard tool used by prosecutors and judges, although the government has given law enforcement the tools for seizing illicit assets shielded by family members. Czech law enforcement and customs authorities should intensify efforts to monitor underground markets and informal remittance systems, such as hawala, used often used by the immigrant communities. Many of these underground systems are based on the misuse of trade. However, changes under discussion to disband the Financial Police are troubling. Doing so would have a negative impact on the government's ability to investigate and prosecute money laundering and terrorist finance cases. The Czech Republic should ratify the UN Convention against Transnational Organized Crime and UN Convention against Corruption.

## Dominica

The Commonwealth of Dominica initially sought to attract offshore dollars by offering a wide range of offshore financial services, low fees and minimal government oversight. A rapid expansion of Dominica's offshore sector without proper supervision made it attractive to international criminals and vulnerable to official corruption. In response to international criticism, Dominica enacted legislation to address many of the deficiencies in its anti-money laundering regime. In September 2006, Dominica announced its intentions to revive its offshore sector through the creation and development of new products and conditions. This includes adjustments to Dominica's economic citizenship program to encourage investors to fund Dominican business projects in exchange for citizenship.

Dominica's financial sector includes one offshore and four domestic banks, 17 credit unions, approximately 11,452 international business companies (IBCs) (a significant increase from 1,435 in 2002), 19 insurance agencies, six money service businesses, one building and loan society, and three operational internet gaming companies (although reports indicate more internet gaming sites exist). There are no free trade zones in Dominica.

Under Dominica's economic citizenship program, individuals can purchase Dominican passports and, in the past, official name changes for approximately $75,000 for an individual and $100,000 for a family of up to four persons. Although not very active, Dominica's economic citizenship program is not adequately regulated. Individuals from the Middle East, the former Soviet Union, the Peoples' Republic of China and other foreign countries have become Dominican citizens and entered the United States via a third country without visas. Subjects of United States criminal investigations have been identified as exploiting Dominica's economic citizenship program in the past.

In June 2000, the Financial Action Task Force (FATF) placed Dominica on its Non-Cooperative Countries and Territories (NCCT) list. As a result, Dominica implemented and revised anti-money laundering reforms and was removed from the NCCT list in October 2002. One of the reforms created was an Offshore Financial Services Council (OFSC). The OFSC's mandate is to advise the Government of the Commonwealth of Dominica (GCOD) on policy issues relating to the offshore sector and to make recommendations with respect to applications by service providers for licenses.

The Eastern Caribbean Central Bank (ECCB) acts as the primary supervisor and regulator of onshore banks in Dominica. A December 2000 agreement between the OFSC and the ECCB places Dominica's offshore banks under the dual supervision of the ECCB and the GCOD Financial Services Unit (FSU). In compliance with the agreement, the ECCB assesses applications for offshore banking licenses, conducts due diligence checks on applicants, and provides a recommendation to the Minister of Finance. The ECCB also conducts on-site inspections for anti-money laundering compliance of onshore and offshore banks in Dominica. The ECCB is unable to share examination information directly with foreign regulators or law enforcement personnel. The Minister of Finance is required to seek advice from the ECCB before exercising his powers with respect to licensing and enforcement.

The Offshore Banking (Amendment) Act 2000 prohibits the opening of anonymous accounts, prohibits IBCs from direct or indirect ownership of an offshore bank, and requires disclosure of beneficial owners and prior authorization to changes in beneficial ownership of banks. All offshore banks are required to maintain a physical presence in Dominica and have available for review on-site books and records of transactions.

The International Business Companies (Amendment) 2000 requires bearer shares to be kept with a registered agent who is required to maintain a register with the names and addresses of beneficial owners. Additional amendments to the Act in September 2001 require previously issued bearer shares to be registered. IBCs are not required to have a physical presence, nor do they have to file annual financial reports. IBCs are restricted from conducting local business activities. The Act empowers the FSU to "perform regulatory, investigatory, and enforcement functions" over IBCs. The International Business Unit (IBU) of the Ministry of Finance supervises and regulates offshore entities and domestic insurance companies.

The Money Laundering Prevention Act (MLPA) of December 2000, as amended in July 2001, criminalizes the laundering of proceeds from any indictable offense. In addition, the law applies not only to narcotics-related money laundering, but also to the illicit proceeds of all criminal acts, whether committed in Dominica or elsewhere. The MLPA overrides secrecy provisions in other legislation and requires financial institutions to keep records of transactions for at least seven years. The MLPA requires a wide range of financial institutions and businesses, including any offshore institutions, to report suspicious transactions simultaneously to the Money Laundering Supervisory Authority (MLSA) and Dominica's financial intelligence unit (FIU). Additionally, financial institutions are required to report any transaction over $5,000. The MLPA also requires persons to report cross-border movements of currency that exceed $10,000 to the FIU.

The MLSA is authorized to inspect and supervise nonbank financial institutions and regulated businesses for compliance with the MLPA. The MLSA consists of five members: a former bank manager, the IBU manager, the Deputy Commissioner of Police, a senior state attorney and the Deputy Comptroller of Customs. The MLSA is also responsible for developing anti-money laundering policies, issuing guidance notes and conducting training. The May 2001 Money Laundering Prevention Regulations apply to all onshore and offshore financial institutions including banks, trusts, insurance companies, money transmitters, regulated businesses and securities companies. The regulations specify client identification requirements, record keeping, and suspicious transaction reporting procedures, and require compliance officers and training programs for financial institutions. The regulations require that the true identity of the beneficial interests in accounts be established, and mandate the verification of the nature of the business and the source of the funds of the account holders and beneficiaries. Reporting entities are protected by law. Anti-Money Laundering Guidance Notes, also issued in May 2001, provide further instructions for complying with the MLPA and provide examples of suspicious transactions to be reported.

The FIU was also established under the MLPA and became operational in August 2001. The FIU is comprised of two full time staff members: a director and a financial analyst/investigator. A police officer with training in financial investigations is also assigned to the FIU on an as-needed basis. The FIU analyzes suspicious transaction reports (STRs) and cross-border currency transactions, forwards appropriate information to the Director of Public Prosecutions, and liaisons with other jurisdictions on financial crimes cases. The FIU has access to the records of financial institutions and other government agencies, with the exception of the Inland Revenue Division. In 2005, the FIU received 19 STRs, which is a significant decrease from the 122 STRs received in 2004. The decline continued in 2006 with the FIU receiving only six STRs.

The MLPA provides for freezing of assets for seven days by the FIU, after which time a suspect must be charged with money laundering or the assets released. Under the Act No. 20 of 2000 and Act No. 3

of 2003, all assets that can be linked to any individual or legitimate business under investigation can be seized or forfeited, providing that the amount seized or forfeited does not exceed the total benefit gained by the subject from the crime committed. The court can order the confiscation of frozen assets. Pursuant to the MLPA, tangible confiscated assets such as vehicles or boats are forfeited to the GCOD. Intangible assets such as cash or bank accounts are split between the Forfeiture Fund and the Government Consolidated Fund by 80 and 20 percent, respectively. The total amount of nonterrorist related assets frozen, forfeited and/or seized in the past year was $55,481, up from zero the year before.

There are no known convictions on money laundering charges in Dominica. In 2006, a French national—under investigation since 2004 for misappropriation of funds from Guadeloupe nationals—was arrested for attempting to obtain a line of credit through fraudulent wire transfers. In 2005, a Haitian national was arrested for human trafficking and money laundering. The GCOD also filed criminal complaints and is working with the United States authorities on a case against St. Regis University for issuing fraudulent degrees and laundering the proceeds in an offshore bank

On June 5, 2003, Dominica enacted the Suppression of Financing of Terrorism Act, which criminalizes the financing of terrorism. The Act also provides authority to identify, freeze and seize terrorist assets, and to revoke the registration of charities providing resources to terrorists. The MLSA and the Office of the Attorney General supervise and examine financial institutions for compliance with counterterrorist financing laws and regulations. The GCOD circulates the United Nations 1267 Sanctions Committee list to financial institutions, but to date, no accounts associated with terrorists or terrorist entities have been found in Dominica. The GCOD has not taken any specific initiatives focused on alternative remittance systems.

In May 2000, a mutual legal assistance treaty between Dominica and the United States entered into force. The GCOD also has a tax information exchange agreement with the United States. The MLPA authorizes the FIU to exchange information with foreign counterparts. The Exchange of Information Act 2002 provides for information exchange between regulators.

Dominica is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). The FIU became a member of the Egmont Group in June 2003. Dominica is a party to the 1988 UN Drug Convention. The GOCD has neither signed nor ratified the UN Convention against Transnational Organized Crime or the UN Convention against Corruption. Dominica acceded to the UN International Convention for the Suppression of the Financing of Terrorism and to the Inter-American Convention against Terrorism in September 2004.

The Government of the Commonwealth of Dominica should fully implement and enforce the provisions of its legislation and provide additional resources for regulating offshore entities, particularly international business companies (IBCs). Dominica should continue to develop the FIU to enable it to fulfill its responsibilities and cooperate with foreign authorities. The GOCD should eliminate its program of economic citizenship.

## Dominican Republic

The Dominican Republic is a major transit country for drug trafficking. Financial institutions in the Dominican Republic engage in currency transactions involving international narcotics trafficking proceeds that include significant amounts of U.S. currency or currency derived from illegal drug sales in the United States. The smuggling of bulk cash by couriers and the use of wire transfer remittances are the primary methods for moving illicit funds from the United States into the Dominican Republic. Once in the Dominican Republic, currency exchange houses, money remittance companies, real estate and construction companies, and casinos facilitate the laundering of these illicit funds.

The 2003 collapse of the country's third largest bank, Banco Intercontinental (Baninter), is a significant example of the corruption and money laundering scandals that plague the financial sector. The Baninter case saw approximately $2.2 billion evaporate over the course of just a few years due to the fraudulent accounting schemes orchestrated by senior officials. The trial phase began in mid-2006, but remains mired in procedural delays that could jeopardize the entire case. The failure of Baninter and two other banks (Banco Mercantil and Bancredito) cost the Government of the Dominican Republic (GODR) in excess of $3 billion and severely destabilized the country's finances. Criminal prosecutions are underway in all three cases. The GODR negotiated an International Monetary Fund (IMF) standby loan in August 2003 to help cover the costs of the failures. The IMF insisted on extensive changes in laws and procedures in order to improve banking supervision. Though legislative changes have been made, full implementation of IMF requirements lags.

The enactment of Act 17 of December 1995 (the 1995 Narcotics Law) made narcotics-related money laundering a criminal offense. To update its anti-money laundering legislation in line with international standards, the GODR passed Law No. 72-02 in 2002 to expand money laundering predicate offenses beyond illegal drug activity to include other serious crimes, such as illicit trafficking in human beings or human organs, arms trafficking, kidnapping, extortion related to recordings and electronic tapes, theft of vehicles, counterfeiting of currency, fraud against the state, embezzlement, and extortion and bribery related to drug trafficking. Law 183-02 further imposes financial penalties on institutions that engage in money laundering. The GODR is currently considering an amendment to this law that would add criminal penalties to perpetrators of financial crimes.

Under Decree No. 288-1996 of the Superintendence of Banks, banks, currency exchange houses and stockbrokers are required to know and identify their customers, keep records of transactions (five years), record currency transactions greater than $10,000, and file suspicious transactions reports (STRs). Law No. 72-02 enhances requirements for customer identification, record keeping of transactions, and reporting of STRs. Law 72-02 also extends reporting requirements to numerous other financial and nonfinancial sectors, including securities brokers, the Central Bank, cashers of checks or other types of negotiable instruments, issuers/sellers/cashers of travelers checks or money orders, credit and debit card companies, fund remittance companies, offshore financial service providers, casinos, real estate agents, automobile dealerships, insurance companies, and certain commercial entities such as those dealing in firearms, metals, archeological artifacts, jewelry, boats and airplanes. The law mandates that these entities must report suspicious transactions as well as all currency transactions exceeding $10,000. Moreover, the legislation requires individuals to declare cross-border movements of currency that are equal to or greater than the equivalent of $10,000 in domestic or foreign currency.

The Unidad de Inteligencia Financiera (UIF) was created in 1997 as the financial intelligence unit (FIU) of the Dominican Republic. The UIF, a department within the Superintendence of Banks, receives financial disclosures and STRs from reporting entities in the financial sector. In 2002, Law 72-02 created the Unidad de Análisis Financiero (Financial Analysis Unit, or UAF) as a second FIU that reports to the National Anti-Money Laundering Committee, and has the mandate to receive financial disclosures and STRs from both financial and nonfinancial reporting entities.

According to the GODR, the UAF has replaced the UIF as the FIU of the Dominican Republic. However, the UAF began operating in May 2005, and the UIF has not ceased operations. Therefore, it appears that a duality of FIU functions continues to exist between these two units. For instance, financial reporting entities may report to either the UIF or the UAF, while nonfinancial reporting entities must report to the UAF. For 2006, the UAF received 229 STRs and 22,610 reports of currency transaction reports. The majority of the reports the UAF received were transferred from the UIF. The UIF, which became a member of the Egmont Group in 2000, lost its membership in November 2006 as it is no longer the legally recognized FIU of the Dominican Republic. The UAF anticipates

applying for Egmont membership once a full transition of FIU functions and responsibilities are complete and the GODR has formally criminalized terrorist financing, as the criminalization of terrorist financing is now a requirement for all new members of the Egmont Group.

In 2005, two asset seizure laws were clarified by an executive order stating that the measures set forth in Law No. 78-03 prevail over those contained in Law No. 72-02. Law No. 78-03 permits the seizure, conservation and administration of assets which are the product or instrument of criminal acts pending judgment and sentencing. The 1995 Narcotics Law allows preventive seizures and criminal forfeiture of drug-related assets, and authorizes international cooperation in forfeiture cases.

While numerous narcotics-related investigations were initiated under the 1995 Narcotics Law, and substantial currency and other assets were confiscated, there have been only three successful money laundering prosecutions under this law. In August 2006, the Attorney General's office created a financial crimes unit to actively pursue financial crimes and money laundering investigations to aide in prosecutors' ability to obtain money laundering convictions.

The GODR continues to support U.S. Government efforts to identify and block terrorist-related funds. Although no assets were identified or frozen, the GODR 's efforts to identify and block terrorist-related funds continue through orders and circulars issued by the Ministry of Finance and the Superintendence of Banks that instruct all financial institutions to continually monitor accounts. The GODR has not enacted specific legislation that would criminalize the financing terrorism and provide reporting entities with a legal basis to carry out counterterrorism financing prevention programs.

According to U.S. law enforcement officials, cooperation between law enforcement agencies on drug cases, human trafficking, and extradition matters remains strong. In 2006, the GODR assisted U.S. law enforcement authorities to disrupt a drug-trafficking and money laundering ring transferring $2-3 million in illicit remittances to the Dominican Republic per month.

The United States continues to encourage the GODR to join a mutual legal assistance treaty with the Organization of American States (OAS) and sign related money laundering conventions. The Dominican Republic is a member of the Caribbean Financial Action Task Force (CFATF) and the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The Dominican Republic is a party to the 1988 UN Drug Convention. The GODR has signed, but has not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism. On October 26, 2006, the GODR ratified the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. On August 10, 2006, the Dominican Republic became a party to the Inter-American Convention against Terrorism.

Weak implementation of anti-money laundering legislation leaves the Dominican Republic vulnerable to criminal financial activity. The Government of the Dominican Republic should enhance supervision of the nonfinancial sector, and ensure this sector's compliance with reporting requirements. The Dominican Republic should bolster the operational capacity of the fledgling UAF and ensure a full transition of FIU functions. The GODR should formally criminalize the financing of terrorism.

## Ecuador

With a dollar economy geographically situated between two major drug producing countries, Ecuador is highly vulnerable to money laundering but is not considered an important regional financial center. Because thus far there has not been fully effective control of money laundering, there is no reliable way to judge the magnitude of such activity in the country. In addition to concerns about illicit transactions through financial institutions, there is evidence that money laundering is taking place through trade and commercial activity. Large amounts of unexplained currency entering and leaving Ecuador indicate that transit and laundering of illicit cash are also significant activities. Though

smuggled goods are regularly brought into the country, there is no evidence that they are significantly funded by drug proceeds.

On October 18, 2005, Ecuador's new comprehensive law against money laundering was published in the country's Official Register. The new law, Law 2005-13, criminalizes the laundering of illicit funds from any source and penalizes the undeclared entry of more than $10,000 in cash or other convertible assets. The law calls for the creation of a financial intelligence unit (FIU) under the purview of the National Council Against Money Laundering. Regulations for application of the law and establishment of the FIU were published in April 2006. The FIU director was appointed in November 2006, and the hiring of personnel began in January 2007.

The National Council Against Money Laundering, established under Law 2005-13, is headed by the Procurador General (solicitor general) and includes representatives of all government entities involved in fighting money laundering, such as the Superintendence of Banks and the National Police. The National Council Against Money Laundering will be responsible for administering the freezing and seizure of funds that are identified as originating from illicit sources. A special fund for forfeited assets will be set up in the Central Bank, and these assets will be distributed among government entities responsible for combating money laundering.

Ecuador's first major money laundering case broke in August 2006 with the arrest of approximately a dozen alleged members of a Colombian money laundering operation and the seizure of a large number of assets in Ecuador. Accused drug trafficker Hernan Prada Cortes, recently extradited to the United States from Colombia, had acquired many Ecuadorian businesses and real properties in the names of other persons since 2000. Faced with the need to prosecute successfully this high-visibility case before the new FIU is in place, the GOE is making efforts to resolve pending issues.

Prior to the passage of the 2005 law, the Narcotics and Psychotropic Substance Act of 1990 (Law 108) criminalized money laundering activities only in connection with illicit drug trafficking. Under the new law, money laundering is criminalized in relation to any illegal activity, including narcotics trafficking, trafficking in persons and prostitution, among others. Money laundering is penalized by a prison term of three to nine years, depending upon the amount laundered, as well as a monetary fine.

All entities that fall under the 1994 Financial System Law, including banks, savings and credit institutions, investment companies, stock exchanges, mutual funds, exchange houses, credit card administrators, money transmitters, mortgage companies, insurance companies and reinsurance companies, are required to report all "unusual and unjustified" transactions to the FIU, once it is operational. Obligated entities are also required to report cash transactions exceeding $10,000, establish "know-your-client" provisions, and maintain financial transaction records for ten years. Any person entering or leaving Ecuador with $10,000 or more must file a report with the customs service. Entities or persons who fail to file the required reports or declarations may be sanctioned by the Superintendence of Banks. The FIU may request information from any of the obligated entities to assist in its analysis of suspicious transactions, and cases that are deemed to warrant further investigation will be sent to the Public Ministry. The FIU is also empowered to exchange information with other financial intelligence units on the basis of reciprocity.

Some existing laws may conflict with the detection and prosecution of money laundering. For example, the Bank Secrecy Law severely limits the information that can be released by a financial institution directly to the police as part of any investigation, and the Banking Procedures Law reserves information on private bank accounts to the Superintendence of Banks. In addition, the Criminal Defamation Law sanctions banks and other financial institutions that provide information about accounts to police or advise the police of suspicious transactions if no criminal activity is proven. These obstacles can be overcome by a judge properly issuing an appropriate warrant. However, as a result of this contradictory legal framework, cooperation between other Government of Ecuador

(GOE) agencies and the police has in the past fallen short of the level needed for effective enforcement of money laundering statutes.

Several Ecuadorian banks maintain offshore offices. The Superintendence of Banks is responsible for oversight of both offshore and onshore financial institutions. Regulations are essentially the same for onshore and offshore banks, with the exception that offshore deposits no longer qualify for the government's deposit guarantee. Anonymous directors are not permitted. Licensing requirements are the same for offshore and onshore financial institutions. However, offshore banks are required to contract external auditors pre-qualified by the Superintendence of Banks. These private accounting firms perform the standard audits on offshore banks that would generally be undertaken by the Superintendence in Ecuador. Bearer shares are not permitted for banks or companies in Ecuador.

A free trade zone law was passed in 1991 in order to promote exports, foreign investment, and employment. The law provides for the import of raw materials and machinery free of duty and tax; the export of finished and semi-processed goods free of duty and tax; and tax exemptions for business activities in the government-established zones. Free trade zones have been established in Esmeraldas, Manabi and Pichincha provinces, and a new zone is planned for the site of the new Quito airport. There is no known evidence to indicate that the free trade zones are being used in trade-based money laundering.

Terrorist financing has not been criminalized in Ecuador. The Ministry of Foreign Affairs, Superintendence of Banks and the Association of Private Banks formed a working group in December 2004 to draft a law against terrorist financing. By year-end 2006, the draft law had passed its first debate in Congress. The Superintendence of Banks has cooperated with the U.S. Government in requesting financial institutions to report transactions involving known terrorists, as designated by the United States as Specially Designated Global Terrorists pursuant to Executive Order 13224, or as named on the consolidated list maintained by the United Nations 1267 Sanctions Committee. No terrorist finance assets have been identified to date in Ecuador. The Superintendence would have to obtain a court order to freeze or seize such assets, in the event they were identified in Ecuador. No steps have been taken to prevent the use of gold and precious metals to launder terrorist assets. Currently, there are no measures in place to prevent the misuse of charitable or nonprofit entities to finance terrorist activities.

Ecuador is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. On July 27, 2006, the Government of Ecuador (GOE) ratified the Inter-American Convention against Terrorism. Ecuador is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Financial Action Task Force of South America (GAFISUD). The GOE is scheduled to undergo a mutual evaluation by GAFISUD in 2007. Ecuador and the United States are parties to a bilateral Agreement for the Prevention and Control of Narcotics Related Money Laundering that entered into force in 1993 and an Agreement to Implement the United Nations Convention against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances of December 1988, as it relates to the transfer of confiscated property, securities and instrumentalities. There is also a Financial Information Exchange Agreement (FIEA) between the GOE and the U.S. to share information on currency transactions.

Ecuador is one of only two countries in South America that is not a member of the Egmont Group of financial intelligence units. Now that the necessary legislative framework exists, the GOE should quickly establish a fully functioning FIU that meets the standards of the Egmont Group and the Financial Action Task Force. Ecuador should criminalize the financing of terrorism, which is a prerequisite for membership in the Egmont Group and is necessary in order to fully comply with international anti-money laundering and counterterrorist financing standards. The GOE should also

address items that were not accounted for in the new money laundering legislation, including the abolition of strict bank secrecy limitations and any potential sanctions for financial institutions that report suspicious transactions.

## Egypt, The Arab Republic of

Egypt is not considered a regional financial center or a major money laundering country. The Government of Egypt (GOE) continued financial sector reform in 2006, privatizing the Bank of Alexandria (BOA), the smallest of the four public banks, which was sold to Italy's Sanpaolo IMI. The GOE also undertook initiatives to improve stock market regulation and transparency, stimulate the mortgage sector, reform Central Bank management and restructure public insurance companies. Despite these reforms, Egypt still has a large, informal cash economy, and many financial transactions do not enter the banking system at all. Of the few money laundering cases that have made it to court in the last several years, most involved illegal dealings in antiquities and misappropriation of public funds.

While there is no significant market for illicit or smuggled goods in Egypt, there is evidence that arms are being smuggled across Egypt's border with Gaza. The funding source is unclear, as is the destination of the proceeds. Other than arms, authorities say that the under-invoicing of imports and exports by Egyptian businessmen is still a relatively common practice. The primary goal for businessmen who engage in such activity is reportedly to avoid taxes and customs fees. Customs fraud and invoice manipulation are also found in regional value transfer and countervaluation in hawala transactions. The Ministry of Finance has indicated that more businesses and individuals are filing tax returns as a result of June 2005 tax cuts. Nevertheless, a large portion of Egypt's economy remains undocumented.

At present, money laundering and terrorist financing are not reported to be widespread. Most cases of money laundering that have been detected have involved laundering of money through the formal banking sector. Informal remittance systems are unregulated and therefore pose a potential means for laundering funds. Egyptian authorities claim that informal remittances are not widespread in Egypt, but the number of remittances officially recorded by banks does not match the large number of Egyptians working overseas, in the Gulf and elsewhere. Reports on the number of Egyptian expatriates are contradictory, but the figure generally stated is 5 million. One report claimed that these expatriates transfer remittances amounting to $5 billion annually: $3.3 billion transmitted through official means (i.e., banks, Western Union); and $1.5 billion through informal means. Many overseas workers use informal means due to a lack of trust in or familiarity with banking procedures or the lower costs associated with informal remittance systems. Due to the unregulated nature of informal remittance systems, it is unclear if and to what extent money laundering actually occurs through these systems. Western Union, the only formal cash transfer operator in Egypt, continues to draw customers.

Egypt does not have a high prevalence of financial crimes, such as counterfeiting or bank fraud. There is no evidence that Egyptian institutions engage in currency transactions involving international narcotics trafficking proceeds. Egypt's Law No. 80 of 2002 criminalizes laundering of funds from narcotics trafficking, prostitution and other immoral acts, terrorism, antiquities theft, arms dealing, organized crime, and numerous other activities. The law did not repeal Egypt's existing law on bank secrecy, but it did provide the legal justification for providing account information to responsible civil and criminal authorities. The law established the Money Laundering Combating Unit (MLCU) as Egypt's financial intelligence unit (FIU), which officially began operating on March 1, 2003, as an independent entity within the Central Bank of Egypt (CBE). The administrative regulations of the anti-money laundering (AML) law provide the legal basis by which the MLCU derives its authority, spelled out the predicate crimes associated with money laundering, established a Council of Trustees to govern the MLCU, defined the role of supervisory authorities and financial institutions, and allowed

for the exchange of information with foreign competent authorities. Article 86 of the Penal Code criminalizes the financing of terrorism.

The CBE's Bank Supervision Unit shares responsibility with the MLCU for regulating banks and financial institutions and ensuring compliance with AML law. Under the AML law, banks are required to keep all records for five years, and numbered or anonymous financial accounts are prohibited. The CBE also requires banks to maintain internal systems enabling them to comply with the AML law and has issued an instruction to banks requiring them to examine large transactions. In addition, banks are required to submit quarterly reports showing compliance with respect to their AML responsibilities. Reporting of suspicious transactions is voluntary by banks and nonbank financial institutions.

In 2006, the CBE and MLCU undertook special compliance assessments of all banks operating in Egypt. The assessments consisted of questionnaires and on-site visits to check AML systems in place in banks. Based on the assessments, banks were divided into three categories: fully compliant, partially compliant, and noncompliant. To date, only one bank has been found noncompliant. Where deficiencies were found, banks were notified of corrective measures to be undertaken with a deadline for making the necessary changes and follow-up visits to reassess compliance. Sanctions for noncompliance include issuing a warning letter; imposing financial penalties; forbidding banks to undertake certain activities; replacing the board of directors; and revoking the bank's license. CBE and MLCU officials have indicated that they will continue to conduct comprehensive periodic assessments of all banks.

The CBE also monitors bureaux de change and money transmission companies for foreign exchange control purposes, giving special attention to those accounts with transactions above certain limits. The Capital Market Authority (CMA), which is responsible for regulating the securities markets, has also undertaken the inspection of firms and independent brokers and dealers under its jurisdiction. The inspections were aimed at explaining and discussing AML regulations and obligations, as well as evaluating the implementation of systems and procedures, including checking for an internal procedures manual and ensuring the appointment of compliance officers.

In 2006, an independent insurance regulatory authority was established and charged with supervising insurance companies for compliance with AML laws and regulations. The General Authority for Free Zones and Investment (GAFI) regulates activity in free zones and Special Economic Zones (SEZ). The Ministry of Communication and Information Technology regulates the Postal Authority and the financial services it offers. Egypt allows gambling in casinos located in international hotels, but only foreigners are allowed to enter the casinos. All cash transactions at casinos are performed by licensed banks subject to AML controls. Individuals acting as financial intermediaries, such as lawyers, accountants, and cash couriers, are not currently subject to AML controls, although MLCU officials have indicated that the law will soon be amended to cover the activities of these individuals. The AML law protects institutions and individuals who cooperate with law enforcement officials.

The executive regulations of the AML law lowered the threshold for declaring foreign currency at borders from the equivalent of $20,000 to $10,000. The declaration requirement was also extended to travelers leaving as well as entering the country. Enforcement of this provision is not consistent, however. The Customs Authority also signed an agreement with the MLCU to share information on currency declarations. Further impetus to law enforcement was added on account of reports that Hamas ministers from the Palestinian Authority were crossing the Egypt-Gaza border with large amounts of cash. Egyptian Customs Authorities now pass all reports of foreign currency declarations at the border to the MLCU, and also alert the European Union border guards of individuals crossing the border with large amounts of cash. Authorities claim that the terrorist attacks of the past several years have given extra impetus to law enforcement agencies to thoroughly scrutinize currency imports/exports.

Egypt is not an offshore financial center. Offshore banks, international business companies, and other forms of exempt or shell companies are not permitted in the country. Egypt has 11 public free zones, several private free zones, and one SEZ, though more of the latter may be opened soon. Public free zones are outside of Egypt's customs boundaries, so firms operating within them have significant freedom with regard to transactions and exchanges. The firms may be foreign or domestic, may operate in foreign currency, and are exempt from customs duties, taxes and fees. Private free zones are established by GAFI decree and are usually limited to a single project such as mixing, repackaging, assembling and/or manufacturing for re-export. The SEZs allow firms operating in them to import capital equipment, raw materials, and intermediate goods duty-free and to operate tax-free. Activity in the free zones and SEZs is not subject to Egypt's anti-money laundering law (AML), but there is no indication that the zones are being used for trade-based money laundering schemes or for financing of terrorism.

The MLCU, Egypt's FIU, is an independent entity within the CBE. The MLCU has its own budget and staff, and also has the full legal authority to examine all Suspicious Transaction Reports (STRs) and conduct investigations. Investigations are conducted with the assistance of counterpart law enforcement agencies, including the Ministry of Interior, the National Security Agency, and the Administrative Control Authority. The MLCU shares information with all of these agencies. The unit handles implementation of the AML law, which includes publishing the executive directives. The MLCU takes its direction from a six-member council, which is chaired by the Assistant Minister of Justice for Legislative Affairs. Other members of the council include the Chairman of the CMA, the Deputy Governor of the CBE, a Sub-Minister from the Ministry of Social Solidarity, a representative from the Egyptian Banking Federation, and an expert in financial and banking affairs. In June 2004, the MLCU was admitted to the Egmont Group of FIUs. MLCU has received extensive training by U.S., European, and Australian anti-money laundering and counterterrorist financing authorities.

The Executive Director of the MLCU is responsible for the operation of the FIU and the implementation of the policies drafted by the Council of Trustees. His responsibilities include: proposing procedures and rules to be observed by different entities involved in combating money laundering; presenting these rules and procedures to the Chairman of the Council of Trustees; reviewing the regulations issued by supervisory authorities for consistency with legal obligations and ensuring that they are up to date; ensuring the capability and readiness of the unit's database; exchanging information with supervisory entities abroad; acting as a point of contact within the GOE; preparing periodic and annual reports on the operational status of the unit; and taking necessary action on STRs recommended to be reported to the Office of Public Prosecution.

Since its inception in 2003, the MLCU has received several thousand STRs from financial institutions and has successfully brought several cases to court. Money laundering investigations are carried out by one of the three law enforcement agencies in Egypt, according to the type of predicate offense involved. The Ministry of Interior, which has general jurisdiction for the investigation of money laundering crimes, has a separate AML department that includes a contact person for the MLCU who coordinates with other departments within the ministry. The AML department works closely with the MLCU during investigations. It has established its own database to record all the information it received, including STRs, cases, and treaties. The Administrative Control Authority has specific responsibility for investigating cases involving the public sector or public funds. It also has a close working relationship with the MLCU. The third law enforcement entity, the National Security Agency, plays a more limited role in the investigation of money laundering cases, where the predicate offense threatens national security. The GOE established a national committee for coordinating issues regarding anti-money laundering in late 2005.

In 2002, the GOE passed the Law on Civil Associations and Establishments (Law No. 84 of 2002), which governs the procedures for establishing nongovernmental organizations (NGOs), including their internal regulations, activities, and financial records. The law places restrictions on accepting foreign

donations without prior permission from the proper authorities. Both the Ministry of Social Solidarity and the CBE continually monitor the operations of domestic NGOs and charities to prevent the funding of domestic and foreign terrorist groups.

Although the AML law does not specifically allow for seizure and confiscation of assets from money laundering, the Penal Code authorizes seizure of assets related to predicate crimes, including terrorism. All assets are subject to seizure, including moveable and immoveable property, rights and businesses. Assets can only be seized with an order from the Public Prosecutor, and the agency responsible for seizing the assets depends on the predicate crime. Typically, the CBE seizes cash and the Ministry of Justice seizes real assets. Confiscated assets are turned over to the Ministry of Finance, and the executive regulations of the AML law allow for sharing of confiscated assets with other governments. The Public Prosecutor's office is currently engaged in negotiations to enhance cooperation with other governments on asset seizure and confiscation.

Because of its own historical problems with domestic terrorism, the GOE has sought closer international cooperation to counter terrorism and terrorist financing. The GOE has shown a willingness to cooperate with foreign authorities in criminal investigations, whether they are related to terrorism or narcotics.

In January 2005, the National Committee for Combating Money Laundering and Terrorist Financing was established to formulate general strategy and coordinate policy implementation among the various responsible agencies of the GOE. The committee includes representatives from the Ministries of Interior, Foreign Affairs, Social Affairs, Justice, and the National Security Agency, in addition to the MCLU. The same agencies sit on a National Committee for International Cooperation in Combating Terrorism, which was established in 1998.

The GOE is in the process of replacing its original counterterrorism law, an emergency law enacted in 1981, with a new and updated law. It will reportedly include specific measures against terrorist financing.

The United States and Egypt have a Mutual Legal Assistance Treaty. Egyptian authorities have cooperated with U.S. efforts to seek and freeze terrorist assets. Egypt also has agreements for cooperation on AML issues with the UK, Romania, Zimbabwe and Peru. The CBE circulates to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224. No related assets were identified, frozen, seized, or forfeited in 2006.

Egypt is a founding member of the Middle East and North Africa Financial Action Task Force (MENAFATF) and follows that organization's recommendations on anti-money laundering and counterterrorist financing. In January 2006, Egypt assumed the presidency of MENAFATF for a one-year period. Egypt is a party to the 1988 UN Drug Convention. In March 2004, it ratified the UN Convention against Transnational Organized Crime. In March 2005, it ratified the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Egypt should follow through with its plans to enact an updated law against terrorism that specifically addresses the threat of terrorist financing, including asset identification, seizure and forfeiture. The GOE must also improve its ability to pursue suspicious financial activities and transactions through the entire investigative and judicial process. Egypt should work to increase the number of successful money laundering investigations, prosecutions, and convictions. It should consider ways of improving the MLCU'S feedback on STRs to reporting institutions. It should improve its enforcement of cross-border currency controls, specifically allowing for seizure of suspicious cross-border currency transfers, regardless of whether couriers have followed required

reporting procedures. Egyptian authorities should investigate underground value transfer systems and their possible relationship with money laundering and terrorist finance.

## El Salvador

Located on the Pacific coast of the Central American isthmus, El Salvador has one of the largest and most developed banking systems in Central America. Its most significant financial contacts are with neighboring Central American countries, as well as with the United States, Mexico and the Dominican Republic. The growth of El Salvador's financial sector, the increase in narcotics trafficking, the large volume of remittances through the formal financial sector and alternative remittance systems, and the use of the U.S. dollar as legal tender make El Salvador vulnerable to money laundering. In 2006, approximately $3.3 billion in remittances were sent to El Salvador through the financial system. Most were sent from Salvadorans working in the United States to family members. The quantity of additional remittances that flow back to El Salvador via other methods such as visiting relatives, regular mail and alternative remittance systems is not known.

Most money laundering is conducted by international criminal organizations. These organizations use bank and wire fund transfers from the United States to disguise criminal revenues as legitimate remittances to El Salvador. The false remittances are collected and transferred to other financial institutions until sufficiently laundered for use by the source of the criminal enterprise, usually a narcotics trafficking organization.

Decree 498 of 1998, the "Law Against the Laundering of Money and Assets," criminalizes money laundering related to narcotics trafficking and other serious crimes, including trafficking in persons, kidnapping, extortion, illicit enrichment, embezzlement and contraband. The law also establishes the financial intelligence unit (FIU), the Unidad de Inteligencia Financiera (UIF), within the Attorney General's Office. The UIF has been operational since January 2000. The National Civilian Police (PNC) and the Central Bank also have their own anti-money laundering units.

Under Decree 498, financial institutions must identify their customers, maintain records for a minimum of five years, train personnel in identification of money and asset laundering, establish internal auditing procedures, and report all suspicious transactions and transactions that exceed approximately $57,000 to the UIF. Entities obligated to comply with these requirements include banks, finance companies, exchange houses, stock exchanges and exchange brokers, commodity exchanges, insurance companies, credit card companies, casinos, dealers in precious metals and stones, real estate agents, travel agencies, the postal service, construction companies and the hotel industry. The law includes a safe harbor provision to protect all persons who report transactions and cooperate with law enforcement authorities, and also contains banker negligence provisions that make individual bankers responsible for money laundering at their institutions. Bank secrecy laws do not apply to money laundering investigations.

Cooperation between the Attorney General's Office and the police has resulted in the conviction of two individuals for money laundering offenses, and the arrests of several high-profile individuals suspected of money laundering and other financial crimes. Additionally, the Government of El Salvador (GOES) has recently begun to investigate private companies and financial service providers involved in suspicious financial activities. Despite demonstrating a greater commitment to pursue financial crimes over the previous year, the GOES still lacks sufficient prosecutorial and police resources to adequately investigate and prosecute financial crimes.

The GOES has established a secure computerized communication link between the Attorney General's office and the financial crimes division of the police. In addition to providing communication, the system has a software component that filters, sorts, and connects financial and other information vital

to money laundering investigations. The system became operational in the last quarter of the year and is expected to greatly enhance investigative capabilities.

To address the problem of international transportation of criminal proceeds, Decree 498 requires all incoming travelers to declare the value of goods, cash or monetary instruments they are carrying in excess of approximately $11,400. Falsehood, omission or inaccuracy on such a declaration is grounds for retention of the goods, cash or monetary instruments, and the initiation of criminal proceedings. If, following the end of a 30-day period, the traveler has not proved the legal origin of said property, the Salvadoran authorities have the authority to confiscate it. In 2006, the PNC seized over $2.2 million in undeclared cash from individuals transiting El Salvador's international airport and land border crossings.

The GOES has established systems for identifying, tracing, freezing, seizing and forfeiting narcotics-related and other assets of serious crimes. Forfeited money laundering proceeds are deposited in a special fund used to support law enforcement, drug treatment and prevention, and other related government programs, while funds forfeited as the result of other criminal activity are deposited into general government revenues. Law enforcement agencies are allowed to use certain seized assets while a final sentence is pending. In practice, however, the process does not often result in the forfeiture of funds that are then channeled to counternarcotics operations. There exists no legal mechanism to share seized assets with other countries. Salvadoran law currently provides only for the judicial forfeiture of assets upon conviction (criminal forfeiture), and not for civil or administrative forfeiture. A draft law to reform Decree 498 to provide for civil forfeiture of assets has stalled in the national legislature.

The GOES passed counterterrorism legislation, Decree No. 108, on September 19, 2006. Decree No. 108 further defines acts of terrorism and establishes tougher penalties for the execution of those acts. Article 29 of Decree No. 108 establishes the financing of terrorism as a criminal offense, punishable by a prison term of 20 to 30 years and a monetary fine ranging from $100,000 to $500,000. The law also granted the GOES the legal authority to freeze and seize suspected assets associated with terrorists and terrorism. However, provisions to improve supervision of cash couriers, wire transfers, and financing of nongovernmental organizations (NGOs) that were included in an early draft were not included in the final law.

The GOES has circulated the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list to financial institutions. These institutions are required to search for any assets related to the individuals and entities on the consolidated list. There is no evidence that any charitable or nonprofit entity in El Salvador has been used as a conduit for terrorist financing.

El Salvador has signed several agreements of cooperation and understanding with financial supervisors from other countries to facilitate the exchange of supervisory information, including permitting on-site examinations of banks and trust companies operating in El Salvador. El Salvador is also a party to the Treaty of Mutual Legal Assistance in Criminal Matters signed by the Republics of Costa Rica, Honduras, Guatemala, Nicaragua and Panama. Salvadoran law does not require the UIF to sign agreements in order to share or provide information to other countries. The GOES is party to the Organization of American States (OAS) Inter-American Convention on Mutual Assistance in Criminal Matters, which provides for parties to cooperate in tracking and seizing assets. The UIF is also legally authorized to access the databases of public or private entities. The GOES has cooperated with foreign governments in financial investigations related to narcotics, money laundering, terrorism, terrorism financing and other serious crimes.

El Salvador is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force. The UIF has been a member of the Egmont Group since 2000. The GOES is party to the OAS Inter-

American Convention against Terrorism, the UN International Convention for the Suppression of the Financing of Terrorism, the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. El Salvador is also a signatory to the Central American Convention for the Prevention and Repression of Money Laundering Crimes Related to Illicit Drug Trafficking and Related Crimes.

The Government of El Salvador made advances in 2006 with the passage of counterterrorist financing legislation. El Salvador should continue to expand and enhance its anti-money laundering policies and strengthen its ability to seize and share assets. Remittances are an important sector of the economy, which must therefore be carefully supervised. The GOES should improve supervision of cash couriers and wire transfers as outlined in the Financial Action Task Force (FATF) Special Recommendations on terrorism financing. The GOES should also ensure that sufficient resources are provided to the overburdened Attorney General's office and the financial and narcotics divisions of the police.

## France

France remains an attractive venue for money laundering because of its sizable economy, political stability, and sophisticated financial system. However, France has put in place comprehensive financial controls, and it is an active partner in international efforts to control money laundering and the financing of terrorism.

The Government of France (GOF) first criminalized money laundering related to narcotics trafficking in 1987. In 1988, the Customs Code was amended to incorporate financial dealings with money launderers as a crime and in May 1996 the criminalization of money laundering was expanded to cover the proceeds of all crimes with Law No. 96-392. In 2004, the French Supreme Court ruled that joint prosecution of individuals was possible on both money laundering charges and the underlying predicate offense. Prior to this judgment, the money laundering charge and the predicate offense were considered the same offense and could only be prosecuted as one offense.

Article 324-1 of the Penal Code provides that money laundering is punishable by five years imprisonment and a fine of 375,000 euro (approximately $481,000). With aggravating circumstances such as habitual or organized activity (Article 324-2) or connection with narcotics trafficking (Article 222-38), the punishment increases to ten years imprisonment and a fine of 750,000 euro (approximately $962,000). In 1990, the obligation for financial institutions to combat money laundering came into effect with the adoption of the anti-money laundering (AML) law—now incorporated in the Monetary and Financial Code (MFC) and France's ratification of the 1988 UN Drug Convention. Suspicious transaction reporting is now required for a wide variety of financial and nonfinancial entities, including banks, insurance companies, casinos, and lawyers.

As a member of the European Union (EU), France is obligated to implement all three EU money laundering directives, including Directive 2001/97/EC, which was transposed into domestic French legislation in 2004. With Decree 2006-736 of 26 June 2006, France incorporated the EU's Second Money Laundering Directive into French law. The EU adopted the Third Money Laundering Directive (2005/60/EC) in late 2005, which must be implemented in France by December 15, 2007.

Decree No. 2002-770 of 2002 addresses the functions of France's Liaison Committee against the Laundering of the Proceeds of Crime. This committee is co-chaired by the French financial intelligence unit (FIU), known as the unit for Treatment of Intelligence and Action Against Clandestine Financial Circuits or TRACFIN, and the Justice Ministry. It comprises representatives from reporting professions and institutions, regulators, and law enforcement authorities. The Committee's purpose is to share information with regulated entities and to make proposals to improve the anti-money laundering system.

The Banking Commission supervises financial institutions and conducts regular audits of credit institutions. The Insurance and Provident Institutions Supervision Commission reviews insurance brokers. The Financial Market Authority, which evolved from the merger of the Securities Exchange Commission and the Financial Markets Council, monitors the reporting compliance of the stock exchange and other nonbank financial institutions. The Central Bank (Banque de France) oversees management of the required records to monitor banking transactions, such as those for means of payment (checks and ATM cards) or extensions of credit. Bank regulators and law enforcement can access the system managed by the French Tax Administration for opening and closing of accounts, which covers depository accounts, transferable securities, and other properties including cash assets that are registered in France. These records are important tools in the French arsenal for combating money laundering and terrorism financing.

TRACFIN is responsible for analyzing suspicious transaction reports (STRs) filed by French financial institutions and nonfinancial professions. TRACFIN participates in FINATER, an informal group created within the French Ministry of the Economy, Finance, and Industry in September 2001 to gather information to fight terrorist financing. TRACFIN may exchange information with foreign counterparts that observe similar rules regarding reciprocity and confidentiality of information. TRACFIN works closely with the Ministry of Interior's Central Office for Major Financial Crimes (OCRGDF), which is the main point of contact for Interpol and Europol in France. With the Law of 15 May 2001, TRACFIN can obtain information from senior police officers and central or local governments. The State Prosecutor informs the FIU of final court orders relating to suspicious transactions that have been reported.

TRACFIN received 10,842 STRs in 2004, 11,553 in 2005 and 12,047 in 2006. Approximately 83 percent of STRs are sent from the banking sector. A total of 308 cases were referred to the judicial authorities in 2003, which resulted in 63 convictions. The FIU referred 347 cases in 2004, 405 in 2005 and 411 in 2006.

In addition to STRs, two other types of reports are required to be filed with the FIU. First, a report must be filed with TRACFIN when the identity of the principal or beneficiary remains doubtful despite due diligence; there is no threshold limit for such reporting. Second, a report must be filed in cases where transactions are carried out on behalf of a third party natural person or legal entity (including their subsidiaries or establishments) by a financial entity acting in the form, or on behalf, of a trust fund or any other asset management instrument, when legal or beneficial owners are not known. The reporting obligation can also be extended by decree to transactions carried out by financial entities, on their own behalf or on behalf of third parties, with natural or legal persons, including their subsidiaries or establishments that are domiciled, registered, or established in any country or territory included on the Financial Action Task Force (FATF) list of noncooperative countries or territories.
Laws No. 98-546 and 2001-420, of July 1998 and May 2001 respectively, extended the reporting obligations to new businesses. In addition, the laws ensured that with regard to criminal law, legal proceedings for "criminal conspiracy" are applicable to money laundering. While Law No. 96-392 of 1996 instituted procedures for seizure and confiscation of the proceeds of crime, these laws permit seizure of all or part of property.

Since 1986, French counterterrorism legislation has provided for the prosecution of those involved in the financing of terrorism under the more severe offense of complicity in the act of terrorism. However, in order to strengthen this provision, the Act of November 15, 2001, introduced several new characterizations of offenses, specifically including the financing of terrorism. The offense of financing terrorist activities (Article 421-2-2 of the Penal Code) is defined according to the UN International Convention for the Suppression of the Financing of Terrorism and can result in ten years' imprisonment and a fine of 225,000 euro (about $289,000). Since 2001, TRACFIN has referred 92 cases of suspected terrorist financing to the judicial authorities for prosecution. An additional penalty

of confiscation of the total assets of the terrorist offender has also been implemented. Accounts and financial assets can be frozen through both administrative and judicial measures.

In 2006, the GOF moved to strengthen France's antiterrorism legal arsenal with the Act of 23 January 2006, authorizing video surveillance of public places, including nuclear and industrial sites, airports, and railway stations. The Act requires telephone operators and Internet café owners to keep extensive records, allows greater government access to e-communications, and allows flight passenger lists and identification information to become accessible to counterterrorism officials. It stiffens prison sentences for directing a terrorist enterprise to 30 years and extends the possible period of detention without charge. The Act permits increased surveillance of potential targets of terrorism. It empowers the Minister of the Economy to freeze the funds, financial instruments and economic resources belonging to individuals committing or attempting to commit acts of terrorism, or to companies directly or indirectly controlled by these individuals. By granting explicit national authority to freeze assets, the Act plugs up a potential loophole concerning the freezing of citizen versus resident EU-member assets. Adopted in January 2006, it was expected to enter into force by presidential decree before the end of 2006.

French authorities moved rapidly to freeze financial assets of organizations associated with al-Qaida and the Taliban under United Nations Security Council Resolution 1267. France takes actions against other terrorist groups through the EU-wide "clearinghouse" procedure. Within the Group of Eight, which it chaired in 2003, France has sought to support and expand efforts targeting terrorist financing. Bilaterally, France has worked to improve the capabilities of its African partners in targeting terrorist financing by offering technical assistance. On the operational level, French law enforcement cooperation targeting terrorist financing continues to be strong.

The United States and France have entered into a mutual legal assistance treaty (MLAT), which came into force in 2001. Through MLAT requests and by other means, the French have provided large amounts of data to the United States in connection with terrorist financing. TRACFIN is a member of the Egmont Group and Egmont Committee and has information-sharing agreements with 30 foreign FIUs.

France is a member of the FATF and held the FATF Presidency for a one-year term during 2004-05. It is a Cooperating and Supporting Nation to the Caribbean Financial Action Task Force (CFATF) and an Observer to the Financial Action Task Force of South America (GAFISUD). France is a party to the 1988 UN Drug Convention; the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the UN Convention against Transnational Organized Crime; the UN International Convention for the Suppression of the Financing of Terrorism; and the UN Convention against Corruption.

The Government of France has established a comprehensive anti-money laundering regime. France should continue its active participation in international organizations to combat the domestic and global threats of money laundering and terrorist financing.

## Germany

Germany is one of the largest financial centers in Europe. Most of the money laundering that occurs in Germany relates to white collar crime. Although not a major drug producing country, Germany continues to be a consumer and a major transit hub for narcotics. Both the domestic consumption and the transiting of narcotics are additional sources of money laundering in Germany. According to the German Financial Intelligence Unit's (FIU's) annual report, about three-fourths of the suspicious transaction reports (STRs) filed in Germany cite suspected fraud, forgery and tax evasion. Germany is not an offshore financial center.

In 2002, the German Government (GOG) enacted a number of laws to improve authorities' ability to combat money laundering and terrorist financing. The 2002 measures brought German laws into line with the first and second European Union (EU) Money Laundering Directives, which mandate suspicious activity reporting by a variety of entities, including notaries, accountants, tax consultants, casinos, luxury item retailers, and attorneys.

Germany's Money Laundering Act, amended by the Act on the Improvement of the Suppression of Money Laundering and Combating the Financing of Terrorism of August 8, 2002, criminalizes money laundering related to narcotics trafficking, fraud, forgery, embezzlement, and membership in a terrorist organization. It also increases due diligence and reporting requirements for banks and financial institutions and requires financial institutions to obtain customer identification for transactions conducted in cash or precious metals exceeding 15,000 euros (approximately $19,520). The legislation mandates more comprehensive background checks for owners of financial institutions and tighter rules for credit card companies. Banks must report suspected money laundering to the FIU located within the Federal Office of Criminal Investigation (Bundeskriminalamt or BKA), as well as to the State Attorney (Staatsanwaltschaft).

The GOG has directed the Interior Ministry to draft new legislation to implement the third EU Money Laundering Directive by December 2007. In addition to requiring that EU member states implement the Financial Action Task Force's (FATF) Forty Recommendations, the directive contains further provisions on customer due diligence and other internal risk-management measures to prevent money laundering. The directive calls for improved integrity and transparency to help prevent financial crime and improve information exchange between the public and private sectors. The EU requirement also expands reporting requirements to encompass transactions which support the financing of terrorism or would do so if actually effected.

In May 2002, the German banking, securities, and insurance industry regulators merged into a single financial sector regulator known as the Federal Financial Supervisory Authority (BaFIN). Germany's anti-money laundering (AML) legislation requires that BaFIN compile a centralized register of all bank accounts in Germany, including 300 million deposit accounts. As a result, in 2003 BaFIN established a central database with electronic access to all key account data held by banks in Germany. Banks cooperate with authorities and use computer-aided systems to analyze customers and their financial dealings to identify suspicious activity. Many of Germany's banks have independently developed risk assessment software to screen potential and existing clients and to monitor transactions for suspicious activity.

In 2002, Germany established a single, centralized, federal FIU within the BKA. Staffed with financial market supervision, customs, and legal experts, the FIU is responsible for developing a central database to use when analyzing cases and responding to reports of suspicious transactions. Another unit under the BKA, the Federal Financial Crimes Investigation Task Force, houses twenty BKA officers and customs agents.

In 2005, obligated entities submitted more than 8,000 STRs to the FIU. Approximately forty-five percent of the persons cited in German STRs are non-German nationals. Eighty-five percent of the reports resulted in investigative action. As with other crimes, actual enforcement under the German federal system is carried out at the state (sub-federal) level. Each state has a joint customs/police/financial investigations unit (GFG), which works closely with the federal FIU. In 2004, that the most recent year for which data is available, there were 109 money laundering convictions. The State Attorney can order a freeze of accounts when warranted.

As an EU member, Germany complies with a recent EU regulation requiring accurate originator information on funds transfers—but only for transfers into or out of the EU, not within the EU. FATF Special Recommendation Seven on Terrorist Financing, which governs wire transfers, however, requires such information on all cross-border transfers, including transfers between EU members.

Germany moved quickly after September 11, 2001, to identify and correct the weaknesses in its laws that had permitted terrorists to live and study in Germany. The first reform package closed loopholes that had permitted members of foreign terrorist organizations to engage in fundraising in Germany (e.g., through charitable organizations) that extremists had exploited to advocate violence. Subsequently, Germany increased its law enforcement efforts to prevent misuse of charitable entities. Germany has used its Law on Associations (Vereinsgesetz) to take administrative action to ban extremist associations that "threaten the democratic constitutional order."

The second reform package, which went into effect January 1, 2002, enhances the capabilities of federal law enforcement agencies and improves the ability of intelligence and law enforcement authorities to coordinate efforts and to share information on suspected terrorists. The law also provides Germany's internal intelligence service with access to information from banks and financial institutions, postal service providers, airlines, and telecommunication and internet service providers. Another proposed counterterrorism reform, will further streamline and simplify security agencies' access to German financial, travel, and telephone records. In 2002, the GOG also added terrorism and terrorist financing to its list predicate offenses for money laundering, as defined by Section 261 of the Federal Criminal Code. A 2002 amendment of the Criminal Code allows prosecution of members of terrorist organizations based outside Germany

An immigration law, effective January 2005, contains provisions designed to facilitate the deportation of foreigners who support terrorist organizations.

A November 2003 amendment to the Banking Act created a broad legal basis for BaFIN to order freezes of assets of suspected terrorists who are EU residents, although authorities concentrate on financial assets. While BaFIN's system allows for immediate identification of financial assets for potential freezes and German law enforcement authorities can freeze accounts for up to nine months, money cannot be seized until authorities prove in court that the funds were derived from criminal activity or intended for terrorist activity. Sanctions imposed by the United Nations Security Council (UNSC) are exempted from the rule.

Germany participates in United Nations and EU processes to monitor and freeze the assets of terrorists. The names of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanctions Committee's consolidated list and those designated by EU or German authorities are regularly disseminated to German financial institutions. In 2005, authorities found and froze less than 20,000 euros (approximately $26,000) in connection with names appearing on the 1267 consolidated list. A court can order the freezing of nonfinancial assets, but Germany typically does not do so, even when the action is pursuant to EU or UNSCR 1267 listings. Germany and several other EU member states have taken the view that the EU Council Common Position requires, at a minimum, a criminal investigation to establish a sufficient legal basis for freezes under the EU Clearinghouse process.

Proceeds from asset seizures and forfeitures are paid into the federal government treasury. German authorities cooperate with U.S. authorities to trace and seize assets to the full extent allowed under German laws. German law does not allow for sharing forfeited assets with other countries.

Since 1998, the GOG has licensed and supervised money transmitters, shut down thousands of unlicensed money remitters, and issued anti-money laundering guidelines to the industry. A 1998 German law requires individuals to declare when they are entering, departing, or transiting the country with over 15,000 euros (approximately $19,400). A new European Union (EU) law, applicable to all EU members, is expected to take effect in June 2007 and will lower this amount to 10,000 euros (approximately $13,000)

Germany considers the activities of alternative remittance systems such as hawala to be banking activities. Accordingly, German authorities require bank licenses for money transfer services, thus allowing authorities to prosecute unlicensed operations and maintain close surveillance over

authorized transfer agents. BaFIN has investigated more than 2,500 cases of unauthorized financial services since 2003. It closed down more than 200 informal financial networks in 2005. There are currently 52 legally licensed money transfer services in Germany.

Germany exchanges law enforcement information with the United States through bilateral law enforcement agreements and informal mechanisms. United States and German authorities have conducted joint investigations. German law enforcement authorities cooperate closely at the EU level, such as through Europol. Germany has Mutual Legal Assistance Treaties (MLATs) with numerous countries. The MLAT with the United States was signed in October 2003. On July 27, 2006, the U.S. Senate ratified the MLAT; once the German parliament ratifies it, the two sides will exchange letters to bring the MLAT into force. In addition, the U.S.-EU Agreements on Mutual Legal Assistance and Extradition are expected to further improve U.S.-German legal cooperation.

Germany is a member of the FATF, the EU and the Council of Europe. Its FIU is a member of the Egmont Group. Germany is party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Germany has signed, but not yet ratified, the UN Convention against Corruption.

The Government of Germany's anti-money laundering laws and its ratification of international instruments underline Germany's continued efforts to combat money laundering and terrorist finance. Germany should amend its wire transfer legislation to ensure that origination information applies to all cross-border transfers, including those within the EU. It should also amend legislation to waive the asset freezing restrictions in the EU Clearinghouse for financial crime and terrorism financing, so that the freezing process does not require a criminal investigation. German legislation should be amended to allow asset sharing with other countries. Germany should ratify the UN Convention against Corruption.

## Gibraltar

Gibraltar is a largely self-governing overseas territory of the United Kingdom (UK), which assumes responsibility for Gibraltar's defense and international affairs. As part of the European Union (EU), Gibraltar is required to implement all relevant EU directives, including those relating to anti-money laundering.

The Drug Offenses Ordinance (DOO) of 1995 and Criminal Justice Ordinance to Combat Money Laundering criminalize money laundering related to all crimes. These ordinances also mandate suspicious transaction reporting for the financial sector and for designated nonfinancial businesses, which include banks, mutual savings companies, insurance companies, financial consultants, postal services, exchange bureaus, attorneys, accountants, financial regulatory agencies, unions, casinos, charities, lotteries, car dealerships, yacht brokers, company formation agents, dealers in gold bullion, and political parties. Obliged entities must submit suspicious transactions reports (STRs) to Gibraltar's financial intelligence unit (FIU).

The Financial Services Commission (FSC) regulates and supervises Gibraltar's financial services industry. Because of statutory requirements, the FSC must match the supervisory standards set by the UK. The FSC issues comprehensive AML Guidance Notes, which have the force of law, to clarify the obligations of Gibraltar's financial service providers. Financial institutions must retain records for at least five years from the date of the most recent transaction. If the obligated institution has submitted an STR to the FIU, or when a client or transaction is under investigation, it must maintain any relevant record even if the five year mandate has expired. Offshore banks are subject to the same legal and supervisory requirements as onshore.

The FSC also licenses and regulates the activities of trust and company management services, insurance companies, and collective investment schemes. The Government of Gibraltar (GOG)

permits internet gaming, and maintains a licensing regime for that sector. Gibraltar has circulated guidelines for correspondent banking, politically exposed persons, bearer securities, and "know your customer" (KYC) procedures.

The 2001 "Terrorism (United Nations Measures) (Overseas Territories) Order" criminalizes terrorism financing. Under this Order, if a financial institution suspects or knows that a customer is a terrorist or is linked to terrorism, including terrorist financing, the institution must report that customer.

In 1996, Gibraltar established the Gibraltar Coordinating Center for Criminal Intelligence and Drugs (GCID) as a sub-unit of the Gibraltar Criminal Intelligence Department. The GCID serves as Gibraltar's FIU. As such, it serves as the central point for receiving both financial and terrorism-related disclosures and receives, analyzes, and disseminates STR information filed by obliged institutions, The GCID is staffed mainly with police and customs officers, but is independent of any law enforcement agency. The FIU received 108 STRs in 2005, and 118 in 2006. There is a confiscation regime in place, but in order to confiscate assets in a money laundering case, the law enforcement agency investigating the case must be able to link the funds passing through the financial system with the original illicit funds. If this link cannot be substantiated, the funds cannot be confiscated.

The United Kingdom has not extended the Mutual Legal Assistance Treaty between itself and the United States to Gibraltar. However, a 1988 U.S.-UK agreement concerning the investigation of drug-trafficking offenses and the seizure and forfeiture of proceeds and instrumentalities of drug-trafficking was extended to Gibraltar in 1992.

The DOO of 1995 provides for mutual legal assistance with foreign jurisdictions on matters related to narcotics trafficking and related proceeds. Gibraltar has passed legislation to update mutual legal assistance arrangements with the EU and Council of Europe partners. The GOG has implemented the 1988 UN Drug Convention pursuant to its Schengen obligations, but the UK has not extended the Convention to Gibraltar. Gibraltar is a member of the Offshore Group of Banking Supervisors (OGBS), and, in 2004, the GCID became a member of the Egmont Group.

The Government of Gibraltar should continue its efforts to implement a comprehensive anti-money laundering regime capable of thwarting terrorist financing. Gibraltar should put in place reporting requirements for cross-border currency movements. The GOG should pass legislation implementing the Financial Action Task Force's Nine Special Recommendations on Terrorist Financing. Gibraltar should also institute a regulatory scheme for its internet gaming sector in addition to its licensing regime. The GOG should work to implement the standards in the UN Convention against Corruption, the UN Convention against Transnational Organized Crime, and the UN Convention for the Suppression of the Financing of Terrorism.

## Greece

While not a major financial center, Greece is fast becoming a regional financial center in the rapidly developing Balkans. Money laundering in Greece, due to the extensive use of currency in Greek society, is inherently difficult to detect. U.S. law enforcement agencies believe that criminally derived funds are typically not laundered through the banking system; rather they are most commonly invested in real estate, the lottery and a growing stock market. U.S. law enforcement agencies also believe Greece's location has led to a moderate increase in cross-border movements of illicit currency and monetary instruments due to the increasing interconnection of various financial services companies operating in Southeastern Europe and the Balkans. Reportedly, currency transactions involving international narcotics trafficking proceeds are not thought to include significant amounts of U.S. currency.

Greek authorities maintain that Greece is not an offshore financial center, and that there are no offshore financial institutions or international business companies (IBCs) per se operating within the country. However, Greek law (89/1967) provides for the establishment of companies which may be based in Greece but operate solely abroad. These firms are effectively excluded from supervision by Greece's tax authorities as they do not file taxes in Greece. "Law 89" companies, as they are known, mainly operate or claim to operate in the shipping industry and are known for their complex corporate and ownership structures. These firms fall under the authority of non-Greek jurisdictions and often operate through a large number of intermediaries. They could serve as a catalyst for money laundering. Although Greek law allows banking authorities to check these companies' transactions, such audits must be executed in conjunction with other Greek jurisdictions to be effective.

Greek law does not provide for nominee directors or trustees in Greek companies. Bearer shares have been abolished for banks and for a limited number of other companies, but most companies may issue bearer shares. Greece has three free trade zones, located at the ports of Piraeus, Thessalonica, and Heraklion, where foreign goods may be brought in without payment of customs duties or other taxes if they are subsequently transshipped or re-exported. Reportedly there is no indication that these zones are being used in trade-based money laundering or in the financing of terrorism.

The GOG criminalized money laundering derived from all crimes with the 1995 Law 2331/1995, entitled "Prevention of and Combating the Legalization of Income Derived from Criminal Activities." That law imposes a penalty for money laundering of up to ten years in prison and confiscation of the criminally-derived assets. The law also requires that banks and nonbank financial institutions file suspicious transaction reports (STRs) with Greece's financial intelligence unit (FIU). Legislation passed in March 2001 targets organized crime by making money laundering a criminal offense when the property holdings laundered are obtained through criminal activity or cooperation in criminal activity.

In November 2005, the GOG enacted Law 3424/2005, which extends the list of predicate offenses for money laundering to include terrorist financing, trafficking in persons, electronic fraud, and stock market manipulation. It also extends the STR reporting requirements to obligate additional sectors such as auction dealers and accountants. It furthermore broadens the powers of the supervisory authorities and clarifies previous legislation by ending a conflict between confidentiality rules and anti-money laundering regulations imposed on banks and other financial institutions. The law also provides supervisory authorities with greater authority to block transactions where money laundering is suspected and authorizes the FIU director to issue a temporary freeze of assets without the issuance of a court order. Through its Act 2577 9/2006, the Bank of Greece has applied the main provisions of the Third European Union (EU) Directive to all financial institutions. The GOG anticipates that the Directive will be formally transposed into national law in early 2008.

In 2003, Greece enacted legislation (Law 3148) that incorporates EU provisions in directives dealing with the operation of credit institutions and the operation and supervision of electronic money transfers. Under this legislation, the Bank of Greece has direct scrutiny and control over transactions by credit institutions and entities involved in providing services for fund transfers. The Bank of Greece issues operating licenses after a thorough check of the institutions, their management, and their capacity to ensure the transparency of transactions.

The Bank of Greece, through its Banking Supervision Department; the Ministry of National Economy and Finance, through its Capital Market Commission; and the Ministry of Development, through its Directorate of Insurance Companies, supervise and monitor credit and financial institutions. Supervision includes the issuance of guidelines and circulars, as well as on-site audits that incorporate a component assessing compliance with anti-money laundering legislation. Supervised institutions must send to their competent authority a description of the internal control and communications procedures they have implemented to prevent money laundering. In addition, banks must undergo

internal audits. Bureaux de change must send the Bank of Greece a monthly report on their daily purchases and sales of foreign currency and audits of such companies are also periodically carried out, albeit infrequently. However, implementation of regulatory requirements documenting the flow of large sums of cash through financial and other institutions is reportedly weak.

Under Decree 2181/93, banks in Greece must demand customer identification information when opening an account or conducting transactions that exceed 15,000 euros (approx. $19,400). If there is suspicion of illegal activities, banks may take measures to gather more information on the identification of the person involved in the transaction. If any question remains, officers must file an STR with the Bank's compliance officer, irrespective of the amount involved. Greek citizens must also provide a tax registration number if they conduct foreign currency exchanges of 1,000 euros (approx. $1300) or more. The law requires that banks and financial institutions maintain adequate records and supporting documents for at least five years after ending a relationship with a customer, or, in the case of occasional transactions, for five years after the date of the transaction.

Every financial institution is required by law to appoint a compliance officer to whom all other branches or other officers must report any suspicious transactions. Reporting obligations also apply to government employees involved in auditing, including employees of the Bank of Greece, the Ministry of Economy and Finance, and the Capital Markets Commission. Reporting individuals must furnish all relevant information to the prosecuting authorities. Safe harbor provisions in Greek law protect individuals reporting violations of anti-money laundering laws and statutes.

Greece has adopted banker negligence laws under which individual bankers may be held liable if their institutions launder money. Banks and credit institutions may be subject to heavy fines if they breach their obligations to report instances of money laundering; bank officers are subject to fines and a prison term of up to two years. In September 2006, the Bank of Greece announced that for the first three-quarters of 2006, it had imposed fines in excess of ten million euros against a number of unidentified institutions for violating anti-money laundering laws and regulations. However, most of the fines reportedly require the offending institution to give the Central Bank a sum of money that the Central Bank holds in a separate, interest free account. After a designated period of time, the Central Bank returns the money to the offending institution. The Bank has imposed fines and administrative sanctions, including prohibiting the opening of new branches, in previous years.

Although authorities have recently targeted the gaming industry to restrain money launderers from using Greece's nine casinos to launder illicit funds, reportedly there is no oversight committee. Casinos are not obligated to report suspicious transactions.

Law 2331/1995 established the Competent Committee (CC), which functions as Greece's FIU. The FIU has been empowered with substantial authority. The CC is chaired by a senior retired judge and includes eleven senior representatives from the Bank of Greece, various government ministries and law enforcement agencies, the Hellenic Bankers Association, and the securities commission. The CC is responsible for receiving and processing all STRs. The STRs are hand delivered to the FIU, where, upon receipt, the committee (which is comprised of senior officials, and not full-time analysts) reviews the STRs to determine whether further investigation is necessary. If the committee requests more information from the reporting institution, the FIU will mail those questions to the institution. Once it receives a reply, the committee reviews the file again to see if the report warrants further investigation.

When the CC considers an STR to warrant further investigation, it forwards the case to the Special Control Directorate (YPEE), a multi-agency group that, in addition to initiating its own investigations, currently functions as the CC's investigative arm. When fully staffed, the Greek FIU will carry out its own investigations without resorting to help by third agencies. The YPEE, which only has investigative authority over cases which, broadly defined, involve smuggling and high-worth tax evasion, is under the direct supervision of the Ministry of Economy and Finance. The YPEE has its own in-house prosecutor in order to facilitate confidentiality and speed of action. The FIU is

responsible for preparing Money laundering cases on behalf of the Public Prosecutor's Office. The FIU is not operating at its envisaged capability because it lacks the parliamentary-approved level of full time staff, has no updated electronic database and inadequate technical capabilities for processing an ever-increasing number of STRs, which, based on unconfirmed numbers, have exceeded 1500 through late 2006.

Law 3424 passed in November 2005 upgraded the CC to an independent authority with access to public and private files, and without tax confidentiality restrictions. The law also broadens the FIU's authority with respect to the evaluation of information it receives from various organizations within Greece as well as from international organizations. However, the FIU requires a memorandum of understanding (MOU) before exchanging information with its international partners. The head of the FIU can temporarily freeze suspects' funds. The committee has the authority to impose heavy penalties on those who fail to report suspicious transactions. Reportedly, the staff limitations at the FIU have contributed to its difficulty in maintaining an effective two-way communication with Greece's broader financial community, as well as with its international counterparts.

Money laundering cases have seldom been prosecuted independently of another crime. Greek authorities do not have an effective information technology system in place to track money laundering prosecution statistics. There have been several prosecutions for money laundering in the past year. A senior judge was sentenced to 86 years in prison on charges of money laundering and receiving bribes. Additionally, the Ministry of Justice has either fired or suspended fourteen judges accused of being involved in bribery and money laundering cases. Recently, a high profile case involving over $125 million in laundered funds made headlines. It involved ten individuals and five companies spread over four countries. A court decision is still pending in the case.

If the FIU director freezes any assets, the FIU must prepare a report and forward it to an investigating magistrate and prosecutor, who conducts a further investigation and who, upon conclusion of the investigation, can issue a freezing order, pending the outcome of the criminal case. With regard to the freezing of accounts and assets, Law 3424/2005 incorporates elements of the EU Framework Decision on the freezing of funds and other financial assets, as well as the EU Council Regulation on the financing of terrorism. The GOG promulgated implementing regulations for Law 3424/2005 in June, 2006. The YPEE has established a mechanism for identifying, tracing, freezing, seizing, and forfeiting assets of narcotics-related and other serious crimes, the proceeds of which are turned over to the GOG. It is unclear what the GOG can seize once it obtains a conviction against a defendant, and whether the GOG can seize not only property as the proceeds of crime, but also property intended for use in a crime. Legitimate businesses can be seized if used to launder drug money. The GOG has not enacted laws for sharing seized narcotics-related assets with other governments.

In March 2001, the Ministry of Justice unveiled legislation on combating terrorism, organized crime, money laundering, and corruption. Parliament passed the legislation in July 2002. Under a recent counterterrorism law (Law 3251/July 2004), anyone who finances the joining or forming of a terrorist group faces imprisonment of up to ten years. If a private legal entity is implicated in terrorist financing, it faces fines of between 20,000 and 3 million euros (approximately $26,000 and $3,885,000), closure for a period of two months to two years, and ineligibility for state subsidies. Technically, it is not illegal in Greece to fund an already established terrorist group. It is only considered a terrorist financing crime if a person funds a specific attack executed by three or more people. The GOG plans to address the Financial Action Task Force's (FATF) Special Recommendation IX on cash couriers at a later date, following the issuance of a relevant EU directive.

The Bank of Greece has circulated to all financial institutions the list of individuals and entities that have been included on the UNSCR 1267 Sanctions Committee's consolidated list as being linked to Usama Bin Laden, the Al-Qaida organization, or the Taliban, as well as the EU's list of designees.

However, in most instances, there must be an active investigation before the GOG can freeze any assets. The GOG has not found any accounts belonging to anyone on the circulated lists.

The Bank of Greece maintains that alternative remittance systems do not exist in Greece and has no plans to introduce initiatives for their regulation. Illegal immigrants or individuals without valid residence permits reportedly send remittances to Albania and other destinations in the form of currency, gold and precious metals, which are often smuggled across the border in trucks and buses. The financial and economic crimes police, as well as tax authorities, closely monitor charitable and nongovernmental organizations. There is no reported evidence that such organizations are used as conduits for the financing of terrorism.

Greece is a member of the FATF, the EU, and the Council of Europe. The CC is a member of the Egmont Group. The GOG is a party to the 1988 UN Drug Convention and in December 2000 became a signatory to the UN Convention against Transnational Organized Crime, but has not yet ratified the law to enact the convention. On April 16, 2004, Greece became a party to the UN International Convention for the Suppression of the Financing of Terrorism. Greece has signed bilateral police cooperation agreements with twenty countries, including the United States. It also has a trilateral police cooperation agreement with Bulgaria and Romania, and a bilateral agreement with Ukraine to combat terrorism, drug trafficking, organized crime, and other criminal activities.

Greece exchanges information on money laundering through its Mutual Legal Assistance Treaty (MLAT) with the United States, which entered into force November 20, 2001. The Bilateral Police Cooperation Protocol provides a mechanism for exchanging records with U.S. authorities in connection with investigations and proceedings related to narcotics trafficking, terrorism, and terrorist financing. Cooperation between the U.S. Drug Enforcement Administration and YPEE has been extensive.

The Government of Greece has made progress in expanding and adjusting its legislation to international standards by gradually incorporating all EU directives on money laundering and terrorist financing. However, these actions do not comprehensively address all of the FATF Forty plus Nine Recommendations. In order to meet its stated goal of effectively addressing money laundering, the Greek Government should:

- Accelerate its efforts to realize the promise of new laws and regulations aimed at upgrading its financial intelligence unit. This includes staffing it fully with experienced analysts. The FIU should also improve its information technology (IT) capabilities so that analysts can develop an comprehensive database as well as use the Egmont Group's secure communications system. These IT upgrades will have the advantage of allowing Greek authorities to implement a system to track statistics on money laundering prosecutions and convictions, as well as asset freezes and forfeitures;
- Improve its asset freezing capabilities and should develop a clear and effective system for identifying and freezing terrorist assets within its jurisdiction. Furthermore, the GOG must also make public its system for releasing any assets it may accidentally freeze in accordance with its UN obligations;
- Take steps to require suspicious transaction reporting for its casinos and for the gaming sector, and institute a supervisory body to monitor its compliance;
- Ensure uniform enforcement of its cross-border currency reporting requirements and take steps to deter the smuggling of currency and precious metals across its borders. The GOG should take steps to codify and implement legislation addressing FATF Special Recommendation IX relating to cash couriers, and not wait for an EU Directive;

- Ensure that its "Law 89" companies, and companies operating within its free trade zones, are subject to the same AML requirements and gatekeeper and due diligence provisions, including know your customer (KYC) rules and the identification of the beneficial owner, as its other sectors;
- Abolish company-issued bearer shares, so that all bearer shares are legally prohibited;
- Ratify the UN Convention against Transnational Organized Crime.

## Grenada

Grenada is not an important regional financial center. Most of the money laundering found in Grenada involves smuggling and narcotics. Proceeds of narcotics trafficking may be laundered through a wide variety of businesses, as well as through the purchase of land, boats, jewelry, cars, and houses and other real estate. Grenada's offshore financial sector is also vulnerable to money laundering.

After being placed on the Financial Action Task Force's (FATF) list of noncooperative countries and territories (NCCT) in the fight against money laundering in September 2001, the Government of Grenada (GOG) implemented and strengthened its legislation and regulations necessary for adequate supervision of Grenada's offshore sector, which prompted the FATF to remove Grenada's name from the NCCT list in February 2003.

As of December 2006, Grenada had one inactive offshore bank, one trust company, one management company, and one international insurance company. Grenada is reported to have over 20 internet gaming sites. There are also nearly 6000 international business companies (IBCs). The domestic financial sector includes six commercial banks, 26 registered domestic insurance companies, two credit unions, and four or five money remitters. The GOG has repealed its economic citizenship legislation.

The Grenada International Financial Services Authority (GIFSA) monitors and regulates offshore financial services. GIFSA is governed by seven directors, appointed by the Minister of Finance, who are qualified or experienced in accounting, banking, commerce, insurance, management or law. GIFSA issues certificates of incorporation for IBCs, and makes recommendations to the Minister of Finance in regard to the revocation of offshore licenses. Bearer shares are not permitted for offshore banks. Currently Grenada's only offshore bank is inactive. However, holders of bearer shares in nonfinancial institutions or IBCs are permitted to issue bearer shares but must lodge these shares with one of the 15 or so registered agents licensed by the GIFSA. Registered agents are required by law to verify the identity of the beneficial owners of all shares. In addition, the International Companies Act requires registered agents to maintain records of the names and addresses of directors and beneficial owners of all shares. There is an ECD 30,000 (approximately $11,500) penalty and possible revocation of the registered agent's license for failure to maintain records. The GIFSA has the ability to conduct on-site inspections; the authority to access the records and information maintained by registered agents; and the authority to obtain customer account records from an offshore institution upon request. The GIFSA is able to share this information with regulatory, supervisory and administrative agencies. The GIFSA also has access to auditors' examination reports and may also share this information with relevant authorities.

To strengthen the supervision of the nonbank financial sector, which includes the insurance sector, cooperatives, offshore financial services, and money remitters, the GOG enacted the Grenada Authority for the Regulation of Financial Institutions (GARFIN) Act in May 2006. The Act provides for the creation of a single regulatory agency responsible for regulating and supervising all nonbank financial institutions and services in Grenada. The Eastern Caribbean Central Bank has responsibility

for the supervision of domestic banks, and will continue to do so. It is anticipated that GARFIN will be operational by spring 2007.

The Money Laundering Prevention Act (MLPA) enacted in 1999 and the Proceeds of Crime Act (POCA) No. 3 of 2003 criminalize money laundering in Grenada. Under the MLPA, the laundering of the proceeds of narcotics trafficking and all serious crimes is an offense. Under the POCA 2003, the predicate offenses for money laundering extend to all criminal conduct, which includes illicit drug trafficking, trafficking of firearms, kidnapping, extortion, corruption, terrorism and its financing, and fraud. According to the POCA 2003, a conviction on a predicate offense is not required in order to prove that certain goods are the proceeds of crime, and subsequently convict a person for laundering those proceeds. Grenada's anti-money laundering legislation applies to banks and nonbank financial institutions, as well as the offshore sector.

Established under the MLPA, the Supervisory Authority supervises the compliance of banks and nonbank financial institutions (including money remitters, stock exchange, insurance, casinos, precious gem dealers, real estate, lawyers, notaries, and accountants) with money laundering and terrorist financing laws and regulations. These institutions are required to know, record and report the identity of customers engaging in significant transactions. This applies to large currency transactions over the threshold of $3,700. Records must be maintained for seven years. In addition, a reporting entity must pay attention to all complex, unusual or large business transactions, or unusual patterns of transactions, whether completed or not. Once a transaction is determined to be suspicious or possibly indicative of money laundering, the reporting entity must forward a suspicious transaction report (STR) to the Supervisory Authority within 14 days.

The Supervisory Authority issued Anti-Money Laundering Guidelines in 2001. The guidelines direct financial institutions to maintain records, train staff, identify suspicious transactions, and designate reporting officers. The guidelines also provide examples to help institutions recognize and report suspicious transactions. The Supervisory Authority is authorized to conduct anti-money laundering inspections and investigations. The Supervisory Authority can also conduct investigations and inquiries on behalf of foreign counterparts and provide them with information. Financial institutions could be fined for not granting access to Supervisory Authority personnel.

In June 2001, the GOG established a Financial Intelligence Unit (FIU), headed by a prosecutor from the Attorney General's office. The FIU's staff includes an assistant superintendent of police, four police officers, and two support personnel. In 2003, Grenada enacted the Financial Intelligence Unit Act No. 1 of 2003. Though the FIU operates within the police force, it is technically assigned to the Supervisory Authority. The FIU is charged with receiving and analyzing suspicious transaction reports (STRs) from the Supervisory Authority, and with investigating alleged money laundering offenses. From January to November 2006, the FIU received 17 STRs. An investigation of one STR resulted in an arrest, which was a joint FIU-Drug Squad operation. The operation netted a quantity of a controlled substance and $3,700. The case is currently pending in court. The FIU has the ability to directly consult bank accounts and can request any documents from institutions that it considers necessary to fulfill its functions. In addition, the FIU also has access to other government agencies' databases. The FIU has the authority to exchange information with its foreign counterparts without a memorandum of understanding (MOU).

The FIU and the Director of Public Prosecution's Office are responsible for tracing, seizing and freezing assets. The time period for restraint of property is determined by the High Court. Presently, only criminal forfeiture is allowed by law. Approximately $42,132 of criminal-related assets was seized by November 2006. The management and disposition of seized and forfeited assets are in the charge of the Minister of Finance. The POCA provides for the establishment of a confiscated assets fund; the Minister of Finance is also responsible for the management of this fund. There is no independent system for freezing terrorist assets; it falls under the general authority of the Director of

Public Prosecution. New legislation is currently under consideration, including the Civil Forfeiture Bill, Interception of Communication Act, Cash Forfeiture Act, and Confiscation of the Proceeds of Crime Bill. These bills are now being reviewed by the relevant ministries.

Grenada regulates the cross-border movement of currency. There is no threshold requirement for currency reporting. Law enforcement and Customs officers have the powers to seize and detain cash that is imported or exported from Grenada. Cash seizure reports are shared between government agencies, particularly between Customs and the FIU.

The GOG criminalized terrorism financing through the Terrorism Act No. 5 2003. The legislation provides the GOG with the authority to identify, freeze, and seize assets related to terrorism. The GOG circulates to the appropriate institutions the names of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list. There has been no known identified evidence of terrorist financing in Grenada. Grenada has not taken any specific initiatives focused on alternative remittance systems or the misuse of charitable and nonprofit entities. The GOG has not identified any indigenous alternative remittance systems, but suspects there are some in operation.

A Mutual Legal Assistance Treaty and an Extradition Treaty have been in force between Grenada and the United States since 1999. Grenada also has a Tax Information Exchange Agreement (TIEA) with the United States. Grenada has cooperated extensively with U.S. law enforcement in numerous money laundering and other financial crimes investigations, contributing to successful prosecutions. Grenada also works actively with other governments to ensure asset tracing, freezing and seizures take place, if and when necessary, regardless of the status of the agreements. In 2003, the GOG passed the Exchange of Information Act No. 2 to permit the ECCB to provide information to foreign regulators on Grenadian banks, both domestic and offshore.

Grenada is a member of the Caribbean Financial Action Task Force (CFATF). The FIU became a member of the Egmont Group in June 2004. Grenada is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The GOG is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Grenada has not yet signed the UN Convention against Corruption. On May 8, 2006, Grenada ratified the Inter-American Convention against Terrorism.

Although the Government of Grenada has strengthened the regulation and oversight of its financial sector, it must remain alert to potential abuses and must steadfastly implement the laws and regulations it has adopted. Grenada should continue to update its Anti-Money Laundering Guidelines. The GOG should also move forward in adopting civil forfeiture legislation, and establish mechanisms to identify and regulate alternative remittance systems. Law enforcement and customs authorities should initiate money laundering investigations based on regional smuggling. Grenada should also continue to enhance its information sharing, particularly with other Caribbean jurisdictions. Grenada should also become a party to the UN Convention against Corruption.

## Guatemala

Guatemala is a major transit country for illegal narcotics from Colombia and precursor chemicals from Europe. Those factors, combined with historically weak law enforcement and judicial regimes, corruption and increasing organized crime activity, lead authorities to suspect that significant money laundering occurs in Guatemala. According to law enforcement sources, narcotics trafficking is the primary source of money laundered in Guatemala; however, the laundering of proceeds from other illicit sources, such as human trafficking, contraband, kidnapping, tax evasion, vehicle theft and corruption, is substantial. Officials of the Government of Guatemala (GOG) believe that couriers, offshore accounts and wire transfers are used to launder funds, which are subsequently invested in real

estate, capital goods, large commercial projects and shell companies, or are otherwise transferred through the financial system.

Guatemala is not considered a regional financial center, but it is an offshore center. Exchange controls have largely disappeared and dollar accounts are common, but some larger banks conduct significant business through their offshore subsidiaries. The Guatemalan financial services industry is comprised of 25 commercial banks, four of which exist in a state of permanent suspension with no commercial offices; ten offshore banks, all of which are affiliated, as required by law, with a domestic financial group; five licensed money exchangers; 14 money remitters, including wire remitters and remittance-targeting courier services; 18 insurance companies; 17 financial societies; 16 bonded warehouses; 308 savings and loans cooperatives; eight credit card issuers; seven leasing entities; 11 financial guarantors; and one check-clearing entity run by the Central Bank. It is also estimated that there are hundreds of unlicensed money exchangers that exist informally.

The Superintendence of Banks (SIB), which operates under the general direction of the Monetary Board, has oversight and inspection authority over the Central Bank (Bank of Guatemala), as well as over banks, credit institutions, financial enterprises, securities entities, insurance companies, currency exchange houses and other institutions as may be designated by the Bank of Guatemala Act. Guatemala's relatively small free trade zones target regional maquila (assembly line industry) and logistic center operations, and are not considered by GOG officials to be a money laundering concern, although proceeds from tax-related contraband are probably laundered through them.

The offshore financial sector initially offered a way to circumvent currency controls and other costly financial regulations. However, financial sector liberalization has largely removed many incentives for legitimate businesses to conduct offshore operations. All offshore institutions are subject to the same requirements as onshore institutions. In June 2002, Guatemala enacted the Banks and Financial Groups Law (No. 19-2002), which places offshore banks under the oversight of the SIB. The law requires offshore banks to be authorized by the Monetary Board and to maintain an affiliation with a domestic institution. It also prohibits an offshore bank that is authorized in Guatemala from doing business in another jurisdiction; however, banks authorized by other jurisdictions may do business in Guatemala under certain limited conditions.

In order to authorize an offshore bank, the financial group to which it belongs must first be authorized, under a 2003 resolution of the Monetary Board. By law, no offshore financial services businesses other than banks are allowed, but there is evidence that they exist in spite of that prohibition. In 2004, the SIB and Guatemala's financial intelligence unit (FIU), the Intendencia de Verificación Especial (IVE), concluded a process of reviewing and licensing all offshore entities, a process which resulted in the closure of two operations. No offshore trusts have been authorized, and offshore casinos and internet gaming sites are not regulated.

There is continuing concern over the volume of money passing informally through Guatemala. Much of the more than $3.5 billion in remittance flows pass through informal channels, although sector reforms are leading to increasing use of banks and other formal means of transmission. Terrorist financing legislation passed in August 2005 requires remitters to maintain name and address information on senders (principally U. S. based) on transfers equal to or over an amount to be determined by implementing regulations. Increasing financial sector competition should continue to expand services and bring more people into the formal banking sector, isolating those who abuse informal channels.

The Financial Action Task Force (FATF) placed Guatemala on the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering in 2001. Guatemala was removed from the NCCT list at the FATF plenary in June 2004, after authorities implemented the necessary reforms to bring Guatemala into compliance with international standards.

One of the reforms is Decree 67-2001, or the "Law Against Money and Asset Laundering." Individuals convicted of money or asset laundering are subject to a noncommutable prison term ranging from six to 20 years, and fines equal to the value of the assets, instruments or products resulting from the crime. Convicted foreigners will be expelled from Guatemala. Conspiracy and attempt to commit money laundering are also penalized. The law holds institutions and businesses responsible for failure to prevent money laundering or allowing money laundering to occur, regardless of the responsibility of owners, directors or other employees, and they may face cancellation of their banking licenses and/or criminal charges. The law also applies to the offshore entities that operate in Guatemala but are registered under the laws of another jurisdiction.

Decree 67-2001 also obligates individuals and legal entities to report to the competent authorities the cross-border movement of currency in excess of approximately $10,000. At Guatemala City airport, a new special unit was formed in 2003 to enforce the use of customs declarations upon entry to and exit from Guatemala. Money seized at the airports—approximately $167,400 in 2006—suggests that proceeds from illicit activity are regularly hand carried over Guatemalan borders. However, apart from a cursory check of a self-reporting customs form, there is little monitoring of compliance at the airport. Compliance is not regularly monitored at land borders.

In addition, the Guatemalan Monetary Board issued Resolution JM-191, approving the "Regulation to Prevent and Detect the Laundering of Assets" (RPDLA) submitted by the SIB. The RPDLA requires all financial institutions under the oversight and inspection of the SIB to establish anti-money laundering measures, and introduces requirements for transaction reporting and record keeping. The Guatemalan financial sector has largely complied with these requirements and has a generally cooperative relationship with the SIB.

Covered institutions are prohibited from maintaining anonymous accounts or accounts that appear under fictitious or inexact names. Nonbank financial institutions, however, may issue bearer shares, and there is limited banking secrecy. Obligated entities are required to keep a registry of their customers as well as of the transactions undertaken by them, such as the opening of new accounts or the leasing of safety deposit boxes. Financial institutions must also keep records of the execution of cash transactions exceeding $10,000 or more per day, and report these transactions to Guatemala's FIU, the IVE. Under the law, obligated entities must maintain records of these registries and transactions for five years. Financial institutions are also required to report all suspicious transactions to the IVE.

Decree 67-2001 establishes the IVE within the Superintendence of Banks in order to supervise covered financial institutions and ensure their compliance with the law. The IVE began operations in 2002 and has a staff of 26. The IVE has the authority to obtain all information related to financial, commercial, or business transactions that may be connected to money laundering. The IVE conducts inspections on the covered entities' management, compliance officers, anti-money laundering training programs, "know-your-client" policies, and auditing programs. The IVE has imposed over $100,000 in civil penalties to date for institutional failure to comply with anti-money laundering regulation.

Since its inception, the IVE has received approximately 1,600 suspicious transaction reports (STRs) from the 400 obligated entities in Guatemala. All STRs are received electronically, and the IVE has developed a system of prioritizing them for analysis. After determining that an STR is highly suspicious, the IVE gathers further information from public records and databases, other covered entities and foreign FIUs, and assembles a case. Bank secrecy can be lifted for the investigation of money laundering crimes. Once the IVE has determined a case warrants further investigation, the case must receive the approval of the SIB before being sent to the Anti-Money or Other Assets Laundering Unit (AML Unit) within the Public Ministry. Under current regulations, the IVE cannot directly share the information it provides to the AML Unit with any other special prosecutors (principally the

anticorruption or counternarcotics units) in the Public Ministry. The IVE also assists the Public Ministry by providing information upon request for other cases the prosecutors are investigating.

In 2006, Guatemala created a money laundering task force. The money laundering task force is a joint unit comprised of individuals from the Guatemalan Tax Authority (SAT), the IVE, Public Ministry, Prosecutor's Office, Government Ministry, National Police and Drug Police. Together they work on investigating financial crimes, building evidence and bringing the cases to prosecution. They are currently working on four cases of suspected money laundering.

Other government agencies have become involved in combating money laundering. In addition to the SIB, the SAT has been working to improve its processes and personnel to better collect taxes and combat tax evasion. This indirectly assists anti-money laundering efforts by making it easier to detect suspicious activity through nonpayment of tax.

Thirty-nine cases have been referred by the IVE to the AML Unit, four of which stem from public corruption. In several cases, assets have been frozen. Thirteen money laundering prosecutions have been concluded, twelve of which resulted in convictions. Eleven of those cases have been sentenced, with the remaining two cases awaiting the completion of appeals. Additional cases have been developed from cooperation between the Public Ministry and the IVE. The Public Ministry's AML Unit had initiated 46 cases as of January 2006. In addition, four cases have been transferred to other offices for investigation and prosecution (such as the anticorruption unit) due to the nature of their particular predicate offenses. The other 46 cases are either still under investigation or in initial trial stages. Several high profile cases of laundering proceeds from major corruption scandals involving officials of the previous government are currently under investigation and have resulted in arrests and substantial seizures of funds and assets. These seizures have been supported by the cooperating financial institutions along with the vast majority of public and political interests.

In 2006, Guatemala passed an organized crime control law. This new legislation permits the use of undercover operations, controlled deliveries and wire taps to investigate many forms of organized crime activity, including money laundering crimes.

Under current legislation, any assets linked to money laundering can be seized. The IVE, the National Civil Police, and the Public Ministry have the authority to trace assets; the Public Ministry can seize assets temporarily or in urgent cases, and the Courts of Justice have the authority to permanently seize assets. In 2003, the Guatemalan Congress approved reforms to enable seized money to be shared among several GOG agencies, including police and the IVE. Nevertheless, the Constitutional Court ruled that forfeited currency remains under the jurisdiction of the Supreme Court of Justice.

An additional problem is that the courts do not allow seized currency to benefit enforcement agencies while cases remain open. For money laundering and narcotics cases, any seized money is deposited in a bank safe and all material evidence is sent to the warehouse of the Public Ministry. There is no central tracking system for seized assets, and it is currently impossible for the GOG to provide an accurate listing of the seized assets in custody. In 2005, Guatemalan authorities seized more than U.S. $6.5 million in bulk currency, significantly less that the $20 million seized in 2003 (although one case alone in 2003 accounted for more than $14 million). The lack of access to the resources of seized assets outside of the judiciary has made sustaining seizure levels difficult for the resource-strapped enforcement agencies.

In June 2005, the Guatemalan Congress passed legislation criminalizing terrorist financing. Implementing regulations were submitted to the Monetary Board in December 2005. According to the GOG, Article 391 of the penal code already sanctioned all preparatory acts leading up to a crime, and financing would likely be considered a preparatory act. Technically, both judges and prosecutors could have issued a freeze order on terrorist assets, but no test case ever validated these procedures. The new counterterrorism financing legislation removed potential uncertainty regarding the legality of freezing

assets when no predicate offense had been legally established but the assets have been determined destined to terrorists or to support terrorist acts. The GOG has been very cooperative in looking for terrorist financing funds. The new legislation brings Guatemala into greater compliance with FATF Special Recommendations on Terrorist Financing and the United Nations Security Council Resolution 1373 Against Terrorism.

Guatemala is a party to the UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. On March 1, 2006, the GOG ratified the Inter-American Convention against Terrorism, and on November 3, 2006, the GOG ratified the UN Convention against Corruption. Guatemala is also a party to the Central American Convention for the Prevention of Money Laundering and Related Crimes. The GOG is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). In 2003, the IVE became a member of the Egmont Group.

Corruption and organized crime remain strong forces in Guatemala and may prove to be the biggest hurdles facing the Government of Guatemala in the long term. Guatemala has made efforts to comply with international standards and improve its anti-money laundering regime; however, Guatemala should take steps to immobilize bearer shares, and to identify and regulate offshore financial services and gaming establishments. The GOG should also continue efforts to improve enforcement and implementation of needed reforms. Cooperation between the IVE and the Public Ministry has improved since the new administration took office in January 2004, and several investigations have led to prosecutions. However, Guatemala should continue to focus its efforts on boosting its ability to successfully investigate and successfully prosecute money laundering cases, and distributing seized assets to law enforcement agencies to assist in the fight against money laundering and other financial crime.

## Guernsey

The Bailiwick of Guernsey (the Bailiwick) covers a number of the Channel Islands (Guernsey, Alderney, Sark, and Herm in order of size and population). The Islands are dependents of the British Crown and the United Kingdom (UK) is responsible for their defense and international relations. However, the Bailiwick is not part of the UK. Alderney and Sark have their own separate parliaments and civil law systems. Guernsey's parliament legislates criminal law for all of the islands in the Bailiwick. The Bailiwick alone has authority to legislate domestic taxation. The Bailiwick is a sophisticated financial center and, as such, it continues to be vulnerable to money laundering at the layering and integration stages.

There are approximately 17,800 companies registered in the Bailiwick. Nonresidents own approximately half of the companies, and they have an exempt tax status. These companies do not fall within the standard definition of an international business company (IBC). Local residents own the remainder of the companies, including trading and private investment companies. Exempt companies are not prohibited from conducting business in the Bailiwick, but must pay taxes on profits of any business conducted on the islands. Companies can be incorporated in Guernsey and Alderney, but not in Sark, which has no company legislation. Companies in Guernsey may not be formed or acquired without disclosure of beneficial ownership to the Guernsey Financial Services Commission (the Commission).

Guernsey has 51 banks, all of which have offices, records, and a substantial presence in the Bailiwick. The banks are licensed to conduct business with residents and nonresidents alike. There are 626 international insurance companies and 684 collective investment funds. There are also 18 bureaux de change, which file accounts with the tax authorities. Ten of the bureaux de change are part of a

licensed bank, and it is the bank that publishes and files those accounts. Bureaux de change and other money service providers are required to register information with the Commission.

Guernsey has put in place a comprehensive legal framework to counter money laundering and the financing of terrorism. The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law 1999, as amended, is supplemented by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) Regulations, 2002. The legislation criminalizes money laundering for all crimes except drug-trafficking, which is covered by the Drug Trafficking (Bailiwick of Guernsey) Law, 2000. The Proceeds of Crime Law and the Regulations are supplemented by Guidance Notes on the Prevention of Money Laundering and Countering the Financing of Terrorism, issued by the Commission. There is no exemption for fiscal offenses. The 1999 law creates a system of suspicious transaction reporting (including tax evasion) to the Guernsey Financial Intelligence Service (FIS). The Bailiwick narcotics trafficking, anti-money laundering, and terrorism laws designate the same foreign countries as the UK to enforce foreign restraint and confiscation orders.

The Drug Trafficking (Bailiwick of Guernsey) Law 2000 consolidates and extends money laundering legislation related to narcotics trafficking. It introduces the offense of failing to disclose the knowledge or suspicion of drug money laundering. The duty to disclose extends beyond financial institutions to cover others as well, for example, bureaux de change and check cashers.

In addition, the Bailiwick authorities enacted the Prevention of Corruption (Bailiwick of Guernsey) Law of 2003. They have also resolved to merge existing drug trafficking, money laundering and other crimes into one statute, and to introduce a civil forfeiture law.

On April 1, 2001, the Regulation of Fiduciaries, Administration Businesses, and Company Directors, etc. (Bailiwick of Guernsey) Law of 2000 ("the Fiduciary Law") came into effect. The Fiduciary Law was enacted to license, regulate and supervise company and trust service providers. Under Section 35 of the Fiduciary Law, the Commission creates Codes of Practice for corporate service providers, trust service providers and company directors. Under the law, the Commission must license all fiduciaries, corporate service providers and persons acting as company directors on behalf of any business. In order to be licensed, these agencies must pass strict tests. These include "know your customer" requirements and the identification of clients. These organizations are subject to regular inspection, and failure to comply could result in the fiduciary being prosecuted and/or its license being revoked. The Bailiwick is fully compliant with the Offshore Group of Banking Supervisors Statement of Best Practice for Company and Trust Service Providers.

Since 1988, the Commission has regulated the Bailiwick's financial services businesses. The Commission regulates banks, insurance companies, mutual funds and other collective investment schemes, investment firms, fiduciaries, company administrators and company directors. The Bailiwick does not permit bank accounts to be opened unless there has been a "know your customer" inquiry and verification details are provided. The AML/CFT Regulations contain penalties to be applied when financial services businesses do not follow the requirements of the Regulations. Company incorporation is by act of the Royal Court, which maintains the registry. All applications to form a Bailiwick company have to be made to the Commission, which then evaluates each application. The Court will not permit incorporation unless the Commission and the Attorney General or Solicitor General has given prior approval. The Commission conducts regular on-site inspections and analyzes the accounts of all regulated institutions.

On July 1, 2005, the European Union Savings Tax Directive (ESD) came into force. The ESD is an agreement between the Member States of the European Union (EU) to automatically exchange information with other Member States about EU tax resident individuals who earn income in one EU Member State but reside in another. Although not part of the EU, the three UK Crown Dependencies (Guernsey, Jersey, and the Isle of Man), have voluntarily agreed to apply the same measures to those

in the ESD and have elected to implement the withholding tax option (also known as the "retention tax option") within the Crown Dependencies.

Under the retention tax option, each financial services provider will automatically deduct tax from interest and other savings income paid to EU resident individuals. The tax will then be submitted to local and Member States tax authorities annually. The tax authorities receive a bulk payment but do not receive personal details of individual customers. If individuals elect the exchange of information option, then no tax is deducted from their interest payments but details of the customer's identity, residence, paying agent, level and time period of savings income received by the financial services provider will be reported to local tax authorities where the account is held and then forwarded to the country where the customer resides.

The Guernsey authorities have established a forum, the Crown Dependencies Anti-Money Laundering Group, where the Attorneys General from the Crown Dependencies, Directors General and other representatives of the regulatory bodies, and representatives of police, Customs, and the Financial Intelligence Service (FIS) meet to coordinate the anti-money laundering and counterterrorism policies and strategy in the Dependencies.

The FIS operates as the Bailiwick's financial intelligence unit (FIU). The FIS began operations in April 2001, and is currently staffed by Police and Customs/Excise Officers. The FIS is directed by the Service Authority, which is a small committee of senior Police and Customs Officers who co-ordinate with the Bailiwick's financial crime strategy and report to the Chief Officers of Police and Customs/Excise. The FIS is mandated to place specific focus and priority on money laundering and terrorism financing issues. Suspicious Transaction Reports (STRs) are filed with the FIS, which serves as the central point within the Bailiwick for the receipt, collation, analysis, and dissemination of all financial crime intelligence. In 2005, the FIS received 650 STRs. The FIS received 757 STRs in 2004 and 705 STRs in 2003.

In November 2002, the International Monetary Fund (IMF) undertook an assessment of Guernsey's compliance with internationally accepted standards and measures of good practice relative to its regulatory and supervisory arrangements for the financial sector. The IMF report states that Guernsey has a comprehensive system of financial sector regulation with a high level of compliance with international standards. As for AML/CFT, the IMF report highlights that Guernsey has a developed legal and institutional framework for AML/CFT and a high level of compliance with the FATF Recommendations.

There has been counterterrorism legislation covering the Bailiwick since 1974. The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002, replicates equivalent UK legislation.

The Criminal Justice (International Cooperation) (Bailiwick of Guernsey) Law, 2000, furthers cooperation between Guernsey and other jurisdictions by allowing certain investigative information concerning financial transactions to be exchanged. Guernsey cooperates with international law enforcement on money laundering cases. In cases of serious or complex fraud, Guernsey's Attorney General can provide assistance under the Criminal Justice (Fraud Investigation) (Bailiwick of Guernsey) Law 1991. The Commission also cooperates with regulatory/supervisory and law enforcement bodies.

On September 19, 2002, the United States and Guernsey signed a Tax Information Exchange Agreement, which is not yet in force. The agreement provides for the exchange of information on a variety of tax investigations, paving the way for audits that could uncover tax evasion or money laundering activities. Currently, similar agreements are being negotiated with other countries, among them members of the European Union.

After its extension to the Bailiwick, Guernsey enacted the necessary legislation to implement the Council of Europe Convention on Mutual Assistance in Criminal Matters, the Council of Europe

Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, and the 1988 UN Drug Convention. The 1988 U.S.-UK Agreement Concerning the Investigation of Drug Trafficking Offenses and the Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking, as amended in 1994, was extended to the Bailiwick in 1996. The Bailiwick has requested that the UK Government seek the extension to the Bailiwick of the UN International Convention for the Suppression of the Financing of Terrorism.

The Attorney General's Office is represented in the European Judicial Network and has participated in the European Union's PHARE anti-money laundering developmental assistance project. The Commission cooperates with regulatory/supervisory and law enforcement bodies. It is a member of the International Association of Insurance Supervisors, the Offshore Group of Insurance Supervisors, the Association of International Fraud Agencies, the International Organization of Securities Commissions, the Enlarged Contact Group for the Supervision of Collective Investment Funds, and the Offshore Group of Banking Supervisors. The FIS is a member of the Egmont Group.

Guernsey has put in place a comprehensive anti-money laundering regime, and has demonstrated its ongoing commitment to fighting financial crime. Bailiwick officials should continue both to carefully monitor Guernsey's anti-money laundering program to assure its effectiveness, and to cooperate with international anti-money laundering authorities.

## Guyana

Guyana is neither an important regional nor an offshore financial center, nor does it have any free trade zones. However, the scale of money laundering is thought to be large relative to the size of the economy, with some experts estimating that the informal economy is 40 to 60 percent of the size of the formal sector. Money laundering has been linked to trafficking in drugs, firearms and persons, as well as to corruption and fraud. Drug trafficking and money laundering appear to be benefiting the Guyanese economy, particularly the construction sector. Investigating and prosecuting money laundering cases is not a priority for law enforcement. The Government of Guyana (GOG) made no arrests or prosecutions for money laundering in 2006 due to a lack of adequate legislation and resources.

The Money Laundering Prevention Act of 2000 criminalizes money laundering related to narcotics trafficking, illicit trafficking of firearms, extortion, corruption, bribery, fraud, counterfeiting and forgery. The Act does not specifically cover the financing of terrorism or all serious crimes in its list of offenses. Licensed financial institutions—including banks, securities brokers, exchange houses, credit unions, building societies and trusts—are required to report suspicious transactions to Guyana's financial intelligence unit (FIU), although they are left to determine thresholds individually according to banking best practices. Financial institutions must keep records of suspicious transaction reports (STRs) for six years. The law also requires that the cross-border transportation of currency exceeding $10,000 be reported. The legislation includes provisions regarding confidentiality in the reporting process, good faith reporting, penalties for destroying records related to an investigation or disclosing investigations, and international cooperation. The Money Laundering Prevention Act establishes the Guyana Revenue Authority, the Customs Anti-Narcotics Unit, the Attorney General, the Director for Public Prosecutions and the FIU as the authorities responsible for investigating financial crime.

The GOG's anti-money laundering regime is ineffective, and the implementing regulations of the Money Laundering Prevention Act are inadequate. Guyana's central bank, the Bank of Guyana, lacks the capacity to fully execute its mandate to supervise financial institutions for compliance with anti-money laundering provisions. There have been no money laundering prosecutions to date, and it is unclear if a conviction for the predicate offense is necessary to obtain a money laundering conviction. The financial intelligence unit, established within the Ministry of Finance in 2003, is currently a one-person organization and is dependent upon the Ministry for its budget and office space. Although the

FIU may request additional information from obligated entities, its analytical capabilities are severely limited by its inability to access to law enforcement data and its lack of authority to exchange information with foreign FIUs. The GOG does not release statistics on the number of suspicious transaction reports received by the FIU, although the requirement to make these statistics available to relevant authorities is mandated by the Financial Action Task Force (FATF).

In order to improve the GOG's anti-money laundering regime, the FIU has prepared drafts of legislation criminalizing the financing of terrorism and expanding the scope of the money laundering offense. The new legislation is also expected to provide for oversight of export industries, the insurance industry, real estate and alternative remittance systems. The draft money laundering act failed to make the legislative agenda before the dissolution of Parliament in May 2006.

In January 2007, the National Assembly passed the Gambling Prevention (Amendment) Bill, which legalizes casino gambling. The bill establishes a Gaming Authority authorized to issue casino licenses to new luxury hotel or resort complexes with a minimum of 150 rooms. Vocal opposition to the bill from religious groups, opposition parties, and the public included concerns that casino gambling would provide a front for money launderers.

The Money Laundering Prevention Act provides for seizure of assets derived as proceeds of crime, including money, investments, and real and personal property. However, guidelines for implementing seizures and forfeitures have not been finalized. Forfeiture and seizure mechanisms are conviction-based, and may be carried out by the Office of the Director of Public Prosecutions if a court order is obtained.

The Ministry of Foreign Affairs and the Bank of Guyana continue to assist U.S. efforts to combat terrorist financing by working towards compliance with relevant United Nations Security Council Resolutions (UNSCRs). In 2001 the Bank of Guyana, the sole financial regulator as designated by the Financial Institutions Act of March 1995, issued orders to all licensed financial institutions expressly instructing the freezing of all financial assets of terrorists, terrorist organizations, and individuals and entities associated with terrorists and their organizations. Guyana has no domestic laws authorizing the freezing of terrorist assets, but the government created a special committee on the implementation of UNSCRs, co-chaired by the Head of the Presidential Secretariat and the Director General of the Ministry of Foreign Affairs. To date the procedures have not been tested, as no terrorist assets have been identified in Guyana. The FIU director also disseminates the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list to relevant financial institutions.

Guyana is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). Guyana underwent its second CFATF mutual evaluation in 2004, and the results of the evaluation were presented at the CFATF plenary in October 2006. The mutual evaluation team found the GOG to be noncompliant or materially noncompliant with approximately half of the FATF Recommendations.

Guyana is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Guyana has not signed the UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Corruption. The GOG has signed, but not yet ratified, the Inter-American Convention against Terrorism. Guyana's FIU is one of the few in the region that is not a member of the Egmont Group.

The Government of Guyana should introduce the draft legislation on money laundering to Parliament early in the legislative session. The GOG should provide greater autonomy for the FIU by making it an independent unit with its own budget and office space, enable the FIU to access law enforcement data, and ensure that the FIU has the operational capacity to meet the membership requirements of the

Egmont Group and other international standards. Guyana should also provide appropriate resources and awareness training to its regulatory, law enforcement and prosecutorial personnel, and establish procedures for asset seizure and forfeiture. Now that Guyana has legalized casino gambling, the GOG should ensure that the necessary anti-money laundering regulations are extended to the gaming sector. Guyana should criminalize terrorist financing and adopt measures that would allow it to block terrorist assets. In addition, Guyana should seize opportunities to sensitize the public to the harmful impact of money laundering on legitimate businesses and the national economy. The GOG should become a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Corruption.

## Haiti

Haiti is not a major financial center. Given Haiti's dire economic condition and unstable political situation, it is doubtful that it will become a major player in the region's formal financial sector in the near future. Haiti is a major drug-transit country, and money laundering activity is linked to the drug trade. Money laundering and other financial crimes occur in the banking system and in casinos, foreign currency transactions and real estate transactions. While the informal economy in Haiti is significant and partly funded by illicit narcotics proceeds, smuggling is historically prevalent and predates narcotics trafficking. Flights to Panama City, Panama, remain the main identifiable mode of transportation for money couriers. Usually travelers, predominantly Haitian citizens, hide large sums, ranging from $30,000 to $100,000 on their persons. Haitian narcotics officers interdicting these outbound funds often collect a six to 12 percent fee and allow the couriers to continue without arrest. During interviews, couriers usually declare that they intend to use the large amounts of U.S. currency to purchase clothing and other items to be sold upon their return to Haiti, a common practice in the informal economic sector. Further complicating the picture is the cash that is routinely transported to Haiti from Haitians and their relatives in the United States in the form of remittances, representing an estimated 30 percent of Haiti's gross domestic product.

In March 2004, an interim government was established in Haiti following former President Jean Bertrand Aristide's resignation and departure. The Interim Government of Haiti (IGOH) took initiatives to establish improvements in economic and monetary policies, as well as working to improve governance and transparency. In response to the corruption that continues to plague Haiti, the IGOH created an Anti-Corruption Unit and a commission to examine transactions conducted by the government from 2001 through February 2004. The commission published its report in July 2005. In early 2006 Presidential elections took place. Neither the IGOH nor the new government have prosecuted any cases based on the information provided in the report.

Despite political instability, Haiti has taken steps to address its money laundering and financial crimes problems. Since 2001, Haiti has used the Law on Money Laundering from Illicit Drug Trafficking and other Crimes and Punishable Offenses (AML Law) as its primary anti-money laundering legislation. All financial institutions and natural persons are subject to the money laundering controls of the AML Law. The AML Law criminalizes money laundering and applies to a wide range of financial institutions, including banks, money remitters, exchange houses, casinos, and real estate agents. Insurance companies are not covered; however, they are only nominally represented in Haiti. The AML Law requires financial institutions to establish money laundering prevention programs and to verify the identity of customers who open accounts or conduct transactions that exceed 200,000 gourdes (approximately $5,420). It also requires exchange brokers and money remitters to obtain declarations identifying the source of funds exceeding 200,000 gourdes or its equivalent in foreign currency. The nonfinancial sector, however, remains largely unregulated.

In 2002, Haiti formed a National Committee to Fight Money Laundering, the Comité National de Lutte Contre le Blanchiment des Avoirs (CNLBA). The CNLBA is in charge of promoting,

coordinating, and recommending policies to prevent, detect, and suppress the laundering of assets obtained from the illicit trafficking of drugs and other serious offenses. Created in 2003, the Unite Centrale de Renseignements Financiers (UCREF) is the financial intelligence unit (FIU) of Haiti. The UCREF is responsible for receiving and analyzing reports submitted in accordance with the law. The UCREF has approximately 42 employees, including 25 investigators. Institutions are required to report to the UCREF any transaction involving funds that appear to be derived from a crime, as well as those exceeding 200,000 gourdes. Failure to report such transactions is punishable by more than three years' imprisonment and a fine of 20 million gourdes (approximately $542,000). Banks are required to maintain records for at least five years and are required to present this information to judicial authorities and UCREF officials upon request. Bank secrecy or professional secrecy cannot be invoked as grounds for refusing information requests from these authorities.

The AML Law has provisions for the forfeiture and seizure of assets; however the government cannot declare the asset or business forfeited until there is a conviction. The inability to seize or freeze assets early in the judicial process reduces the government's authority and resources to pursue cases. The IGOH was supportive of a stronger, more proactive asset seizure law, yet its temporary governmental mandate did not allow for the passage of new laws. The IGOH set-up a Financial Crimes Task Force under the auspices of the Central Bank and the Ministries of Justice and Finance, charged with identifying and investigating major financial crimes and coordinating with the UCREF in recommending prosecutions. The recently elected Government of Haiti has not recognized the Task Force and the Task Force has become dormant.

In 2006, UCREF confiscated $801,000 and froze 157 million gourdes (approximately $4.3 million), in addition to $1.4 million related to money laundering offenses. It is unknown how many current investigations are active at this time. The director of UCREF was jailed for a short period of time by a magistrate on unknown charges. At the time of his incarceration over $1.4 million was unfrozen and released to the persons who claimed ownership.

In 2006 the UCREF assisted the U.S. in at least three major investigations. The UCREF also assisted the IGOH in filing the first-ever civil lawsuit in a U.S. court for reparation of Haitian government funds diverted through U.S. banks and businesses. However, the law suit was dropped shortly after the new government took office. Though the recent achievements of the UCREF are a marked improvement, it is still not fully functional or funded, and many of the UCREF's employees still lack experience and the ability to independently investigate cases, which translates into slow progress in moving cases into the judicial system.

Haiti still has not passed legislation specifically criminalizing the financing of terrorists and terrorism, nor has it signed the UN International Convention for the Suppression of the Financing of Terrorism. Reportedly, Haiti does circulate the UN 1267 list. The AML Law provides for investigation and prosecution in all cases of illegally derived money. Under this law, terrorist finance assets may be frozen and seized. Currently, there is no indication of the financing of terrorism in Haiti.

Haiti is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the Inter-American Convention against Terrorism. Haiti is a member of the OAS/CICAD Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force. The UCREF is not a member of the Egmont Group of financial intelligence units; however, it has three memoranda of understanding with the FIUs of the Dominican Republic, Panama and Honduras.

While improvements were made to Haiti's anti-money laundering regime under the IGOH, the new administration should implement and enforce the AML Law. The Government of Haiti should confront the rampant corruption present in almost all public institutions. The GOH should recognize the Financial Crimes Task Force and should strengthen the organizational structures and personal skills of employees both in the UCREF and the Financial Crimes Task Force. Steps should be taken so

that the UCREF fully meets international standards and is eligible for membership in the Egmont Group. The GOH should enact legislation to criminalize the financing of terrorism and become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

## Honduras

Honduras is not an important regional or offshore financial center and is not considered to have a significant black market for smuggled goods, although there have been recent high-profile smuggling cases involving gasoline and other consumer goods. Money laundering, however, does take place, primarily through the banking sector but also through currency exchange houses and front companies. The vulnerabilities of Honduras to money laundering stem primarily from significant trafficking of narcotics, particularly cocaine, throughout the region. An estimated $2 billion in remittances and smuggling of contraband may also generate funds that are laundered through the banking system. Money laundering in Honduras derives both from domestic and foreign criminal activity, and the proceeds are controlled by local drug trafficking organizations and organized crime syndicates. Honduras is not experiencing an increase in financial crimes such as bank fraud. It is not a matter of government policy to encourage, facilitate or engage in laundering the proceeds from illegal drug transactions, terrorist financing or other serious crimes. However, corruption remains a serious problem, particularly within the judiciary and law enforcement sectors.

There is no indication Honduran free trade zone companies are being used in trade-based money laundering schemes or by financiers of terrorism. Under Honduran legislation, companies may register for “free trade zone” status, and benefit from the associated tax benefits, regardless of their location in the country. Companies that wish to receive free trade zone status must register within the Office of Productive Sectors within the Ministry of Industry and Commerce. The majority of companies with free trade zone status operate mostly in the textile and apparel industry.

Money laundering has been a criminal offense in Honduras since 1998, when the passage of Law No. 27-98 criminalized the laundering of narcotics-related proceeds and introduced various record keeping and reporting requirements for financial institutions. However, weaknesses in the law, including a narrow definition of money laundering, made it virtually impossible to successfully prosecute the crime.

In 2002, Honduras passed Decree No. 45-2002, which strengthened its legal framework and available investigative and prosecutorial tools to fight money laundering. Under the new legislation, the definition of money laundering was expanded to include the transfer of assets that proceed directly or indirectly from trafficking of drugs, arms, human organs or persons; auto theft; kidnapping; bank and other forms of financial fraud; and terrorism, as well as any sale or movement of assets that lacks economic justification. The penalty for money laundering is a prison sentence of 15-20 years. The law also requires all persons entering or leaving Honduras to declare-and, if asked, present-cash and convertible securities (títulos valores de convertibilidad inmediata) that they are carrying if the amount exceeds $10,000 or its equivalent.

Decree No. 45-2002 created the financial intelligence unit (FIU), the Unidad de Información Financiera (UIF), within the National Banking and Securities Commission. Banks and other financial institutions are required to report to the UIF currency transactions over $10,000 in dollar denominated accounts or the equivalent in local currency accounts, as well as all suspicious transactions. The law requires the UIF and reporting institutions to keep a registry of reported transactions for five years. Banks are required to know the identity of all their clients and depositors, regardless of the amount of a client’s deposits, and to keep adequate records of the information. The law also includes banker negligence provisions that make individual bankers subject to two- to five-year prison terms if, by carelessness, negligence, inexperience or non-observance of the law, they permit money to be laundered through their institutions. Anti-money laundering requirements apply to all financial

institutions that are regulated by the National Banking and Securities Commission, including state and private banks, savings and loan associations, bonded warehouses, stock markets, currency exchange houses, securities dealers, insurance companies, credit associations, and casinos.

Decree No. 45-2002 requires that a public prosecutor be assigned to the UIF. In practice, two prosecutors are assigned to the UIF, each on a part-time basis, with responsibility for specific cases divided among them depending upon their expertise. The prosecutors, under urgent conditions and with special authorization, may subpoena data and information directly from financial institutions. Public prosecutors and police investigators are permitted to use electronic surveillance techniques to investigate money laundering.

Under the Criminal Procedure Code, officials responsible for filing reports on behalf of obligated entities are protected by law with respect to their cooperation with law enforcement authorities. However, some have alleged that their personal security is put at risk if the information they report leads to the prosecution of money launderers. This has not been an issue throughout 2006, however, as only cases originating from the police and prosecutors have been presented in court.

There had been some ambiguity in Honduran law concerning the responsibility of banks to report information to the supervisory authorities, and the duty of these institutions to keep customer information confidential. A new law passed in September 2004, the Financial Systems Law (Decree No. 129-2004), clarifies this ambiguity, explicitly stating that the provision of information requested by regulatory, judicial, or other legal authorities shall not be regarded as an improper divulgence of confidential information.

In December 2004, Decree No. 24-2004 created the Interagency Commission for the Prevention of Money Laundering and Financing of Terrorism (CIPLAFT). The group was tasked as the coordinating entity responsible for ensuring that all anti-money laundering and anti-financing of terrorism systems operate efficiently and consistently with all relevant laws, regulations, resolutions, and directives. However, the size of the group and overly political environment stifled effective discussions and marginalized any positive developments that came out of the meetings. In early 2006, the new head of the banking commission effectively terminated the CIPLAFT.

At roughly the same time as the termination of the CIPLAFT, a new agreement among the Public Ministry, the banking commission, and the UIF was drafted with the intent to more effectively prioritize money laundering cases and determine which cases to pursue. Previously, an average of 20 nonpriority cases were sent to prosecutors for review each month. This has been streamlined to a more manageable five cases, each of which has been determined to be promising for potential prosecution, and many older cases have been officially closed. The result is fewer active cases, allowing the overloaded prosecutors and under-funded police units to focus on the strongest and most important cases.

Prior to 2004, there had been no successful prosecutions of money laundering crimes in Honduras. In 2004, however, Honduran authorities arrested 16 persons for money laundering crimes, issued six additional outstanding arrest warrants, and secured five convictions. Through November of 2006, another six convictions have been obtained.

The Honduran Congress first enacted an asset seizure law in 1993. Decree No. 45-2002 strengthens the asset seizure provisions of the law, and established an Office of Seized Assets (OABI) under the Public Ministry. Decree 45-2002 authorizes the OABI to guard and administer all goods, products or instruments of a crime, and states that money seized or money raised from the auctioning of seized goods should be transferred to the public entities that participated in the investigation and prosecution of the crime. Under the Criminal Procedure Code, when goods or money are seized in any criminal investigation, a criminal charge must be submitted against the suspect within 60 days of the seizure; if one is not submitted, the suspect has the right to demand the release of the seized assets.

Decree No. 45-2002 is not entirely clear on the issue of whether a legitimate business can be seized if used to launder money derived from criminal activities. The chief prosecutor for organized crime maintains that the authorities do have this power, because once a "legitimate" business is used to launder criminal assets, it ceases to be "legitimate" and is subject to seizure proceedings. However, this authority is not explicitly granted in the law, and there has been no test case to date which would set an interpretation. There are currently no new laws being considered regarding seizure or forfeiture of assets of criminal activity.

As of December 2006, the total value of assets seized since the 2002 law came into effect is estimated at $5.7 million, including $4.6 million in tangible assets such as cars, houses and boats. To date in 2006, two new cases have added approximately $20,000 to the total assets seized. Most of these seized assets are alleged to have derived from crimes related to drug trafficking; none is suspected of being connected to terrorist activity. The law allows for both civil and criminal forfeiture, and there are no significant legal loopholes that allow criminals to shield their assets.

In addition to undergoing the financial audit verifying the bank accounts, OABI has moved to distribute funds to various law enforcement units and nongovernmental organizations (NGOs). The funds, which constituted the first systematic distribution under the new guidelines, went to the Supreme Court, federal prosecutors, OABI, and two civil society groups. Momentum is now gaining for OABI to more quickly liquidate all assets once confiscated, in an effort to avoid parking lots full of deteriorating assets or high protection and maintenance fees. With new management and guidelines in place, OABI is set to expand its role significantly when a witness protection law passes that will allow the unit to hold all seized assets, not just assets seized under the money laundering law.

The GOH has been supportive of counterterrorism efforts. Decree No. 45-2002 states that an asset transfer related to terrorism is a crime; however, terrorist financing has not been identified as a crime itself. This law does not explicitly grant the GOH the authority to freeze or seize terrorist assets; however, under separate authority, the National Banking and Insurance Commission has issued freeze orders promptly for the organizations and individuals named by the United Nations 1267 Sanctions Committee and those organizations and individuals on the list of Specially Designated Global Terrorists designated by the United States pursuant to Executive Order 13224. The Ministry of Foreign Affairs is responsible for instructing the Commission to issue freeze orders. The Commission directs Honduran financial institutions to search for, hold and report on terrorist-linked accounts and transactions, which, if found, would be frozen. The Commission has reported that, to date, no accounts linked to the entities or individuals on the lists have been found in the Honduran financial system.

While Honduras is a major recipient of flows of remittances (estimated at $2 billion in 2006), there has been no evidence to date linking these remittances to the financing of terrorism. Remittances primarily flow from Hondurans living in the United States to their relatives in Honduras. Most remittances are sent through wire transfer or bank services, with some cash probably being transported physically from the United States to Honduras. There is no significant indigenous alternative remittance system operating in Honduras, nor is there any evidence that charitable or nonprofit entities in Honduras have been used as conduits for the financing of terrorism.

Honduras cooperates with U.S. investigations and requests for information pursuant to the 1988 United Nations Drug Convention. No specific written agreement exists between the United States and Honduras to establish a mechanism for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing, and other crime investigations. However, Honduras has cooperated, when requested, with appropriate law enforcement agencies of the U.S. Government and other governments investigating financial crimes. The UIF has signed memoranda of understanding to exchange information on money laundering investigations with Panama, El Salvador, Guatemala, Mexico, Peru, Colombia and the Dominican Republic.

Honduras is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the Inter-American Convention against Terrorism. Honduras strives to comply with the Basel Committee's "Core Principles for Effective Banking Supervision," and the new Financial System Law, Decree No. 129-2004, is designed to improve compliance with these international standards. At the regional level, Honduras is a member of the Central American Council of Bank Superintendents, which meets periodically to exchange information. Honduras is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Group of Experts to Control Money Laundering, and the Caribbean Financial Action Task Force (CFATF). In 2005, the UIF became a member of the Egmont Group.

Four years after passing a new law against money laundering, the Government of Honduras (GOH) continued to make considerable progress in implementing the law, establishing and training the entities responsible for the investigation of financial crimes, and improving cooperation among these entities. In 2006, the Government of Honduras continues its positive steps to implement Decree No. 45-2002. The number of good cases identified for investigation has helped focus the poorly funded prosecutors and police force, while the number of cases closed continues to climb. The asset seizure organization, OABI, continues to improve, and seized assets could soon become a significant funding source for the Public Ministry and police forces. The GOH should continue to support the developing law enforcement and regulatory entities responsible for combating money laundering and other financial crimes, and ensure that resources are available to strengthen its anti-money laundering regime. Sustained progress will depend upon increased commitment from the government to aggressively prosecute financial crimes. Honduras should draft and pass legislation specifically criminalizing the financing of terrorism to comport with international standards.

## Hong Kong

Hong Kong is a major international financial center. Its low taxes and simplified tax system, sophisticated banking system, the availability of secretarial services and shell company formation agents, and the absence of currency and exchange controls, facilitate financial activity but also make Hong Kong vulnerable to money laundering. The primary sources of laundered funds are tax evasion, fraud, illegal gambling and bookmaking, and intellectual property rights violations. Laundering channels include Hong Kong's banking system, and its legitimate and underground remittance and money transfer networks. The proceeds from narcotics trafficking are believed to be only a small percentage of illicit proceeds laundered. However, over the past two years, reportedly legitimate Hong Kong business entities and financial institutions have been playing an increasingly important role in the Black Market Peso Exchange (BMPE). The BMPE in Hong Kong is perpetuated by local Hong Kong business entities that either knowingly or unknowingly enter into business agreements with individuals directly associated with the BMPE process. The BMPE is a trade-based money laundering scheme used by Colombian drug cartels to launder illicit drug profits. Hong Kong is substantially in compliance with the Financial Action Task Force's (FATF) Forty Recommendations on Money Laundering, and has pledged to adhere to the revised FATF Forty Recommendations. It is a regional leader in anti-money laundering efforts. Hong Kong has been a member of the FATF since 1990.

Money laundering is a criminal offense in Hong Kong under the Drug Trafficking (Recovery of Proceeds) Ordinance (DTRoP) and the Organized and Serious Crimes Ordinance (OSCO). The money laundering offense extends to the proceeds of drug-related and other indictable crimes. Money laundering is punishable by up to 14 years' imprisonment and a fine of HK$5,000,000 (approximately $641,000).

Money laundering ordinances apply to covered institutions including banks and nonbank financial institutions, as well as to intermediaries such as lawyers and accountants. All persons must report suspicious transactions of any amount to the Joint Financial Intelligence Unit (JFIU). The JFIU does not investigate suspicious transactions itself, but receives, stores, and disseminates suspicious transactions reports (STRs) to the appropriate investigative unit. Typically, STRs are passed to the Narcotics Bureau or the Organized Crime and Triad Bureau of the Hong Kong Police Force, or to the Customs Drug Investigation Bureau of the Hong Kong Customs and Excise Department.

Financial regulatory authorities issued anti-money laundering guidelines reflecting the revised FATF Forty Recommendations on Money Laundering to institutions under their purview, and monitor compliance through on-site inspections and other means. The Hong Kong Monetary Authority is responsible for supervising and examining compliance of financial institutions that are authorized under Hong Kong's Banking Ordinance. The Hong Kong Securities and Futures Commission (SFC) is responsible for supervising and examining compliance of persons that are licensed by the SFC to conduct business in regulated activities as defined in Schedule 5 of the Securities and Futures Ordinance. The Office of the Commissioner of Insurance (OCI) is responsible for supervising and examining compliance of insurance institutions. Hong Kong law enforcement agencies provide training and feedback on suspicious transaction reporting.

Financial institutions are required to know and record the identities of their customers and maintain records for five to seven years. The filing of a suspicious transaction report cannot be considered a breach of any restrictions on the disclosure of information imposed by contract or law. Remittance agents and money changers must register their businesses with the police and keep customer identification and transaction records for cash transactions equal to or over HK$20,000 (approximately $2,564), and must retain these records for at least six years. Under a directive from Hong Kong's Monetary Authority, Hong Kong would reduce this threshold amount to HK$8000 (approximately $1000) effective January 1, 2007.

Hong Kong does not require reporting of the movement of currency above any threshold level across its borders, or reporting of large currency transactions above any threshold level. Hong Kong is examining the effectiveness of its existing regime in interdicting illicit cross border cash couriering activities. Reportedly, Hong Kong is deliberating ways of complying with FATF Special Recommendation Nine but does not intend to put in place the recommended "declaration system." Law enforcement agents in Hong Kong are already empowered to seize criminal proceeds at any place, including at the border.

There is no distinction made in Hong Kong between onshore and offshore entities, including banks, and no differential treatment is provided for nonresidents, including on taxes, exchange controls, or disclosure of information regarding the beneficial owner of accounts or other legal entities. Hong Kong's financial regulatory regimes are applicable to residents and nonresidents alike. The Hong Kong Monetary Authority (HKMA) regulates banks. The Office of Commissioner of Insurance (OCI) and the Securities and Futures Commission (SFC) regulate insurance and securities firms, respectively. All three impose licensing requirements and screen business applicants. There are no legal casinos or internet gambling sites in Hong Kong.

In Hong Kong, it is not uncommon to use solicitors and accountants, acting as company formation agents, to set up shell or nominee entities to conceal ownership of accounts and assets. Hong Kong registered 7,279 new international business companies (IBCs) in 2005. Many of the more than 500,000 IBCs created in Hong Kong are owned by other IBCs registered in the British Virgin Islands. Many of the IBCs are established with nominee directors. The concealment of the ownership of accounts and assets is ideal for the laundering of funds. Additionally, some banks permit the shell companies to open bank accounts based only on the vouching of the company formation agent. In such cases, the HKMA's anti-money laundering guidelines require banks to verify the identity of the

owners of the company, including beneficial owners. The bank should also assess whether the intermediary is "fit and proper." However, solicitors and accountants have filed a low number of suspicious transaction reports in recent years, and consequently have become a focus of attention to improve reporting through regulatory requirements and oversight.

The open nature of Hong Kong's financial system has long made it the primary conduit for funds being transferred out of China. Hong Kong's role has been evolving as China's financial system gradually opens. On February 25, 2004, Hong Kong banks began to offer Chinese currency- (renminbi or RMB) based deposit, exchange, and remittance services. Later in the year, Hong Kong banks began to issue RMB-based credit cards, which could be used both in mainland China and in Hong Kong shops that had signed up to the Chinese payments system, China Union Pay. In November 2005, Hong Kong banks were permitted modest increases in the scope of RMB business they can offer to clients. The new provisions raised daily limits and expanded services. Making loans in Hong Kong in RMB, however, is still not permitted for any bank. This change brought many financial transactions related to China out of the money-transfer industry and into the more highly regulated banking industry, which is better equipped to guard against money laundering.

Under the Drug Trafficking (Recovery of Proceeds) Ordinance (DTRoP) and the Organized and Serious Crimes Ordinance (OSCO), a court may issue a restraining order against a defendant's property at or near the time criminal proceedings are instituted. Both ordinances were strengthened in January 2003, through a legislative amendment lowering the evidentiary threshold for initiating confiscation and restraint orders against persons or properties suspected of drug trafficking. Property includes money, goods, real property, and instruments of crime. A court may issue confiscation orders at the value of a defendant's proceeds from illicit activities. Cash imported into or exported from Hong Kong that is connected to narcotics trafficking may be seized, and a court may order its forfeiture. Legitimate businesses can be seized if the business is the "realizable property" of the defendant or one of the defendants. Realizable property is defined under the DTRoP and OSCO as any property held by the defendant; any property held by a person to whom the defendant has directly or indirectly made a gift; or any property that is subject to the effective control of the defendant.

Hong Kong Customs and Hong Kong Police are responsible for conducting financial investigations. The Secretary of Justice is responsible for the legal procedures involved in restraining and confiscating assets. There is no time frame ascribed to freezing drug proceeds or the proceeds of other crimes. Regarding terrorist property, a formal application for forfeiture must be made within two years of freezing. Confiscated or forfeited assets and proceeds are paid into general government revenue.

As of October 31, 2006, the value of assets under restraint was $178 million, and the value of assets under a court confiscation order, but not yet paid to the government, was $8.85 million, according to figures from the JFIU. It also reported that as of October 31, 2006, the amount confiscated and paid to the government since the enactment of DTRoP and OSCO was $55.4 million, and a total of 395 persons had been convicted of money laundering over that period. Hong Kong has shared confiscated assets with the United States.

In July 2002, the legislature passed several amendments to the DTRoP and OSCO to strengthen restraint and confiscation provisions. These changes, which became effective on January 1, 2003, include the following: there is no longer a requirement of actual notice to an absconded offender; there is no longer a requirement that the court fix a period of time in which a defendant is required to pay a confiscation judgment; the court is allowed to issue a restraining order against assets upon the arrest (rather than charging) of a person; the holder of property is required to produce documents and otherwise assist the government in assessing the value of the property; and an assumption is created under the DTRoP, to be consistent with OSCO, that property held within six years of the period of the violation by a person convicted of drug money laundering is proceeds from that money laundering.

Since legislation was adopted in 1994 mandating the filing of suspicious transaction reports (STRs), the number of STRs received by JFIU has generally increased. In the first nine months of 2006, a total of 10,782 STRs were filed, of which 1330 were referred to law enforcement agencies. This compares to a total of 13,505 STRs filed during all of 2005; 14,029 filed during 2004; and 11,671 during 2003. The JFIU plans to launch an electronic system for reporting STRs by registered users in late 2006.

The JFIU receives disclosures, conducts analysis, and in suitable cases distributes them to law enforcement investigating units. The JFIU can distribute cases to all Hong Kong law enforcement agencies, to similar overseas bodies and, in certain circumstances, to regulatory bodies in Hong Kong. The JFIU also conducts research on money laundering trends and methods, and provides case examples (typologies) to financial and nonfinancial institutions in order to assist them in identifying suspicious transactions. The JFIU has no regulatory responsibilities.

The Hong Kong Police has a number of dedicated units responsible for investigating financial crime, but the Commercial Crimes and Narcotics Bureaus in the Police Headquarters are the primary units responsible for investigating money laundering and terrorist financing.

The JFIU analyzes STRs to develop information that could aid in prosecuting money laundering cases, the number of which has also increased since 1996, soon after the passage of OSCO (1994). There were 44 prosecutions for money laundering during the first 9 months of 2006, compared to 40 for the entire year of 2004 and 29 for 2003. Hong Kong Customs had a significant money laundering case in 2006, in which the mastermind of a local pirated optical disc syndicate was convicted of money laundering involving HK$ 27.4 million ($3.5 million). These proceeds accrued over a four-year period from piracy activities. In July 2002, Hong Kong's legislature passed the United Nations (Anti-Terrorism Measures) Ordinance criminalizing supplying funds to terrorists. On July 3, 2004, the Legislative Council passed the United Nations (Anti-Terrorism Measures) (Amendment) Ordinance. This law is intended to implement UNSCR 1373 and the FATF Special Eight Recommendations on Terrorist Financing that were in place in July 2004. It extends the Hong Kong Government's freezing power beyond funds to the nonfund property of terrorists and terrorist organizations. Furthermore, it prohibits the provision or collection of funds by a person intending or knowing that the funds will be used in whole or in part to commit terrorist acts. Hong Kong's financial regulatory authorities have directed the institutions they supervise to conduct record searches for assets of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224.

The People's Republic of China (PRC) represents Hong Kong on defense and foreign policy matters, including UN affairs. After the PRC becomes a party to a UN terrorism treaty, the Hong Kong Government submits implementing legislation to Hong Kong's Legislative Council. After passage, the HKG executes the relevant UN treaty. Through the PRC, the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime], the UN Convention against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism are all applicable to Hong Kong. The PRC ratified the UN Convention against Corruption on 13 January 2006 and the UN Convention for the Suppression of the Financing of Terrorism on 19 April 2006.

To help deal with anti-money laundering (AML) issues from a practical perspective and reflect business needs, the Hong Kong Monetary Authority (HKMA) has recently coordinated the establishment of an Industry Working Group on AML, which includes representatives of some 20 authorized institutions. The Group has met twice, and three sub-groups have been established to share experiences and consider the way forward on issues such as PEPs (politically exposed persons), terrorist financing, transaction monitoring systems and private banking issues. The HKMA is also taking a number of initiatives on AML issues, including issuing circulars and guidance to authorized institutions on combating the financing of weapons of mass destruction, conducting in-depth

examinations of institutions' AML controls, and setting out best practices for AML in high-risk areas such as correspondent banking, private banking and remittance.

The HKMA circulated guidelines in 2004 incorporating the FATF Special Eight Recommendations on Terrorist Financing which require banks to maintain a database of terrorist names and management information systems to detect unusual patterns of activity in customer accounts. The Securities and Futures Commission (SFC) and the Office of the Commissioner of Insurance (OCI) circulated guidance notes in 2005 that provided additional guidance on customer due diligence and other issues, reflecting the new requirements in the Revised FATF Forty Recommendations on Money Laundering, and Special Recommendations on Terrorist Financing. The Hong Kong government has modified its regulations in order to make them consistent with the revised FATF Forty Recommendations on Money Laundering. In 2006, the OCI and the SFC revised their guidance notes to take into account the latest recommendations by the FATF.

Other bodies governing segments of the financial sector are also active in anti-money laundering efforts. The Hong Kong Estates Agents Authority, for instance, has drawn up specific guidelines for real estate agents on filing suspicious transaction reports, and the Law Society of Hong Kong and the Hong Kong Institute of Certified Public Accountants are in the process of drafting such guidance.

In 2003, Hong Kong took part in the International Monetary Fund's Financial Sector Assessment Program (FSAP), which aims to strengthen the financial stability of a jurisdiction by identifying the strengths and weaknesses of its financial system and assessing compliance with key international standards. As part of the FSAP, a team of IMF and World Bank-sponsored legal and financial experts assessed the effectiveness of Hong Kong's anti-money laundering regime against the FATF Forty Recommendations on Money Laundering and the FATF Special Recommendations on Terrorist Financing. The team described Hong Kong's anti-money laundering measures as "resilient, sound, and overseen by a comprehensive supervisory framework."

The Financial Investigations Division of the Narcotics Bureau has assisted the FBI in the investigation of the fugitives arrested in the United States in conjunction with the Bank of China case. In 2006, in a joint operation among the U.S. Immigration and Customs Enforcement (ICE), the U.S. Food and Drug Administration and Hong Kong Customs, a major mainland Chinese trafficker in counterfeit pharmaceutical drugs was identified. In September 2006, when the subject of the investigation arrived at a meeting in Hong Kong arranged by undercover agents, he was arrested by Hong Kong Customs officers under the Fugitive Offenders Ordinance.

Through the PRC, Hong Kong is subject to the 1988 UN Drug Convention. It is an active member of the FATF and Offshore Group of Banking Supervisors and also a founding member of the Asia Pacific Group on Money Laundering (APG). Hong Kong's banking supervisory framework is in line with the requirements of the Basel Committee on Banking Supervision's "Core Principles for Effective Banking Supervision." Hong Kong's JFIU is a member of the Egmont Group and is able to share information with its international counterparts. Hong Kong is known to cooperate with foreign jurisdictions in combating money laundering.

Hong Kong's mutual legal assistance agreements generally provide for asset tracing, seizure, and sharing. Hong Kong signed and ratified a mutual legal assistance agreement with the United States that came into force in January 2000.

Hong Kong has mutual legal assistance agreements with a total of 21 other jurisdictions: Australia, Canada, the United States, Italy, the Philippines, the Netherlands, Ukraine, Singapore, Portugal, Ireland, France, the United Kingdom, New Zealand, the Republic of Korea, Belgium, Switzerland, Denmark, Israel, Poland, Germany and Malaysia. Hong Kong has also signed surrender-of-fugitive-offenders agreements with 16 countries, and has signed Agreements for the transfer-of-sentenced-persons with eight countries, including the United States.

Hong Kong authorities exchange information on an informal basis with overseas counterparts, with Interpol, and with Hong Kong-based liaison officers of overseas law enforcement agencies. An amendment to the Banking Ordinance in 1999 allows the HKMA to disclose information to an overseas supervisory authority about individual customers, subject to conditions regarding data protection. The HKMA has entered into memoranda of understanding with overseas supervisory authorities of banks for the exchange of supervisory information and cooperation, including on-site examinations of banks operating in the host country.

The Government of Hong Kong should further strengthen its anti-money laundering regime by establishing threshold reporting requirements for currency transactions and putting into place "structuring" provisions to counter evasion efforts. Per FATF Special Recommendation Nine, Hong Kong should also establish mandatory cross-border currency reporting requirements. Hong Kong should continue to encourage more suspicious transaction reporting by lawyers and accountants, as well as by business establishments such as auto dealerships, real estate companies, and jewelry stores. Hong Kong should also take steps to stop the use of "shell" companies, IBCs, and other mechanisms that conceal the beneficial ownership of accounts by more closely regulating corporate formation agents. Particularly since Hong Kong is a major trading center, Hong Kong law enforcement and customs authorities should seek to identify trade-based money laundering.

## Hungary

Taking advantage of its pivotal location in central Europe, its cash-based economy and its well-developed financial services industry, criminal organizations from countries such as Russia and Ukraine have reportedly entrenched themselves in Hungary. Money laundering is related to a variety of criminal activities, including narcotics, prostitution, trafficking in persons, and organized crime. Additional financial crimes such as counterfeiting of euros, real estate fraud, and the copying/theft of bankcards are also prevalent. Financial crime has not increased in recent years, though there have been some isolated, albeit well-publicized, cases.

Hungary has been continuously improving its money laundering enforcement regime following its 2003 removal from the Financial Action Task Force (FATF) list of noncooperative countries and territories. Since then, it has worked to implement the FATF Forty Recommendations and the Nine Special Recommendations on Terrorist Financing. In early 2005, the International Monetary Fund (IMF), in conjunction with the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), conducted the third-round mutual evaluation of Hungary's anti-money laundering and counterterrorism financing regime. The evaluation team published the results of their assessment in June 2005.

Reacting to the advice cited in the mutual evaluation report, Hungary adopted an Action Plan and a new draft Anti-Money Laundering Act (AMLA) that will be submitted to the Parliament in September 2007. The draft AMLA addresses several (but not all) of the deficiencies cited in the mutual evaluation report. The draft law brings Hungary into compliance with the Vienna and Palermo Conventions by enlarging the scope of the money laundering offense so that it covers the transfer of proceeds to a third party even if it is carried out through a nonbanking or nonfinancial transaction. The draft AMLA also addresses reporting problems within Hungary's AML reporting system. According to the evaluation report, harsh criminal penalties for nonreporting have resulted in over filing by Hungarian financial institutions which are producing a high volume of suspicious transaction reports (STRs)—but which are of low quality. The draft law reduces the maximum punishment for the intentional failure to comply with reporting obligations from three years imprisonment to two years imprisonment. The maximum penalty for negligence in reporting has likewise been reduced from two years imprisonment to one year imprisonment, community service, or fine. Currently, the Hungarian Criminal Code only criminalizes terrorist acts committed by a group. The draft AMLA will include

provisions punishing the financing of terrorist acts which are committed by an individual. The draft law also establishes a clear legal basis for the obligation to report suspicious transactions relating to the financing of terrorism.

The AMLA also addresses FATF Special Recommendation Nine regarding cash couriers by requiring the declaration to Customs authorities of all movements of cash exceeding 10,000 euros (approximately $13,000). The draft law also calls for the establishment of an electronic database for the managing and processing of data contained in the Customs declarations.

Hungary banned offshore financial centers by Act CXII of 1996 on Credit Institutions. Offshore casinos are also prohibited from operating by the 1996 Act. At one time, there were offshore companies registered in Hungary that enjoyed a preferential tax benefits. However, the preferential tax treatment was phased out at the end of 2005 and in 2006, these companies were converted automatically into Hungarian companies. The only special status they retain is the ability to keep financial records in foreign currencies. Hungary no longer permits the operation of free trade zones.

Hungary's first enacted anti-money laundering legislation in 1994 with Act XXIV. Hungary's money laundering legislation covers all serious crimes punishable by imprisonment. In April 2002, Section 303 of the Penal Code on Money Laundering was amended to criminalize self- laundering. In 2003, the Government of Hungary (GOH) re-codified its money laundering legislation in Act XV of 2003, "On the Prevention and Impeding of Money Laundering," which became effective on June 16, 2003. The 2003 Act extends the anti-money laundering legislation to encompass the following additional professions and business sectors: financial services, investment services, insurance, stock brokers, postal money transfers, real estate agents, auditors, accountants, tax advisors, gambling casinos, traders of gems or other precious metals, private voluntary pension funds, lawyers, and public notaries. Act XV also criminalizes tipping off and forces self-regulating professions to submit internal rules to identify asset holders, track transactions, and report suspicious transactions.

Hungary's financial regulatory body, the Hungarian Financial Supervisory Authority (HFSA), is charged with supervising financial service providers with the exception of cash processors, which are supervised by the National Bank of Hungary. Most designated nonfinancial businesses and professions (DNFBP) such as auditors, casinos, lawyers, and notaries are supervised by their own trade associations. Either the Hungarian National Police (HNP) or the Financial Intelligence Unit (FIU) within the HNP acts as the regulator for all other entities that are covered under the 2003 Act and that have no formal supervisory authority. In 2005, the HFSA conducted 169 on-site AML compliance inspections and issued enforcement warnings in 62 cases. In 2006, the HFSA established a new department specializing in issues pertaining to money laundering and financial crimes. That department is responsible for the coordination of supervisory tasks and duties related to money laundering and terrorist financing, and also assists other departments of the HFSA with on-site inspections.

The 2003 Act also states that covered service providers are required to identify their customers, or any authorized individual representing their customers, when entering into a business relationship. In transactions exceeding two million HUF (approximately $10,300) or transactions of any amount where suspicion of money laundering arises, the customer must be identified. Under the anti-money laundering legislation, banks, financial institutions, and other service providers are required to maintain records for at least ten years. All service providers are required to report suspicious transactions directly, or through their representation bodies, to the police authority as soon as they occur. Lawyers and notaries are obliged to file reports, except when they are representing their clients in a criminal court case. Both lawyers and notaries submit their reports to their respective bar and notary associations, which then forward the reports on to the police. All other service providers submit their reports directly to the police. The police may randomly perform on-site checks of service

providers. According to Hungarian bank secrecy regulations, financial service providers are obliged to supply law enforcement authorities with relevant data.

Safe harbor provisions protect individuals when executing their anti-money laundering reporting obligations. If the report involves suspicious activity related to terrorist financing, the law allows for the possibility of protection. Currently, however, actual extension of protection is granted at the discretion of the prosecutor.

As of 2001, only banks or their authorized agents can operate currency exchange booths. There are currently approximately 300 exchange booths in Hungary. These exchange booths are subject to "double supervision," because they are subject to the banks' internal control mechanisms, which are in turn subject to supervision by the HFSA. Exchange booths must verify customer identity for currency exchange transactions totaling or exceeding HUF 300,000 (approximately $1,500). These amounts can derive either from a single transaction or consecutive separate transactions which, in sum, exceeds this threshold. The exchange booths are also required to file suspicious transaction reports (STRs) for questionable currency exchange transactions in any amount. Monitoring of these suspicious transactions has resulted in ongoing criminal investigations.

Act CXX of 2001 eliminated bearer shares and required that all such shares be transferred to identifiable shares by the end of 2003. All shares now are subject to transparency requirements, and both owners and beneficiaries must be registered. By mid-2003, Hungary had successfully transferred 90 percent of anonymous savings accounts into identifiable accounts. Individuals must now have written permission from the police in order to access them.

Hungary's Financial intelligence Unit (FIU) is an investigative FIU and is part of the HNP. It investigates money laundering cases and has considerable authority to request and release information, both domestically and internationally. In the summer of 2004, the HNP completed a major organizational restructuring that included the establishment of the National Bureau of Investigation (NBI). The NBI is responsible for the detection and investigation of major corruption and money laundering cases. This restructuring has eliminated the parallel jurisdictions that existed in economic and financial crime investigations, and implemented a more coordinated investigative effort for money laundering investigations. The NBI houses the resulting new division, the Economic and Financial Crimes Department. The NBI has a staff of 134 at the headquarters level.

The FIU receives and investigates suspicious transaction information. In the first six months of 2006, the FIU received 5,195 STRs, opened 5,197 cases, and referred twenty of these cases to prosecutors. Banks filed the majority of these reports (80 percent), as well as currency exchange houses (16 percent). The 2005 Action Plan requires an impact study to review the supervision of these sectors, and aims to create programs to improve supervision and provide increased outreach and guidance to DNFBP's with regard to reporting obligations. Currently all obligated entities file reports using a paper system. However, the FIU is currently developing and testing a new electronic reporting system. During the first six months of 2006, a total of 20 money laundering investigations, involving 26 individuals had been opened. Five of these cases (14 persons) have reached the prosecution stage and are awaiting final judgments.

The Hungarian Criminal Code, Act XIX of 1998, and amended by Act II of 2003, contains a provision on the forfeiture of assets. Under this provision, assets that were used to commit crimes, would endanger public safety, or were created as a result of criminal activity, are subject to forfeiture. All property related to criminal activity during the period of time when the owner was a party to a criminal organization can be seized, unless proven to have been obtained in good faith as due compensation. Act II of 2003 states that persons or members of criminal organizations sponsoring activities of a terrorist group by providing material assets or any other support face five to fifteen years of imprisonment.

For most crimes, with the exception of terrorism financing, the police (including the FIU) freeze the assets and must then inform the bank within 24 hours as to whether there will be an investigation. Police investigations must be completed within two years of filing charges. Forfeiture and seizure for all crimes, including terrorist financing, is determined by a court ruling. The banking community has cooperated fully with enforcement efforts to trace funds and seize/freeze bank accounts. In all cases, some of the frozen assets may be released, for example, to cover health-related expenses or basic sustenance, if the FIU approves a written request from the owner of the assets. After subtracting any related civil damages, proceeds from asset seizures and forfeitures go to the government. In the first half of 2006, authorities seized assets in two money laundering cases worth a total of approximately 435,000 euro ($563,000).

Act IV of 1978, Article 261, criminalizes terrorist acts. Hungary has criminalized terrorism and all forms of terrorism financing with Act II of 2003, which modifies Criminal Code Article 261. The offense includes providing or collecting funds for terrorist actions or facilitating or supporting such actions by any means. The penalty for such crimes is imprisonment of five to fifteen years. The Hungarian Criminal Code does not include a separate provision for the financing of a terrorist act conducted by an individual. The FIU reported that only two of the STRs filed in 2006 were related to the financing of terrorism, in part because Hungary's current AML law does not provide a solid legal basis for an obligation to report suspicious financial activity related to terrorism financing. The draft AMLA contains provisions to correct these legal deficiencies.

The Hungarian Criminal Code treats terrorist financing-related crimes differently than all other crimes. Hungary can freeze terrorist finance-related assets. Act XIX of 1998 on Criminal Procedures, Articles 151, 159, and 160, provide for the immediate seizure, sequestration, and precautionary measures against terrorist assets. In cases where terrorist financing is suspected, banks freeze the assets and then promptly notify HFSA, the FIU, and the Ministry of Finance. The FIU must inform the banks within 24 hours whether or not it will conduct an investigation. The GOH circulates to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. Act CXII of 1996 on Credit Institutions bans the use of any indigenous alternative remittance systems that bypass, in whole or in part, financial institutions. In cases where money is transferred to a charitable or nonprofit entity, the GOH will freeze the assets regardless of the amount.

Hungary and the United States have a Mutual Legal Assistance Treaty and a nonbinding information-sharing arrangement designed to enable U.S. and Hungarian law enforcement to work more closely to fight organized crime and illicit transnational activities. In May 2000, Hungary and the U.S. Federal Bureau of Investigation established a joint task force to combat Russian organized crime groups. Hungary has signed bilateral agreements with 41 other countries to cooperate in combating terrorism, drug-trafficking, and organized crime.

Hungary is a member of the Council of Europe's MONEYVAL. Hungary's FIU has been a member of the Egmont Group since 1998.

Hungary is a party to the UN International Convention for the Suppression of the Financing of Terrorism; 1988 UN Drug Convention; and the UN Convention against Corruption. In December 2006 Hungary ratified the UN Convention against Transnational Organized Crime.

Hungary has made progress in developing its anti-money laundering regime. However, the GOH needs to continue its efforts with regard to implementation. An increased level of cooperation and coordination is needed among the different law enforcement entities involved in the anti-money laundering regime in Hungary. Prosecutors, judges, and police require additional training in order to promote the successful prosecution of money laundering cases. The HFSA and other supervisory bodies should improve supervision and provide increased outreach and guidance to financial

institutions with regard to reporting obligations. The GOH should take steps to ensure that nonbank financial institutions file suspicious transactions reports. Increased AML/CTF training for the employees of financial institutions and other obliged entities is also necessary in order to improve the number and quality of STRs filed, in particular those which may be related to the financing of terrorism. The FIU should continue work on the electronic reporting system until it is operational, and implement it. The GOH should enact the draft AMLA in September 2007 to ensure that Hungary comports with international standards, including those relating to the financing of terrorism.

## India

India's growing status as a regional financial center, its large system of informal cross-border money flows, and its widely perceived tax avoidance problems all contribute to the country's vulnerability to money laundering activities. Some common sources of illegal proceeds in India are narcotics trafficking, trade in illegal gems (particularly diamonds), smuggling, trafficking in persons, corruption, and income tax evasion. Historically, because of its location between the heroin-producing countries of the Golden Triangle and Golden Crescent, India has been a drug-transit country.

India's strict foreign-exchange laws and transaction reporting requirements, combined with the banking industry's due diligence policy, make it difficult for criminals to use banks or other financial institutions to launder money. Accordingly, large portions of illegal proceeds are laundered through the alternative remittance system called "hawala" or "hundi." The hawala market is estimated at anywhere between 30 and 40 percent of the formal market. Remittances to India reported through legal, formal channels in 2005-2006 amounted to $24 billion (reportedly the largest in the world).

Reportedly, many Indians do not trust banks and prefer to avoid the lengthy paperwork required to complete a money transfer through a financial institution. The hawala system can provide the same remittance service as a bank with little or no documentation and at lower rates and provide anonymity and security for their customers. The Government of India (GOI) neither regulates hawala dealers nor requires them to register with the government. The Reserve Bank of India (RBI), the country's Central Bank, argues that the widespread hawala dealers operate illegally and therefore cannot be registered and are beyond the reach of regulation. Reportedly, the RBI does intend to increase its regulation of nonbank money transfer operations by entities such as currency exchange kiosks and wire transfer services.

Historically, gold has been one of the most important commodities involved in Indian hawala transactions. There is a widespread cultural demand for gold in the region. India liberalized its gold trade restrictions in the mid-1990s. In recent years, many believe the growing Indian diamond trade has also been increasingly important in providing countervaluation, a method of "balancing the books" in external hawala transactions. Invoice manipulation is used extensively to avoid both customs duties, taxes and to launder illicit proceeds through trade-based money laundering.

India has illegal black market channels for selling goods. Smuggled goods such as food items, computer parts, cellular phones, gold, and a wide range of imported consumer goods are routinely sold through the black market. By dealing in cash transactions and avoiding customs duties and taxes, black market merchants offer better prices than those offered by regulated merchants. However, due to trade liberalization and an increase in the number of foreign companies doing business in India, the business volume in smuggled goods has fallen significantly. Most products previously sold in the black market are now traded through lawful channels.

While tax evasion is also widespread, the GOI is gradually making changes to the tax system. The government now requires individuals to use a personal identification number to pay taxes, purchase foreign exchange, and apply for passports. The GOI also introduced a value added tax (VAT) in April 2005 which replaced numerous complicated state sales taxes and excise taxes. As a result, the

incentives and opportunities for businesses to conceal their sales or income levels have been reduced. Most of the twenty-eight Indian states have implemented the national VAT mandate, and the GOI anticipates that all states will be compliant by April 2007.

The Criminal Law Amendment Ordinance allows for the attachment and forfeiture of money or property obtained through bribery, criminal breach of trust, corruption, or theft, and of assets that are disproportionately large in comparison to an individual's known sources of income. The 1973 Code of Criminal Procedure, Chapter XXXIV (Sections 451-459), establishes India's basic framework for confiscating illegal proceeds. The Narcotic Drugs and Psychotropic Substances Act (NDPSA) of 1985, as amended in 2000, calls for the tracing and forfeiture of assets that have been acquired through narcotics trafficking and prohibits attempts to transfer and conceal those assets. The Smugglers and Foreign Exchange Manipulators Act (SAFEMA) also allows for the seizure and forfeiture of assets linked to Customs Act violations. The competent authority (CA), located in the Ministry of Finance (MOF), administers both the NDPSA and the SAFEMA.

2001 Amendments to the NDPSA allow the CA to seize any asset owned or used by a narcotics trafficker immediately upon arrest. Previously, assets could only be seized after a conviction. Even so, Indian law enforcement officers lack training in the procedures for identifying individuals who might be subject to asset seizure/forfeiture and in tracing assets to be seized. They also appear to lack sufficient training in drafting and expeditiously implementing asset freezing orders. In 2005, pursuant to the NDPSA and with U.S. Government funding through its Letter of Agreement with India, the CA held nine asset seizure and forfeiture workshops in New Delhi, Himachal Pradesh, Uttar Pradesh, Rajasthan, and Andra Pradesh to train law enforcement officers in asset seizure and forfeiture procedures and regulations. The GOI hopes the training will lead to increased seizures and forfeitures from illicit narcotics proceeds.

The Foreign Exchange Management Act (FEMA), implemented in 2000, is one of the GOI's primary tools for fighting money laundering. The FEMA's objectives include establishing controls over foreign exchange, preventing capital flight, and maintaining external solvency. FEMA also imposes fines on unlicensed foreign exchange dealers. A closely related piece of legislation is the Conservation of Foreign Exchange and Prevention of Smuggling Act (COFEPOSA), which provides for preventive detention in smuggling and other matters relating to foreign exchange violations. The MOF's Directorate of Enforcement (DOE) enforces FEMA and COFEPOSA. The RBI also plays an active role in the regulation and supervision of foreign exchange transactions.

The Prevention of Money Laundering Act (PMLA) was signed into law in January 2003. This legislation criminalizes money laundering, establishes fines and sentences for money laundering offenses, imposes reporting and record keeping requirements on financial institutions, provides for the seizure and confiscation of criminal proceeds, and provides for the creation of a financial intelligence unit (FIU). Implementing rules and regulations for the PMLA were promulgated in July 2005. Penalties for offenses under the PMLA are severe and may include imprisonment for three to seven years and fines as high as $10,280. If the money laundering offense is related to a drug offense under the NDPSA, imprisonment can be extended to a maximum of ten years. The PMLA mandates that banks, financial institutions, and intermediaries (such as stock market brokers) maintain records of all cash transactions exceeding $21,740. However, to date, there have been no prosecutions or convictions under the PMLA.

With the notification of the PMLA in July 2005, a financial intelligence unit (FIU) was established in January 2006 with the mandate to combat money laundering and terrorist financing. The FIU is the central repository to receive process, analyze, and disseminate information from suspicious transaction reports (STRs) and general cash transaction reports from financial institutions, banking companies, and intermediaries. It acts independently to refer such cases to the appropriate enforcement agency. Since it was initiated, India's FIU has received about 450 STRs.

The FIU is also responsible for strengthening efforts amongst the intelligence, investigative, and law enforcement agencies towards reaching global standards to prevent money laundering and related crimes. The FIU reports directly to the Economic Intelligence Council, which is headed by the Finance Minister. Administratively, it falls under the supervision of MOF's Department of Revenue. The FIU is not a regulatory agency but is permitted to exchange information with foreign FIUs on the basis of reciprocity, mutual agreement, or critical threat information on a case-by-case basis. There have been approximately 20 such information exchanges since FIU's establishment. As an Egmont observer, India's exchange of information with foreign FIUs is limited whereas full membership enables access to a global framework of sharing and obtaining terrorism financing information.

The MOF's Enforcement Directorate is responsible for investigations and for the prosecution of money laundering cases. The GOI has established an Economic Intelligence Council (EIC) to enhance coordination among the various enforcement agencies and directorates in the MOF. The EIC provides a forum for enforcement agencies to strengthen intelligence and operational coordination, to formulate common strategies to combat economic offenses, and to discuss cases requiring interagency cooperation. In addition to the EIC, there are eighteen regional economic committees in India. The Central Economic Intelligence Bureau (CEIB) functions as the secretariat for the EIC. The CEIB interacts with the National Security Council, the Intelligence Bureau, and the Ministry of Home Affairs on matters concerning national security and terrorism.

The FIU and the MOF are actively working to amend regulations in order to be compliant with international standards. At present, the PMLA does not include comprehensive provisions on terrorism financing. The MOF has organized a committee of the relevant departments and ministries to amend the PMLA, which are likely to be introduced in the July-August, 2007 parliamentary session. Amendments will include provisions to criminalize terrorism financing and incorporate most of the FATF recommended categories of offenses.

In October 2006, the Finance Ministry stated that India had agreed to reconcile its list of predicate crimes with that of the Financial Action Task Force (FATF) and not set minimum property value thresholds on predicate crimes. As of December 2006, India is a FATF observer and has a two year probationary period to become compliant with FATF norms to become a member. Full FATF membership has been one criterion identified to help India move towards a sufficient anti-money laundering and terrorist financing (AML/CTF) regime required by the U.S. Federal Reserve Board in making determinations on foreign bank branch applications. In this context, the GOI is seeking to amend the PMLA to block terrorism financing through banking and financial institution channels. After PMLA changes are fully enacted, the Securities and Exchange Board of India (SEBI) Act will also be revised to include similar offenses.

The Central Bureau of Investigation (CBI), the Directorate of Revenue Intelligence (DRI), Customs and Excise, RBI, the Competent Authority, and the MOF are all active in anti-money laundering efforts. During 2004, DRI referred four hawala-based money laundering cases with a U.S. nexus to the U.S. Department of Homeland Security/Immigration and Customs Enforcement (DHS/ICE). DHS/ICE carried out successful investigations on three of these cases and forwarded tangible results to the MOF's Department of Enforcement. During 2005, the Directorate of Enforcement (DOE) forwarded two additional hawala-linked money laundering cases to DHS/ICE. DHS/ICE has provided investigative assistance.

Many banking institutions, prompted by the RBI, have taken steps on their own to combat money laundering. For example, banks are beginning to hire compliance officers to ensure that anti-money laundering regulations are being observed. The RBI issued a notice in 2002 to commercial banks instructing them to adopt the due diligence rules. The Indian Bankers Association established a working group to develop self-regulatory anti-money laundering procedures. Foreign customers, applying for accounts in India must show proof of identity when opening a bank account. Banks also

require that the source of funds must be declared if the deposit is more than $10,000. Finally, banks must report suspicious transactions.

Since March 2006, the FIU has been receiving reports on suspicious transactions and cash flows from banks, financial institutions, and intermediaries involving over USD $22,490. About 50 percent of such transactions are reported electronically by public and private banks (led by the large private banks) while the other institutions are only equipped to report manually. The FIU is in the process of developing a secure gateway for submission of electronic STRs which should be in place by December 2007.

A circular to all intermediaries registered with SEBI was issued on the obligations to prevent money laundering. The circular included information on the maintenance of records, preservation of information with respect to certain transactions, and reporting to the Director of the FIU suspicious cash flows and financial transactions.

The GOI has the power to order banks to freeze assets. In November 2004, the RBI issued a circular updating its due diligence guidelines drafted to ensure that they comply with Financial Action Task Force (FATF) recommendations. The guidelines include the requirement that banks identify politically-connected account holders residing outside India and identify the source of funds before accepting deposits from these individuals. The UNSCR 1267 Sanctions Committee's consolidated list is routinely circulated to all financial institutions. The RBI also asked all commercial banks to become FATF-compliant in terms of customer identification for existing as well as new accounts. These guidelines went into effect in December 2005. Banks have been enforcing the guidelines strictly with new customers and gradually phasing in the procedures with old customers. High-risk accounts are subject to intense monitoring.

India does not have an offshore financial center but does license offshore banking units (OBUs). These OBUs are required to be predominantly owned by individuals of Indian nationality or origin resident outside India. The OBUs include overseas companies, partnership firms, societies, and other corporate bodies. OBUs must be audited to confirm that ownership by a nonresident Indian is not less than 60 percent. These entities are susceptible to money laundering activities, in part because of a lack of stringent monitoring of transactions in which they are involved. Finally, OBUs must be audited financially; however, the auditing firm is not required to obtain government approval.

The CBI is a member of INTERPOL. All state police forces and other law enforcement agencies have a link through INTERPOL/New Delhi to their counterparts in other countries for purposes of criminal investigations. India's Customs Service is a member of the World Customs Organization and shares enforcement information with countries in the Asia/Pacific region.

GOI regulations governing charities remain antiquated and the process by which charities are governed at the provincial and regional levels remain weak. The GOI does require charities to register with the state-based Registrar of Societies, and, if seeking tax exempt status, they must apply separately with the Exemptions Department of the Central Board of Direct Taxes. There remain no guidelines or provisions governing the oversight of charities for AML/CFT purposes, and there remains a need for increased integration between charities regulators and law enforcement authorities regarding the threat of terrorist finance. In April 2002, the Indian Parliament passed the Prevention of Terrorism Act (POTA), which criminalizes terrorist financing. In March 2003, the GOI announced that it had charged 32 terrorist groups under the POTA. In July 2003, the GOI announced that it had arrested 702 persons under the POTA. In November 2004, the Parliament repealed the POTA and amended the 1967 Unlawful Activities (Prevention) Act to include the POTA's salient elements such as criminalization of terrorist financing.

India is a party to the 1988 UN Drug Convention, and is a member of the Asia/Pacific Group (APG) on Money Laundering. India implements the 1988 UN Drug Convention through amendments to the

NDPSA (in 1989 and 2001) and the PMLA. It is a signatory to, but has not yet ratified, the UN Convention against Transnational Organized Crime. India is a party to the UN International Convention for the Suppression of the Financing of Terrorism. In October 2001, the GOI and the United States signed a mutual legal assistance treaty, which took effect in October 2005. India has also signed a police and security cooperation protocol with Turkey that provides for joint efforts to combat money laundering. The GOI is implementing this convention through the Unlawful Activities Prevention Act.

Since terrorist financing in India is linked to the hawala system, the Government of India should cooperate fully with international initiatives to provide increased transparency in alternative remittance systems, and, if necessary should initiate regulation and increase law enforcement actions in this area. India should examine the scope of its citizens' involvement in the illicit international diamond trade. It also needs to quickly finalize the implementation of regulations to the anti-money laundering law and ensure that the new FIU is fully operational. Meaningful tax reform will also assist in negating the popularity of hawala and lessen money laundering. Increased enforcement action should also be taken in order to effectively combat trade-based money laundering. Additionally, India should become a party to the UN Convention against Transnational Organized Crime.

## Indonesia

Although neither a regional financial center nor an offshore financial haven, Indonesia is vulnerable to money laundering and terrorist financing due to a poorly regulated financial system, the lack of effective law enforcement, and widespread corruption. Most money laundering in the country is connected to nondrug criminal activity such as gambling, prostitution, bank fraud, piracy and counterfeiting, illegal logging, and corruption. Indonesia also has a long history of smuggling, a practice facilitated by thousands of miles of un-patrolled coastline and a law enforcement system riddled with corruption. The proceeds of these illicit activities are easily parked offshore and only repatriated as required for commercial and personal needs.

As a result of Indonesia's ongoing efforts to implement the reforms to its Anti-Money Laundering (AML) regime, the Financial Action Task Force (FATF) removed Indonesia from its list of Non-Cooperative Countries and Territories (NCCT) on February 11, 2005 and subsequent special FATF monitoring on February 11, 2006. The removal of Indonesia from the NCCT list and special monitoring recognized a concerted, interagency effort-supported by President Susilo Bambang Yudhoyono-to further develop Indonesia's nascent AML regime.

Indonesia's Financial Intelligent Unit (PPATK), established in December 2002 and fully functional since October 2003, continues to make steady progress in developing its human and institutional capacity. The PPATK is an independent agency that receives, analyzes, and evaluates currency and suspicious financial transactions, provides advice and assistance to relevant authorities, and issues publications. As of November 30, 2006 the PPATK has received approximately 6,884 suspicious transactions reports (STRs) from 115 banks and 47 nonbank financial institutions. The volume of STRs has increased from an average of 70 per month in 2004 to 324 per month in 2006. The agency also reported that it had received over 1.9 million cash transaction reports (CTRs). Based on their analysis of 608 STRs, PPATK investigators have referred 417 cases to the police. Based on referrals of STRs and other related information from the PPATK, there have been over 30 convictions for money laundering or its predicate crimes, including six for money laundering only. Of the six money laundering convictions, three were handed down in January and included sentences between five to seven years.

Indonesia's Anti-Money Laundering and Counter Terrorism Finance (CTF) Donors' Coordination Group, co-chaired by the PPATK and the Australian Agency for International Development (AUSAID), has become a model for AML/CTF donors' coordination groups in other countries. Since

Indonesia's removal form the NCCT list, donors and the Government of Indonesia (GOI) have placed greater emphasis on more practical training; technical and capacity-building assistance for the nonbank financial sector, police, prosecutors and judges; cash smuggling; and regulation of charities and money changers. In July 2006, the Asia Pacific Group (APG) named PPATK Chairman Yunus Husein a co-chair of the regional FATF style organization for a two-year term. In November 2006, Indonesia hosted the annual APG Typologies Workshop.

The PPATK is actively pursuing broader cooperation with relevant GOI agencies. The PPATK has signed ten domestic memoranda of understanding (MOUs) to assist in financial intelligence information exchange with the following entities: Attorney General's Office (AGO), Bank Indonesia (BI), the Capital Market Supervisory Agency (Bapepam), the Ministry of Finance Directorate General of Financial Institutions, the Directorate General of Taxation, Director General for Customs and Excise, the Ministry of Forestry Center for International Forestry Research, the Indonesian National Police, the Supreme Audit Board (BPK), and the Corruption Eradication Committee.

Sustained public awareness campaigns, new bank and financial institution disclosure requirements, and the PPATK's support for Indonesia's first credible anticorruption drive have led to increased public awareness about money laundering and, to a lesser degree, terrorism finance. However, weak human and technical capacity, poor interagency cooperation, and corruption, still remain significant impediments to the continuing development of an effective and credible AML regime.

Banks and other financial institutions now routinely question the sources of funds or require identification of depositors or beneficial owners. Financial reporting requirements were put in place in the wake of the 1998 Asian financial crisis when the GOI became interested in controlling capital flight and recovering foreign assets of large-scale corporate debtors or alleged corrupt officials.

In April 2002, Indonesia passed Law No. 15/2002 Concerning the Crime of Money Laundering, making money laundering a criminal offense. The law identifies 15 predicate offenses related to money laundering, including narcotics trafficking and most major crimes. Law No. 15/2002 established the PPATK to develop policy and regulations to combat money laundering and terrorist financing.

In September 2003, Parliament passed Law No. 25/2003 amending Law No. 15/2002 Concerning the Crime of Money Laundering in order to address many FATF concerns. Amending Law No. 25/2003 provides a new definition of the crime of money laundering making it an offense for anyone to deal intentionally with assets known or reasonably suspected to constitute proceeds of crime with the purpose of disguising or concealing the origins of the assets. The amendment removes the threshold requirement for proceeds of crime and expands the definition of proceeds of crime to cover assets employed in terrorist activities. The amendment expands the scope of regulations requiring STRs to include attempted or unfinished transactions. The amendment also shortens the time to file an STR to three days or less after the discovery of an indication of a suspicious transaction. The amendment makes it an offense to disclose information about the reported transactions to third parties, which carries a maximum of five years' imprisonment and a maximum of one billion rupiah (approximately $110,000). Articles 44 and 44A provide for mutual legal assistance with respect to money laundering cases, with the ability to provide assistance using the compulsory powers of the court. Article 44B imposes a mandatory obligation on the PPATK to implement provisions of international conventions or international recommendations on the prevention and eradication of money laundering. In March 2006, the GOI enacted Indonesia's first Mutual Legal Assistance (MLA) Law (No. 1/2006), establishing formal, binding procedures to facilitate MLA with other states.

Bank Indonesia (BI), the Indonesian Central Bank, issued Regulation No. 3/10/PBI/2001, "The Application of Know Your Customer Principles," on June 18, 2001. This regulation requires banks to obtain information on prospective customers, including third party beneficial owners, and to verify the identity of all owners, with personal interviews if necessary. The regulation also requires banks to

establish special monitoring units and appoint compliance officers responsible for implementation of the new rules and to maintain adequate information systems to comply with the law. Finally, the regulation requires banks to analyze and monitor customer transactions and report to BI within seven days any "suspicious transactions" in excess of Rp 100 million (approximately $11,000). The regulation defines suspicious transactions according to a 39-point matrix that includes key indicators such as unusual cash transactions, unusual ownership patterns, or unexplained changes in transactional behavior. BI specifically requires banks to treat as suspicious any transactions to or from countries "connected with the production, processing and/or market for drugs or terrorism."

BI has issued an Internal Circular Letter No. 6/50/INTERN, dated September 10, 2004 concerning Guidelines for the Supervision and Examination of the Implementation of KYC and AML by Commercial Banks. In addition, BI also issued a Circular Letter to Commercial Banks No. 6/37/DPNP dated September 10, 2004 concerning the Assessment and Imposition of Sanctions on the Implementation of KYC and other Obligations Related to Law on Money Laundering Crimes. BI is also preparing Guidelines for Money Changers on Record Keeping and Reporting Procedures, and Money Changer Examinations to be given by BI examiners.

Currently, banks must report all foreign exchange transactions and foreign obligations to BI. With respect to the physical movement of currency, Article 16 of Law No. 15/2002 contains a reporting requirement for any person taking cash into or out of Indonesia in the amount of 100 million Rupiah (approximately $11,000) or more, or the equivalent in another currency, which must be reported to the Director General of Customs and Excise. These reports must be given to the PPATK in no later than five business days and contain details of the identity of the person. Indonesian Central Bank regulation 3/18/PBI/2001 and the Directorate General of Customs and Excise Decree No.01/BC/2005 contain the requirements and procedures of inspection, prohibition, deposit of Indonesia Rupiah into or out of Indonesia. The Decree provides implementing guidance for Ministry of Finance Regulation No.624/PMK.04/2004 of December 31, 2004, and requires individuals who import or export more than rupiah 50 to 100 million in cash (approximately $5,500-$11,000) to report such transactions to Customs. This information is to be declared on the Indonesian Customs Declaration (BC2.2). As of October 2006, the PPATK has received more than 1,200 reports from Customs on cross border cash carrying issues. The reports came from five entry points as follows: Batam Port, Jakarta's Soekarno Hatta Airport, Tanjung Balai Karimun Port, Ngurah Rai Bali Airport, and Husein Sastranegara Bandung Airport.

Indonesia's bank secrecy law covers information on bank depositors and their accounts. Such information is generally kept confidential and can only be accessed by the authorities in limited circumstances. However, Article 27(4) of the Law No. 15/2002 now expressly exempts the PPATK from "the provisions of other laws related to bank secrecy and the secrecy of other financial transactions" in relation to its functions in receiving and requesting reports and conducting audits of providers of financial services. In addition, Article 14 of the Law No. 15/2002 exempts providers of financial services from bank secrecy provisions when carrying out their reporting obligations. Article 15 of the anti-money laundering legislation gives providers of financial services, their officials, and employees protection from civil or criminal action in making such disclosures.

Indonesia's laws provide only limited authority to block or seize assets. Under BI regulation 2/19/PBI/2000, police, prosecutors, or judges may order the seizure of assets of individuals or entities that have been either declared suspects or indicted for a crime. This does not require the permission of BI, but, in practice, for law enforcement agencies to identify such assets held in Indonesian banks, BI's permission is sought. In cases when money laundering is the alleged crime, however, bank secrecy laws would not apply, according to the anti-money laundering law.

The GOI has the authority to trace and freeze assets of individuals or entities on the UNSCR 1267 Sanctions Committee's consolidated list, and through BI, has circulated the consolidated list to all

banks operating in Indonesia, with instructions to freeze any such accounts. The interagency process to issue freeze orders, which includes the Foreign Ministry, Attorney General, Police, and BI, takes several weeks or more from UN designation to bank notification. The implementation of this process has not led to the discovery of accounts or assets of individuals or entities on the UN 1267 consolidated list. However, during the course of terrorism investigations, the Indonesia police have located and frozen accounts of individuals on the UN 1267 consolidated list.

In August, 2006, the GOI enacted Indonesia's first Witness and Victim Protection Law (No. 13/2006). Indonesia's AML Law and Government Implementing Regulation No. 57/2003 also provides protection to whistleblowers and witnesses.

In October 2006, the GOI submitted to Parliament additional amendments to Law No. 15/2002 that would provide the PPATK with preliminary investigative authority and the ability to temporarily freeze assets. The amendments are intended to provide technical investigative support to police and prosecutors and to deter capital flight.

The October 18, 2002 emergency counterterrorism regulation, the Government Regulation in Lieu of Law of the Republic of Indonesia (Perpu), No. 1 of 2002 on Eradication of Terrorism, criminalizes terrorism and provides the legal basis for the GOI to act against terrorists, including the tracking and freezing of assets. The Perpu provides a minimum of three years and a maximum of 15 years imprisonment for anyone who is convicted of intentionally providing or collecting funds that are knowingly used in part or in whole for acts of terrorism. This regulation is necessary because Indonesia's anti-money laundering law criminalizes the laundering of "proceeds" of crimes, but it is often unclear to what extent terrorism generates proceeds. In October 2004, an Indonesian court convicted and sentenced one Indonesian to four years in prison on terrorism charges connected to his role in the financing of the August 2003 bombing of the Jakarta Marriott Hotel.

The GOI has just begun to take into account alternative remittance systems, such as charitable and nonprofit entities in its strategy to combat terrorist finance and money laundering. The PPATK has issued guidelines for nonbank financial service providers and money remittance agents on the prevention and eradication of money laundering and the identification and reporting of suspicious and other cash transactions. The GOI has initiated a dialogue with charities and nonprofit entities to enhance regulation and oversight of those sectors.

Indonesia is an active member of the Asia/Pacific Group on Money Laundering (APG) and the Bank for International Settlements. BI claims that it voluntarily follows the Basel Committee's "Core Principles for Effective Banking Supervision." The GOI is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. In June, 2006, Indonesia became a party to the UN International Convention for the Suppression of the Financing of Terrorism.

In June 2004, the PPATK became a member of the Egmont Group and, as such, is committed to the Group's established Principles governing the exchange of financial intelligence with other members. The PPATK is actively pursuing broader cooperation through the MOU process with approximately twenty other FIUs. The PPATK has also entered into an Exchange of Letters enabling international exchange with Hong Kong. Indonesia has signed Mutual Legal Assistance Treaties with Australia, China and South Korea, and Indonesia joined other ASEAN nations in signing the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters on November 29, 2004. The Indonesian Regional Law Enforcement Cooperation Centre was formally opened in 2005 and was created to develop the operational law enforcement capacity needed to fight transnational crimes.

The highest levels of GOI leadership should continue to demonstrate strong support for strengthening Indonesia's anti-money laundering regime. In particular, the GOI must continue to improve capacity and interagency cooperation in analyzing suspicious and cash transactions, investigating and

prosecuting cases, and achieving deterrent levels of convictions and custodial and administrative sentences and penalties. As part of this effort, Indonesia should review the adequacy of its Code for Criminal Procedure and Rules of Evidence and enact legislation to allow the use of modern techniques to enter evidence in court proceedings. Indonesia should reassess and streamline its processes for reviewing UN designations and for identifying, freezing and seizing terrorist assets. The GOI should expand its list of predicate crimes for money laundering. Indonesia should also become a party to the UN Convention against Transnational Organized Crime.

## Iran

Iran is not a regional financial center. Iran's economy is marked by an inefficient state sector, over-reliance on the petroleum industry—Iran's huge oil and gas reserves produce 60 percent of government revenue—and state-centered policies that cause major distortions in the economy. Reportedly, a prominent Iranian banking official estimates that money laundering encompasses an estimated 20 percent of Iran's economy. There are other reports that over $11 billion a year is laundered via smuggling commodities in Iran and over $6 billion is laundered by international criminal networks. The World Bank reports that about 19 percent of Iran's GDP pertains to unofficial economic activities. Money laundering in Iran encompasses narcotics trafficking, smuggling, trade fraud, counterfeit merchandise and intellectual property rights violations, cigarette smuggling, trafficking in persons, hawala, capital flight, and tax evasion.

After the Iranian Revolution of 1979, the Government of Iran (GOI) nationalized the country's banks, leaving a total of six banks: Bank Refah, Bank Melli Iran, Bank Saderat, Bank Tejarat, Bank Mellat and Bank Sepah, and three specialized institutions, Bank Keshavrzi, Bank Maskan and Bank Sanat va Madden. No foreign banks were allowed to operate in the country. Since 1983, consistent with Islamic law, banks have been prohibited from paying interest on deposits or charging interest on loans. However, alternative financial instruments were developed including profit-sharing and financing based on trade. In 1994, Iran authorized the creation of private credit institutions. Licenses for these banks were first granted in 2001. Currently, these banks include Larafarinan, Parsian, Saman Eghtesad and Eghtesade Novin. Standard Chartered Bank became the first foreign bank to be awarded a license to establish a branch in Iran, although this was limited to Kish, a free-zone island. Currently, some 40 international banks have representative offices in Iran, which may undertake lending but not accept deposits.

There are currently no meaningful anti-money laundering (AML) controls on the Iranian banking system. The Central Bank of Iran (CBI) has issued AML circulars that address suspicious activity reporting and other procedures that demonstrate an awareness of international standards, but there is a lack of implementation. In 2003, the Majlis (Parliament) reportedly passed an anti-money laundering act. The act includes customer identification requirements, mandatory record keeping for five years after the opening of accounts, and the reporting of suspicious activities. However, the act has not been implemented due to reported pressure by vested interests within the government.

Iran has reported to the United Nations that it has established a financial intelligence unit (FIU). However, Iran has not provided any documentation or details on the FIU.

The U.S. Department of State has designated Iran as a State Sponsor of Terrorism. On September 8, 2006 the U.S. Treasury Department issued a regulation prohibiting U.S. financial institutions from handling any assets, directly or indirectly, relating to Iran's Bank Saderat, based on evidence of its involvement in transferring funds to terrorist groups. Bank Saderat is one of Iran's largest with approximately 3,400 branches.

On January 9, 2007, the U.S. Treasury Department imposed sanctions against Bank Sepah, a state-owned Iranian financial institution for providing support and services to designated Iranian

proliferation firms, particularly Iran's missile procurement network. Bank Sepah is the fifth largest Iranian state-owned bank with more than 290 domestic branches as well as international branches in Europe.

Iran has a very large underground economy, which is spurred by restrictive taxation, widespread smuggling, currency exchange controls, capital flight, and a large Iranian expatriate community. Anyone engaging in transfers or transactions of foreign currency into or out of Iran must abide by CBI regulations, including registration and licensing. Those who do not are subject to temporary or permanent closure. The regulations and circulars address money transfer businesses, including hawaladars. However, underground hawala and moneylenders in the bazaar are active in Iran. Since there is an absence of an adequate banking system and working capital, the popular informal system meets the need for currency exchange and money lending. Many hawaladars and traditional bazaari are linked directly to the regional hawala hub in Dubai. Countervaluation in hawala transactions is often accomplished via trade. The trade and smuggling of goods into Iranian commerce leads to a significant amount of trade-based money laundering and value transfer.

Iran's real estate market is often used to launder money. Often times, real estate settlements and payment are made overseas. In addition, there are reports that a massive amount of Iranian capital has been invested in the United Arab Emirates, particularly in Dubai real estate.

Via a transit trade agreement, goods purchased primarily in Dubai are sent to ports in southern Iran and then via land routes to markets in Afghanistan. There are reports that the transit trade facilitates the laundering of Afghan narcotics proceeds. According to the United Nations Office on Drugs and Crime, approximately 60 percent of Afghanistan's opium is trafficked across Iran's border. Reportedly, Iran has an estimated 3 million drug users and the worst heroin addiction rate in the world. Opiates not intended for the Iranian domestic market transit Iran to Turkey, where the morphine base is converted to heroin. Heroin and hashish are delivered to buyers located in Turkey. The drugs are then shipped to the international market, primarily Europe. In Iran and elsewhere in the region, proceeds from narcotics sales are sometimes exchanged for trade goods via value transfer.

Iran's "bonyads," or charitable religious foundations, were originally established at the time of the Iranian revolution to help the poor. They have rapidly expanded beyond their original mandate. Although still funded, in part, by Islamic charitable contributions, today's bonyads monopolize Iranian import-export concerns and major industries including petroleum, automobiles, hotels, and banks. Bonyad conglomerates account for a substantial percentage of Iran's gross national product. Individual bonyads such as Imman Reza Foundation and the Martyrs' Foundation have billions of dollars in assets. Mullahs direct the bonyad foundations. Given the low rate of capital accumulation in the Iranian economy, the foundations constitute one of the few governmental institutions for internal economic investment. Reportedly, the bonyads stifle entrepreneurs not affiliated with them due to the bonyads' favored status, which includes exemption from taxes, the granting of favorable exchange rates, and lack of accounting oversight by the Iranian government. Corruption is widespread throughout Iranian society; at the highest levels of government, favored individuals and families benefit from "baksheesh" deals. Iran is ranked 106 out of 163 countries listed in Transparency International's 2006 Corruption Perception Index. Despite some limited attempts at reforming bonyads, there has been little transparency or substantive progress. Bonyads have been involved in funding terrorist organizations and serving as fronts for the procurement of nuclear capacity and prohibited weapons and technology.

Iran is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Iran has signed but not ratified the UN Convention Against Corruption. It has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Iran should construct and implement a viable anti-money laundering and terrorist finance regime that adheres to international standards. Iran should be more active in countering regional smuggling. Iran should implement meaningful reforms in bonyads that promote transparency and accountability. Iran should create an anti-corruption law with strict penalties and enforcement, applying it equally to figures with close ties to the government and the clerical communities. It should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Iran should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism. Iran should not support terrorism or the funding of terrorism.

## Iraq

Iraq's economy is cash-based. There is little data available on the extent of money laundering in Iraq. However, cross-border smuggling is widespread, including the smuggling of bulk cash. Iraq is a major market for smuggled cigarettes and counterfeit goods, and money is laundered from intellectual property right violations. There is a large market for stolen cars from Europe and the United States. Ransoms generated from kidnapping generate tens of millions of dollars every year. Kidnappings are linked to human exploitation and terrorist finance. Iraq is a source country for human trafficking. Trade-based money laundering, customs fraud, and value transfer are found in the underground economy and are commonly used in informal value transfer systems such as hawala. Hawala networks are prevalent and are widely used in Iraq and the region. Cash, trade-based money laundering, and hawala are all components of terrorist and insurgent finance found in Iraq. In early 2006, the Iraqi oil ministry estimated that ten percent of the $4 billion to $5 billion in fuel imported for public consumption at subsidized rates in 2005 was smuggled internally and out of the country for resale at market rates. Moreover, there are reports that approximately ten percent of all oil smuggling profits are going to insurgents. Subsidy scams and black market sales also exist for gasoline, kerosene, and cooking fuel. Corruption is a severe problem that permeates society and commerce and is also found at the highest levels of government and other institutions. Transparency International's 2006 International Corruption Perception Index listed Iraq 161 out of 163 countries surveyed. The formal financial sector is growing and at least ten new banks, both domestic and international, have been licensed to operate in Iraq. The two state-owned banks control at least 90 percent of the banking sector.

The Coalition Provisional Authority (CPA), the international body that governed Iraq beginning in April 2003, issued regulations and orders that carried the weight of law in Iraq. The CPA ceased to exist in June 2004, at which time the Iraqi Interim Government assumed authority for governing Iraq. Drafted and agreed to by Iraqi leaders, the Transitional Administrative Law (TAL) described the powers of the Iraqi government during the transition period. Under TAL Article 26, regulations and orders issued by the CPA pursuant to its authority under international law remain in force until rescinded or amended by legislation duly enacted and having the force of law. The constitution, which was ratified in October 2005, also provides for the continuation of existing laws, including CPA regulations and orders that govern money laundering.

The CPA Order No. 93, "Anti-Money Laundering Act of 2004" (AMLA) governs financial institutions in connection with: money laundering, financing of crime, financing terrorism, and the vigilance required of financial institutions in regard to financial transactions. The law also criminalizes money laundering, financing crime (including the financing of terrorism), and structuring transactions to avoid legal requirements. The AMLA covers: banks; investment funds; securities dealers; insurance entities; money transmitters and foreign currency exchange dealers, as well as persons who deal in financial instruments, precious metals or gems; and persons who undertake hawala transactions. Covered entities are required to verify the identity of any customer opening an account for any amount. Covered entities are also required to verify the identity of non-account holders performing a transaction or series of potentially related transactions whose value is equal to or greater than five

million Iraqi dinars (approximately $3,500). Beneficial owners must be identified upon account opening or for transactions exceeding ten million Iraqi dinar (approximately $7,000). Records must be maintained for at least five years. Covered entities must report suspicious transactions and wait for guidance before proceeding with the transaction; the relevant funds are frozen until guidance is received. Suspicious transaction reports (STRs) are to be completed for any transaction over four million Iraqi dinar (approximately $3,000) that is believed to involve funds that are derived from illegal activities or money laundering, intended for the financing of crime, (including terrorism), or over which a criminal organization has disposal power, or a transaction conducted to evade any law and which has no apparent business or other lawful purpose. The "tipping off" of customers by bank employees where a transaction has generated a suspicious transaction report is prohibited. Bank employees are protected from liability for cooperating with the government. Willful violations of the reporting requirement may result in imprisonment or fines.

CPA Order No. 94, "Banking Law of 2004," gives the Central Bank of Iraq (CBI) the authority to license banks and to conduct due diligence on proposed bank management. Order No. 94 establishes requirements for bank capital, confidentiality of records, audit and reporting requirements for banks, and prudential standards. The CBI is responsible for the supervision of financial institutions. The CBI was mandated by the AMLA to issue regulations and require financial institutions to provide employee training, appoint compliance officers, develop internal procedures and controls to deter money laundering, and establish an independent audit function. The AMLA provides that the CBI will issue guidelines on suspicious financial activities and conduct on-site examinations to determine institutions' compliance. The CBI also may issue regulations to require large currency transaction reports for the cross-border transport of currency of more than 15 million Iraqi dinars (approximately $10,000). Neither Iraqis nor foreigners are permitted to transport more than $10,000 in currency when exiting Iraq. The CBI is also mandated by the AMLA to distribute the UN 1267 Sanction Committee's consolidated list of suspected terrorists or terrorist organizations. No asset freezes pertaining to any names on the consolidated list have been reported to date. Order No. 94 gives administrative enforcement authority to the CBI, up to and including the removal of institution management and revocation of bank licenses.

The AMLA calls for the establishment of the Money Laundering Reporting Office (MLRO) within the CBI. The MLRO was recently formed in June/July 2006 and has a small but dedicated staff. The CBI and representatives from the United States are working together to build the MLRO's capacity and implement the day-to-day functions of a financial intelligence unit (FIU). The MLRO will operate independently to collect, analyze and disseminate information on financial transactions subject to financial monitoring and reporting, including suspicious activity reports. The MLRO is also empowered to exchange information with other Iraqi or foreign government agencies. The CBI and its MLRO finalized implementing regulations to the AMLA, which became effective September 15, 2006.

The predicate offenses for the crimes of money laundering and the financing of crime are quite broad and extend beyond "all serious offenses" to include "some form of unlawful activity." The penalties for violating the AMLA depend on the specific nature of the underlying criminal activity. For example, "money laundering" is punishable by a fine of up to 40 million dinar (approximately $27,080), or twice the value of the property involved in the transaction (whichever is greater), or imprisonment of up to four years, or both. Other offenses for which there are specific penalties include the financing of crime (a fine of up to 20 million dinar (approximately $13,540), two years' imprisonment, or both) and structuring transactions (up to 10 million dinar (approximately $6,770), one year imprisonment, or both). No arrests or prosecutions under the AMLA have been reported to date.

The AMLA includes provisions for the forfeiture of any property Such property includes, but is not limited to, funds involved in a covered offense, or any property traceable to the property, or any

property gained as a result of such an offense, without prejudicing the rights of bona fide third parties. The AMLA also blocks any funds or assets, other than real property (which is covered by a separate regulation), belonging to members of the former Iraqi regime and authorizes the Minister of Finance to confiscate such assets following a judicial or administrative order. The lack of automation or infrastructure in the banking sector, however, hinders the government's ability to identify and freeze assets linked to illicit activity.

Iraq has free trade zones in Basra/Khor al-Zubair, Ninewa/Falafel, Sulaymaniyah, and Al-Quaymen. Under the Free Zone (FZ) Authority Law, goods imported and exported from the FZ are generally exempt from all taxes and duties, unless the goods are imported into Iraq. Additionally, capital, profits, and investment income from projects in the FZ are exempt from taxes and fees throughout the life of the project, including in the foundation and construction phases.

Iraq became a member of the Middle East and North Africa Financial Action Task Force (MENAFATF) in September 2005. Iraq is a party to the 1988 UN Drug Convention, but not the UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Transnational Organized Crime.

In 2006, in a challenging environment, the Government of Iraq continued to lay the foundation for anti-money laundering and counterterrorist finance regimes. In these efforts, there was strong cooperation with the U.S. Government. However, there is much work ahead. Iraq should become a party to the UN Conventions for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. It should take a more active part in MENAFATF and implement its recommendations. Iraq should continue its efforts to build capacity and actively implement the provisions of the AMLA and related authorities. As a priority, as Iraq's MLRO becomes fully functional, it should develop increased capacity to investigate financial crimes and enforce the provisions of the AMLA. Iraqi law enforcement, border authorities, and customs service should strengthen border enforcement and identify and pursue smuggling and trade-based money laundering networks. Increased border enforcement is also a prerequisite in combating terrorist finance. Iraq should also take concerted steps to combat corruption.

## Ireland

Ireland is an increasingly significant European financial hub, with the international banking and financial services sector concentrated in Dublin's International Financial Services Centre (IFSC). Narcotics trafficking, fraud, and tax offenses are the primary sources of funds laundered in Ireland. Money laundering occurs in credit institutions, although launderers have also made use of money remittance companies, solicitors, accountants, and second-hand car dealerships. The most common laundering methods are: the purchase of high-value goods for cash; the use of credit institutions to receive and transfer funds in and out of Ireland; the use of complex company structures to filter funds; and the purchase of properties in Ireland and abroad.

The Shannon Free Zone was established in 1960 as a free trade zone, offering investment incentives for multinational companies. The Shannon Free Zone is supervised by "Shannon Development," a government-founded body. Reportedly, there are no indications that the Shannon Free Zone is being used in trade-based money laundering schemes or by financiers of terrorism.

The international banking and financial services sector concentrated in Dublin's International Financial Services Centre (IFSC). In 2006, there were approximately 430 international financial institutions and companies operating in the IFSC. Services offered include banking, fiscal management, re-insurance, fund administration, and foreign exchange dealing. The use of offshore bank accounts, the creation of shell corporations and trusts, all of which obfuscate the true beneficial owner are additional sources of money laundering that represent significant vulnerabilities common to

jurisdictions that offer offshore financial services. Casinos, including internet casinos, are illegal in Ireland. Private gaming clubs, however, operate casino-like facilities that fall outside the scope of the law.

Ireland criminalized money laundering relating to narcotics trafficking and all indictable offenses under the 1994 Criminal Justice Act. Financial institutions (banks, building societies, the Post Office, stockbrokers, credit unions, bureaux de change, life insurance companies, and insurance brokers) are required to report suspicious transactions. There is no monetary threshold for reporting suspicious transactions. Designated entities submit suspicious transaction reports (STRs) to the Garda (Irish Police) Bureau of Fraud Investigation, Ireland's Financial Intelligence Unit (FIU). In 2003, a new legal requirement went into effect, mandating that covered institutions file STRs with the Revenue (Tax) Department in addition to the FIU.

Financial institutions are required to implement customer identification procedures and retain records of financial transactions. In 2003, Ireland amended its Anti-Money Laundering law to extend the requirements of customer identification and suspicious transaction reporting to lawyers, accountants, auditors, real estate agents, auctioneers, and dealers in high-value goods, thus aligning its laws with the Second European Union (EU) Money Laundering Directive. Ireland's Customer Due Diligence requires designated entities to take measures to identify customers when opening new accounts or conducting transactions exceeding 13,000 euros (approximately $17,000). These requirements do not extend to existing customers prior to May 1995 except in cases where authorities suspect that money laundering or another financial crime is involved.

The Corporate Law, amended in 1999, requires that every company applying for registration in Ireland must demonstrate that it intends to carry on an activity in the country. Companies must maintain an Irish resident director at all times, or post a bond as a surety for failure to comply with the appropriate company law. In addition, the law limits the number of directorships that any one person can hold to 25, with certain exemptions. This limitation aims to curb the use of nominee directors as a means of disguising beneficial ownership or control.

The Company Law Enforcement Act 2001 (Company Act) established the Office of the Director of Corporate Enforcement (ODCE). The ODCE investigates and enforces provisions of the Company Act. Under the law, directors of a company must be named, and the ODCE has power to establish the company's beneficial ownership and control. The Company Act also creates a mandatory reporting obligation for auditors to report suspicions of breaches of company law to the ODCE. In 2005, the ODCE secured the conviction of 30 company directors and other individuals on 49 charges for breaching various requirements of the Company Act. In addition, 21 company officers were disqualified from eligibility for a lead position in companies for periods ranging from one to 10 years.

The Third EU Money Laundering Directive entered into force in December 2005 and must be transposed into Irish law by December 2007. The Government of Ireland (GOI) is likely to implement new legislation to address customer due diligence, the identification of beneficial owners, politically exposed persons, and the designation of trusts.

A Mutual Evaluation conducted in 2005 by the Financial Action Task Force (FATF) which was published in 2006 noted that Ireland's money laundering definition met the FATF requirements. The mutual evaluation report (MER) acknowledged that Ireland achieved a high standing in anti-money laundering legal structures and international cooperation, although the number of money laundering prosecutions and convictions was low.

The Irish Financial Services Regulatory Authority (IFSRA), the financial regulator, is a component of the Central Bank and Financial Services Authority of Ireland (CBFSAI) and is responsible for supervising the financial institutions for compliance with money laundering procedures. IFSRA is obliged to report to the FIU and the Revenue Commissioners regarding any suspected breaches of the

Criminal Justice Act 1994 by the institutions under its supervision. Such reports cover suspicion of money laundering and terrorism financing, failure to establish identity of customers, failure to retain evidence of identification, and failure to adopt measures to prevent and detect the commission of a money laundering offense. IFSRA regulates the IFSC companies that conduct banking, insurance, and fund transactions. Tax privileges for IFSC companies were phased out over recent years and expired in 2005.

Ireland currently has no legislative requirement to report cross-border transportation of currency or bearer-negotiable instruments, although reportedly the government is likely to introduce customs reporting requirements in 2007 for those transporting more than euro 10,000 (approximately $12,900) into or out of the EU. In addition, movements of gold, precious metals, and precious stones into or out of the EU when Ireland is the initial entry or final exit point must be reported to Irish Customs. The FIU will have access to these reports.

Ireland estimates that up to 80 percent of STRs may involve tax violations. Value Added Tax (VAT) Intra-Community Missing Trader Fraud is extensive within the EU, and there is evidence in several fraud investigations that conduit traders involved in the supply chain have been established in Ireland. This particular fraud is a systematic criminal attack on the VAT system, detected in many EU countries, in which criminals obtain VAT registration to acquire goods VAT free from other Member States. They then sell on the goods at VAT inclusive prices and disappear without remitting the VAT paid by their customers to the tax authorities.

Ireland's FIU analyzes financial disclosures, and disseminates them for investigation. There are no legal provisions, however, governing the time period within which an STR must be filed; rather, the requirement is to submit the STR before a suspicious transaction is finalized. The MER found that Ireland's FIU, as a whole, met the requirements of the FATF methodology, but had limited technical and human resources to manage and evaluate STRs effectively.

In 2005, the FIU received 10,735 STRs, in comparison with 5,491 in 2004 and 4, 254 in 2003. 2005 saw eight prosecutions for money laundering and three convictions. In 2006, three people were convicted for money laundering. A conviction on charges of money laundering carries a maximum penalty of 14 years' imprisonment and an unlimited fine. The lengthiest penalty applied for a money laundering conviction to date has been six years. Under certain circumstances, the High Court can freeze, and, where appropriate, seize the proceeds of crimes.

The Criminal Assets Bureau (CAB) was established in 1996 to confiscate the proceeds of crime in cases where there is no criminal conviction. The CAB reports to the Minister for Justice and includes experts from the Garda, Tax, Customs, and Social Security Agencies. Under the 1996 Proceeds of Crime Act, specified property valued in excess of 13,000 euro (approximately $17,000) may be frozen for seven years, unless the court is satisfied that all or part of the property is not criminal proceeds. In February 2005, the Proceeds of Crime (Amendment) Act 2005 came into effect, enabling the authorities, with the consent of the High Court and the parties concerned, to dispose of assets without having to await the expiry of seven years. To date, the authorities have executed five such consent orders. This Act also allows foreign criminality to be taken into account in assessing whether assets are the proceeds of criminal conduct. In 2005, the CAB obtained final and interim restraint orders on assets valued at approximately $76 million. The Proceeds of Crime (Amendment) Act 2005 has a specific provision that allows the CAB to cooperate with agencies in other jurisdictions, which should strengthen Irish cooperation with asset recovery agencies in the UK, including Northern Ireland.

In March 2005, the Irish government enhanced its capacity to address international terrorism with the enactment of the Criminal Justice (Terrorism Offenses) Act. This legislation brought Ireland in line with United Nations Conventions and European Union Framework decisions on combating terrorism. In addition, the IFSRA works with the Department of Finance to draft guidance for regulated institutions on combating and preventing terrorist financing. The authorities revised and issued the

guidance to institutions upon the passage of the Criminal Justice Act in 2005. Implementation of the new antiterrorism legislation and its anti-money laundering law amendments, in addition to stringent enforcement of all such initiatives, should enhance Ireland's efforts to maintain an effective anti-money laundering program.

To date, there have been no prosecutions for terrorism offenses under the Criminal Justice Act. The 2006 FATF MER noted that the Act neglects to cover funding of either a terrorist acting alone or two terrorists acting in concert. The MER also noted inadequate implementation of UN Security Council Resolution (UNSCR) 1373, in that Ireland relies exclusively on an EU listing system without subsidiary mechanisms to deal with terrorists on the list who are European citizens (the EU Regulations do not apply for freezing purposes to such persons) or with persons designated as terrorists by other jurisdictions who are not on the EU list. The Criminal Justice (Terrorism Offenses) Act imposes evidentiary requirements contrary to obligations under UNSCR 1373 to freeze all funds and assets of individuals who commit terrorist acts, whether or not there is evidence that those particular funds are intended for use in terrorist acts.

The Garda can apply to the courts to freeze assets when certain evidentiary requirements are met. From 2001 through 2006, Ireland had reported to the European Commission the names of five individuals (most recently in 2004) who maintained a total of seven accounts that were frozen in accordance with the provisions of the European Union's (EU) Anti-Terrorist Legislation. The aggregate value of the funds frozen was approximately $6,400.

In July 2005, the United States and Ireland signed instruments on extradition and mutual legal assistance. These instruments are part of a sequence of bilateral agreements that the United States is concluding with all 25 EU Member States, in order to implement twin agreements on extradition and mutual legal assistance with the European Union that were concluded in 2003. The instruments signed by Ireland supplement and update the 1983 U.S.-Ireland extradition treaty and the 2001 bilateral treaty on mutual legal assistance (MLAT). The 1983 extradition treaty between Ireland and the U.S. is in force, while the ratification process for the 2001 MLAT has not yet been completed by the GOI. In November 2006, Ireland extradited a U.S. citizen, the first successful case in the last eighteen requests. The new MLAT instrument signed in July 2005 provides for searches of suspect foreign located bank accounts, joint investigative teams, and testimony by video-link.

Ireland is a member of the FATF, and its FIU is a member of the Egmont Group. Ireland is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the 1988 UN Drug Convention.

The GOI should enact legislation to disallow the establishment of "shell" companies. Law enforcement should have a stronger role in identifying the true beneficial owners of shell companies as well as of trusts in the course of investigations. Ireland should increase the technical and human resources provided to the FIU in order to manage and evaluate STRs effectively. The GOI should enact legislation that covers funding of a terrorist acting alone and funding of two terrorists acting in concert, as well as legislation fully implementing UNSCR 1373. To this end, Ireland should remove the evidentiary requirements acting as obstacles to full compliance, as well as circulate the UN and the U.S. lists to its regulators and obligated entities.

## Isle of Man

The Isle of Man (IOM) is a Crown Dependency of the United Kingdom located between England and Ireland in the Irish Sea. Its large and sophisticated financial center is potentially vulnerable to money laundering. The U.S. dollar is the most common currency used for criminal activity in the IOM. Most of the illicit funds in the IOM are from fraud schemes and narcotics trafficking in other jurisdictions,

including the United Kingdom. Identity theft and Internet abuse are growing segments of financial crime activity.

Money laundering related to narcotics trafficking was criminalized in 1987. The Prevention of Terrorism Act 1990 made it an offense to contribute to terrorist organizations, or to assist a terrorist organization in the retention or control of terrorist funds. In 1998, money laundering arising from all serious crimes was criminalized. Financial institutions and professionals such as banks, fund managers, stockbrokers, insurance companies, investment businesses, credit unions, bureaux de change, check cashing facilities, money transmission services, real estate agents, auditors, casinos, accountants, lawyers, and trustees are required to report suspicious transactions and comply with the requirements of the anti-money laundering (AML) code, such as customer identification.

The Financial Supervision Commission (FSC) and the Insurance and Pension Authority (IPA) regulate the IOM financial sector. The FSC is responsible for the licensing, authorization, and supervision of banks, building societies, investment businesses, collective investment schemes, corporate service providers, and companies. The IPA regulates insurance companies, insurance management companies, general insurance intermediaries, and retirement benefit schemes and their administrators. In addition, the FSC also maintains the Company Registry Database for the IOM, which contains company records dating back to the first company incorporated in 1865. Statutory documents filed by IOM companies can now be searched and purchased online through the FSC's website.

Instances of failure to disclose suspicious activity would result in both a report being made to the Financial Crimes Unit (FCU), the IOM's financial intelligence unit (FIU), and possible punitive action by the regulator, which could include revoking the business license. To assist license holders in the effective implementation of anti-money laundering techniques, the regulators hold regular seminars and additional workshop training sessions in partnership with the FCU and the Isle of Man Customs and Excise.

In December 2000, the FSC issued a consultation paper, jointly with the Crown Dependencies of Guernsey and Jersey, called Overriding Principles for a Revised Know Your Customer Framework, to develop a more coordinated approach on anti-money laundering. Further work between the Crown Dependencies is being undertaken to develop a coordinated strategy on money laundering, to ensure compliance as far as possible with the revised Financial Action Task Force (FATF) Forty Recommendations on Money Laundering. The IOM is also assisting the FATF Working Groups considering matters relating to customer identification and companies' issues.

In August 2002, money service businesses (MSBs) not already regulated by the FSC or IPA were required to register with Customs and Excise. This implemented the 1991 EU Directive on Money Laundering, revised by the Second Directive 2001/97/EC, for MSBs and provides for their supervision by Customs and Excise to ensure compliance with the AML Codes.

The IPA, as regulator of the IOM's insurance and pensions business, issues Anti-Money Laundering Standards for Insurance Businesses (the "Standards"). The Standards are binding upon the industry and include the Overriding Principles. These include a requirement that all insurance businesses check their whole book of businesses to determine that they have sufficient information available to prove customer identity. The current set of Standards became effective March 31, 2003. In addition, the IPA conducts on-site visits to examine procedures and policies of companies under its supervision.

The Online Gambling Regulation Act 2001 and an accompanying AML (Online Gambling) Code 2002 are supplemented by AML guidance notes issued by the Gambling Control Commission, a regulatory body which provides more detailed guidance on the prevention of money laundering through the use of online gambling. The Online Gambling legislation brought regulation to what was technically an unregulated gaming environment. The dedicated Online Gambling AML Code was at the time unique within this segment of the gambling industry.

The Companies, Etc. (Amendment) Act 2003 calls for additional supervision for all licensable businesses, e.g., banking, investment, insurance and corporate service providers. The act further provides that no future bearer shares will be issued after April 1, 2004, and all existing bearer shares must be registered before any rights relating to such shares can be exercised.

The FCU, formed in April 2000, evolved from the police Fraud Squad and now includes both police and customs staff. It is the central point for the collection, analysis, investigation, and dissemination of suspicious transaction reports (STRs) from obligated entities. The entities required to report suspicious transactions include banks/financial institutions, bureaux de change, casinos, post offices, lawyers, accountants, advocates, and businesses involved with investments, real estate, gaming/lotteries, and insurance. In 2006, the FIU received approximately 1,625 suspicious transaction reports (STRs); in 2005 the FIU received 2,265 STRs and in 2004 it received 2,315 STRs. In 2006, the FIU referred approximately 16 percent of the STRs to the United Kingdom, 10 percent to other European jurisdictions and 15 percent to non-European jurisdictions as referrals to law enforcement for investigation. The Isle of Man's International Co-operation team responded to 70 letters of request (from January to November 2006), under Mutual Legal Assistance Treaties (MLATs). The International Co-operation team responded to 103 requests for information in 2005 and 115 requests in 2004. There is no minimum threshold for obligated entities to file a STR and reporting individuals (compliance officers, bankers, etc.) are protected by law when filing suspicious transactions.

The FCU is organized under the Department of Home Affairs. The FIU has access to Customs, police and tax information. The STRs are disseminated through agreements to the IOM Customs, Tax Administrators, Financial Supervision Commission (FSC) and the Insurance and Pension Authority (IPA). The FCU is responsible for investigating financial crimes and terrorist financing cases. In 2006, there were two individuals charged for money laundering offences involving narcotics. The FCU also has three additional investigations on-going relating to money laundering offences involving fraud.

The Criminal Justice Acts of 1990 and 1991, as amended, extend the power to freeze and confiscate assets to a wider range of crimes, increase the penalties for a breach of money laundering codes, and repeal the requirement for the Attorney General's consent prior to disclosure of certain information. Assistance by way of restraint and confiscation of assets of a defendant is available under the 1990 Act to all countries and territories designated by Order under the Act, and the availability of such assistance is not convention-based nor does it require reciprocity. Assistance is also available under the 1991 Act to all countries and territories in the form of the provision of evidence for the purposes of criminal investigations and proceedings.

Under the 1990 Act the provision of documents and information is available to all countries and territories for the purposes of investigations into serious or complex fraud. Similar assistance is also available to all countries and territories in relation to drug trafficking and terrorist investigations. All decisions for assistance are made by the Attorney General of the IOM on a case-by-case basis, depending on the circumstances of the inquiry. The law also addresses the disclosure of a suspicion of money laundering. Since June 2001, it has been an offense to fail to make a disclosure of suspicion of money laundering for all predicate crimes, whereas previously this just applied to drug- and terrorism-related crimes. The law also lowers the standard for seizing cash from "reasonable grounds" to believe that it was related to drug or terrorism crimes to a "suspicion" of any criminal conduct. The law also provides powers to constables, including customs officers, to investigate whether a person has benefited from any criminal conduct. These powers allow information to be obtained about that person's financial affairs. These powers can be used to assist in criminal investigations abroad as well as in the IOM.

The United Kingdom implemented the amendments to its Proceeds of Crime Act in 2004. The IOM is currently reviewing new legislation that will revise its Criminal Justice Act along similar lines. The new amendments are under consideration and are expected to come into force in 2007.

The Customs and Excise (Amendment) Act 2001 gives various law enforcement and statutory bodies within the IOM the ability to exchange information, where such information would assist them in discharging their functions. The Act also permits Customs and Excise to release information it holds to any agency within or outside the IOM for the purposes of any criminal investigation and proceeding. Such exchanges can be either spontaneous or by request.

The Government of the IOM enacted the Anti-Terrorism and Crime Act, 2003. The purpose of the Act is to enhance reporting, by making it an offense not to report suspicious transactions relating to money intended to finance terrorism. The IOM Terrorism (United Nations Measure) Order 2001 implements UNSCR 1373 by providing for the freezing of terrorist funds, as well as by creating a criminal offense with respect to facilitators of terrorism or its financing. All charities are registered and supervised by the Charities Commission. All other UN and EU financial sanctions have been adopted or applied in the IOM, and are administered by Customs and Excise. Institutions are obliged to freeze affected funds and report the facts to Customs and Excise. The FSC's anti-money laundering guidance notes have been revised to include information relevant to terrorist events. The Guidance Notes were issued in December 2001. Additional amendments are being reviewed that will incorporate the new FATF recommendations and EU directives.

The IOM has developed a legal and constitutional framework for combating money laundering and the financing of terrorism. There appears to be a high level of awareness of anti-money laundering and counterterrorist financing issues within the financial sector, and considerable effort has been made to put appropriate practices into place. In November 2003, the Government of the IOM published the full report made by the International Monetary Fund (IMF) following its examination of the regulation and supervision of the IOM's financial sector. In this report the IMF commends the IOM for its robust regulatory regime. The IMF found that "the financial regulatory and supervisory system of the Isle of Man complies well with the assessed international standards." The report concludes the Isle of Man fully meets international standards in areas such as banking, insurance, securities, anti-money laundering, and combating the financing of terrorism.

The IOM is a member of the Offshore Group of Banking Supervisors. The IOM is also a member of the International Association of Insurance Supervisors and the Offshore Group of Insurance Supervisors. The FCU belongs to the Egmont Group. The IOM cooperates with international anti-money laundering authorities on regulatory and criminal matters. Application of the 1988 UN Drug Convention was extended to the IOM in 1993.

Isle of Man officials should continue to support and educate the local financial sector to help it combat current trends in money laundering. The authorities should continue to protect the integrity of the Island's financial system by aggressively identifying, investigating, and prosecuting those involved with money laundering and other financial crimes. The Isle of Man should continue to work with international anti-money laundering authorities to deter financial crime and the financing of terrorism and terrorists.

## Israel

Despite its relatively high GDP, per capita income, and developed financial markets, Israel is not a regional financial center. It primarily conducts financial activity with the financial markets of the United States and Europe, and to a lesser extent with the Far East. Reportedly, less than a quarter of all Israeli money laundering or terrorist financing seizures are related to narcotics proceeds. The majority of the seizures are related to fraud, theft, embezzlement, and illegal money services providers (MSP). Most financial crime investigations in 2006 were related to the intentional failure to report major financial transactions, or the falsification of transaction reports—particularly property transactions. Israel does not have free trade zones and is not considered an offshore financial center, as offshore

banks and other forms of exempt or shell companies are not permitted. Bearer shares, however, are permitted for banks and/or for companies.

In August, 2000, Israel enacted its anti-money laundering legislation, the "Prohibition on Money Laundering Law" (PMLL), (Law No. 5760-2000). The PMLL established a framework for an anti-money laundering system, but required the passage of several implementing regulations before the law could fully take effect. Among other things, the PMLL criminalized money laundering and included more than 18 serious crimes, in addition to offenses described in the prevention of terrorism ordinance, as predicate offenses for money laundering.

In 2001, Israel adopted the Banking Corporations Requirement Regarding Identification, Reporting, and Record Keeping Order. The Order establishes specific procedures for banks with respect to customer identification, record keeping, and the reporting of irregular and suspicious transactions. The PMLL requires the declaration of currency transferred (including cash, travelers' checks, and banker checks) into or out of Israel for sums above 80,000 new Israeli shekels (NIS) (approximately $17,200). This applies to any person entering or leaving Israel, and to any person bringing or taking money into or out of Israel by mail or any other methods, including cash couriers. This offense is punishable by up to six months imprisonment or a fine of NIS 202,000 (approximately $43,400), or ten times the amount that was not declared, whichever is higher. Alternatively, an administrative sanction of NIS 101,000 (approximately $21,700), or five times the amount that was not declared, may be imposed. In 2003, the Government of Israel (GOI) lowered the threshold for reporting cash transaction reports (CTRs) to NIS 50,000 (approximately $10,500), lowered the document retention threshold to NIS 10,000 (approximately $2,100), and imposed more stringent reporting requirements.

The PMLL also provided for the establishment of the Israeli Money Laundering Prohibition Authority (IMPA), as the country's financial intelligence unit (FIU). IMPA became operational in 2002. The PMLL requires financial institutions to report "unusual transactions" to IMPA as soon as possible under the circumstances. The term "unusual transactions" is loosely defined. However, it is used so that the IMPA will receive reports even when the financial institution is unable to link the unusual transaction with money laundering. In addition, suspicious transaction reporting is required of members of the stock exchange, portfolio managers, insurers or insurance agents, provident funds and companies managing a provident fund, providers of currency services, and the Postal Bank. The PMLL does not apply to intermediaries, such as lawyers and accountants.

In 2002, Israel enacted several new amendments to the PMLL that resulted in the addition of the money services businesses (MSB) to the list of entities required to file cash transaction reports (CTRs) and suspicious transaction reports (STRs), the establishment of a mechanism for customs officials to input into the IMPA database, the creation of regulations stipulating the time and method of bank reporting, and the creation of rules on safeguarding the IMPA database and rules for requesting and transmitting information between IMPA, the Israeli National Police (INP) and the Israel Security Agency (Shin Bet). The PMLL also authorized the issuance of regulations requiring financial service providers to identify, report, and keep records for specified transactions for seven years.

In April 2006, the Justice Ministry proposed an amendment to the PMLL that extends Israel's Anti-Money Laundering (AML) regime to cover its substantial diamond trading industry. The amendment defines "dealers in precious stones" as those merchants whose annual transactions reach NIS 50,000 (approximately $11,800). It places significant obligations on dealers to verify the identity of their clients, report all transactions above a designated threshold (and all unusual client activity) to IMPA, as well as maintain all transaction records and client identification for at least five years. This proposal has not yet been passed into legislation by the Knesset.

In October 2006, the Knesset Committee on Constitution, Law and Justice approved an amendment to the Banking Order and the Regulations on the Prohibition on Financing Terrorism. The Order and Regulations were additional steps in the legislation intended to combat the financing of terrorism

while maintaining correspondent and other types of banking relationships between Israeli and Palestinian commercial banks. Although the amendment to the Order and the Regulations impose serious obligations on banks to examine clients and file transaction reports, banks are still exempted from criminal liability if, *inter alia*, they fulfill all of their obligations under the order. The Banking Order was expanded to cover the prohibition on financing terrorism to include obligations to check the identification of parties to a transaction against declared terrorists and terrorist organizations, as well as obligations of reporting by size and type of transaction. The Banking Order sets the minimum size of a transaction that must be reported at NIS 5,000 (approximately $1,180) for transactions with a high-risk country or territory. The order also includes examples for unusual financial activity suspected to be related to terrorism, such as transfers from countries with no anti-money laundering or counterterrorist finance (AML/CTF) regime to nonprofit organizations (NGOs) within Israel and the occupied territories.

Another new regulation added in 2006 allows the INP and the Shin Bet to use information provided to them by IMPA to investigate other offenses in addition to money laundering and terror financing. As Israel does not have legislation preventing financial service companies from disclosing client and ownership information to bank supervisors and law enforcement authorities, the new regulation establishes conditions for the use of such information in order to avoid its abuse and to set guidelines for the police and security services. Other legislative initiatives passed in 2006 include provisions to the Combating Criminal Organizations Law, which applies forfeiture and seizure provisions to criminal offenses resulting from trafficking-in-persons.

The PMLL mandates the registration of MSBs through the Providers of Currency Services Registrar at the Ministry of Finance. In 2004, Israeli courts convicted several MSBs for failure to register with the Registrar of Currency Services. In addition, several criminal investigations have been conducted against other currency-services providers, some of which have resulted in money laundering indictments, which are still pending. The closure of unregistered MSBs remained a priority objective of the INP in 2006. The INP and the Financial Service Providers Regulatory Authority maintain a high level of coordination, routinely exchange information, and have conducted multiple joint enforcement actions. In the past year, Israeli courts convicted several MSBs for violating the obligation to register with the Registrar of Currency Services. In addition, several criminal investigations were brought against other MSBs, some of which resulted in money laundering indictments that are still pending criminal trials.

The INP reports no indications of an overall increase in financial crime relative to previous years. In 2006, IMPA reported 77 arrests and five prosecutions relating to money laundering and/or terrorist financing. In one of this year's major AML operations, the INP arrested three senior employees of the Mercantile Discount Bank branch in Ramleh, as well as 23 customers, under suspicion of conspiring to launder tens of millions of shekels earned from extortion and gambling. Another extensive investigation revealed an organized criminal operation that had gained control over several gas stations in the greater Jerusalem area, and was diluting gasoline with other liquids in order to increase profits. The investigation resulted in 12 arrests, property seizures, and an indictment against 28 defendants for filing fictitious invoices amounting to NIS 350 million, and money laundering among other offenses. IMPA reported six other large criminal cases in 2006 totaling over NIS 160 million (approximately $37,749,310) in laundered money.

In December 2004, the Israeli Parliament adopted the prohibition on terrorist financing law 5765-2004, which is geared to further modernize and enhance Israel's ability to combat terrorist financing and to cooperate with other countries on such matters. The Law went into effect in August 2005. The Israeli legislative regime criminalizing the financing of terrorism includes provisions of the Defense Regulations State of Emergency/1945, the Prevention of Terrorism Ordinance/1948, the Penal Law/1977, and the PMLL. Under the International Legal Assistance Law of 1998, Israeli courts are empowered to enforce forfeiture orders executed in foreign courts for crimes committed outside Israel.

Israeli authorities regularly distribute the names of individuals and entities on the UNSCR 1267 Sanctions Committee consolidated list.

Israel has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets, as well as assets derived from or intended for other serious crimes, including the funding of terrorism. The identification and tracing of such assets is part of the ongoing function of the Israeli intelligence authorities and IMPA. In 2006, IMPA received 9,400 suspicious transaction reports. During this period IMPA disseminated 384 intelligence reports to law enforcement agencies and to foreign FIUs in response to requests, and on its own initiative. In addition, twelve different investigations yielded indictments (some of them multiple indictments). In another case, prosecutors indicted a number of bank officials for money laundering offenses for violation of the obligation to report unusual transactions and for advising their customers on ways of avoiding reporting to IMPA. In 2006, the INP seized approximately $12 million in suspected criminal assets, a significant decrease from the $75 million seized in 2005. Total seizures for each of the previous three years ranged from $23-$27 million each year.

Israel is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. In December 2006 Israel ratified the UN Convention against Transnational Organized Crime. Israel has signed but not yet ratified the UN Convention against Corruption. Israel is also in the final stages of domestic approval for its accession to the Second Additional Protocol to the Council of Europe Convention, which is designed to provide more effective and modern means of assisting member states in law enforcement matters. There is a Mutual Legal Assistance Treaty in force between the United States and Israel.

The Government of Israel continues to make progress in strengthening its anti-money laundering and terrorist financing regime in 2006. Israel should continue the aggressive investigation of money laundering activity associated with organized criminal operations and syndicates. Israel should also continue its efforts to address the misuse of the international diamond trade to launder money.

## Italy

Italy is not an offshore financial center. Italy is part of the euro area and is fully integrated in the European Union (EU) single market for financial services. Money laundering is a concern both because of the prevalence of homegrown organized crime groups and the recent influx of criminal organizations from abroad, especially from Albania, Romania, and Russia.

The heavy involvement in international narcotics trafficking of domestic and Italian-based foreign organized crime groups complicates counternarcotics activities. Italy is both a consumer country and a major transit point for heroin coming from the Near East and Southwest Asia through the Balkans en route to Western/Central Europe and, to a lesser extent, the United States. Italian and ethnic Albanian criminal organizations work together to funnel drugs to Italy and, in many cases, on to third countries. Additional important trafficking groups include other Balkan organized crime entities, as well as Nigerian, Colombian, and other South American trafficking groups.

In addition to the narcotics trade, laundered money originates from myriad criminal activities, such as alien smuggling, contraband cigarette smuggling, pirated goods, extortion, usury, and kidnapping. Financial crimes not directly linked to money laundering, such as credit card and Internet fraud, are increasing.

Money laundering occurs both in the regular banking sector and in the nonbank financial system, including in casinos, money transfer houses, and the gold market. Money launderers predominantly use nonbank financial institutions for the illicit export of currency—primarily U.S. dollars and euros—to be laundered in offshore companies. There is a substantial black market for smuggled goods in the

country, but it is not funded significantly by narcotics proceeds. Italy's underground economy in 2002 was an estimated 27 percent of Italian GDP, or approximately 200 billion euros.

According to a 2006 IMF evaluation, Italy's anti-money laundering and counterterrorist financing system is comprehensive. Money laundering is defined as a criminal offense when laundering relates to a separate, intentional felony offense. All intentional criminal offenses are predicates to the crime of money laundering, regardless of the applicable sentence for the predicate offense. With approximately 600 money laundering convictions a year, Italy has one of the highest rates of successful prosecutions in the world.

Italy has strict laws on the control of currency deposits in banks. Banks must identify their customers and record any transaction that exceeds 12,500 euros (approximately $15,000). Bank of Italy mandatory guidelines require the reporting of all suspicious cash transactions, and other activity—such as a third party payment on an international transaction—must be reported on a case-by-case basis. Italian law prohibits the use of cash or negotiable bearer instruments for transferring money in amounts in excess of approximately $15,000, except through authorized intermediaries or brokers.

Banks and other financial institutions are required to maintain for ten years records necessary to reconstruct significant transactions, including information about the point of origin of funds transfers and related messages sent to or from Italy. Banks operating in Italy must record account data on their own standardized customer databases established within the framework of the anti-money laundering regulation. A "banker negligence" law makes individual bankers responsible if their institutions launder money. The law protects bankers and others with respect to their cooperation with law enforcement entities.

Italy has addressed the problem of international transportation of illegal-source currency and monetary instruments by applying the $15,000-equivalent reporting requirement to cross-border transport of domestic and foreign currencies and negotiable bearer instruments. Reporting is mandatory for cross-border transactions involving negotiable bearer monetary instruments. In any event, financial institutions are required to maintain a uniform anti-money laundering database for all transactions (including wire transfers) over $15,000 and to submit this data monthly to the Italian Exchange Office (known in Italian as Ufficio Italiano dei Cambi, or UIC). The data is aggregated by class of transaction, and any reference to customers is removed. The UIC analyzes the data and can request specific transaction details if warranted.

In 2005, the UIC received 8,576 suspicious transaction reports (STRs) related to money laundering and 482 related to terrorism finance. Italian law requires that the Anti-Mafia Investigative Unit (DIA) and the Guardia di Finanza (GdF) be informed about almost all STRs, including those that the UIC does not pursue further. The UIC does, however, have the authority to perform a degree of filtering before passing STRs to law enforcement. Law enforcement opened 328 investigations based on STRs, which resulted in 103 prosecutions.

Because of Italy's banking controls, narcotics traffickers are using different ways of laundering drug proceeds. To deter nontraditional money laundering, the Government of Italy (GOI) has enacted a decree to broaden the category of institutions and professionals subject to anti-money laundering regulations. The list now includes accountants, debt collectors, exchange houses, insurance companies, casinos, real estate agents, brokerage firms, gold and valuables dealers and importers, auction houses, art galleries, antiques dealers, labor advisors, lawyers, and notaries. The required implementing regulations for the decree, as far as nonfinancial businesses and professions are concerned, were issued in February 2006 and came into force in April 2006 (Ministerial Decrees no. 141, 142 and 143 of 3.02.2006). However, while Italy now has comprehensive internal auditing and training requirements for its (broadly-defined) financial sector, implementation of these measures by nonbank financial institutions lags behind that of banks, as evidenced by the relatively low number of STRs filed by nonbank financial institutions. As of 2005, according to UIC data, banking institutions submit about

80 per cent of all STRs. Money remittance operators submit 13.5 per cent of the total number of STRs, and all other sectors together account for less than ten per cent.

The UIC, which is an arm of the Bank of Italy (BoI), receives and analyzes STRs filed by covered institutions, and then forwards them to either the Anti-Mafia Investigative Unit (DIA) or the Guardia di Finanza (GdF) (financial police) for further investigation. The UIC compiles a register of financial and nonfinancial intermediaries which carry on activities that could be exposed to money laundering. The UIC has access to the banks' customer database. Investigators from the GdF and other Italian law enforcement agencies must obtain a court order prior to being granted access to the archive. The UIC also performs supervisory and regulatory functions such as issuing decrees, regulations, and circulars. It does not require a court order to compel supervised institutions to provide details on regulated transactions.

A special currency branch of the GdF is the Italian law enforcement agency with primary jurisdiction for conducting financial investigations in Italy. STRs helped lead the GdF to identify $14,400,000 in laundered money in 2003.

Italy has established reliable systems for identifying, tracing, freezing, seizing, and forfeiting assets from narcotics trafficking and other serious crimes, including terrorism. These assets include currency accounts, real estate, vehicles, vessels, drugs, legitimate businesses used to launder drug money, and other instruments of crime. Under anti-Mafia legislation, seized financial and nonfinancial assets of organized crime groups can be forfeited. The law allows for forfeiture in both civil and criminal cases. Through October 2004, Italian law enforcement seized more than 160 million euro in forfeited assets due to money laundering.

Italy does not have any significant legal loopholes that allow traffickers and other criminals to shield assets. However, the burden of proof is on the Italian government to make a case in court that assets are related to narcotics trafficking or other serious crimes. Law enforcement officials have adequate powers and resources to trace and seize assets; however, their efforts can be affected by which local magistrate is working a particular case. Funds from asset forfeitures are entered into the general State accounts. Italy shares assets with member states of the Council of Europe and is involved in negotiations within the EU to enhance asset tracing and seizure.

In October 2001, Italy passed a law decree (subsequently converted into law) that created the Financial Security Committee (FSC), charged with coordinating GOI efforts to track and interdict terrorist financing. FSC members include the Ministries of Finance, Foreign Affairs, Home Affairs, and Justice; the BoI; UIC; CONSOB (Italy's securities market regulator); GdF; the Carabinieri; the National Anti-Mafia Directorate (DNA); and the DIA. The Committee has far-reaching powers that include waiving provisions of the Official Secrecy Act to obtain information from all government ministries.

A second October 2001 law decree (also converted into law) made financing of terrorist activity a criminal offense, with prison terms of between seven and fifteen years. The legislation also requires financial institutions to report suspicious activity related to terrorist financing. Both measures facilitate the freezing of terrorist assets. Per FSC data as of December 2004, 57 accounts have been frozen belonging to 55 persons, totaling $528,000 under United Nations resolutions relating to terrorist financing. The GOI cooperates fully with efforts by the United States to trace and seize assets. Italy is second in the EU only to the United Kingdom in the number of individual terrorists and terrorist organizations the country has submitted to the UN 1267 Sanctions Committee for designation.

The UIC disseminates to financial institutions the EU, UN, and U.S. Government lists of terrorist groups and individuals. The UIC may provisionally suspend for 48 hours transactions suspected of involving money laundering or terrorist financing. The courts must then act to freeze or seize the assets. Under Italian law, financial and economic assets linked to terrorists can be directly frozen by

the financial intermediary holding them, should the owner be listed under EU regulation. Moreover, assets can be seized through a criminal sequestration order. Courts may issue such orders as part of criminal investigation of crimes linked to international terrorism or by applying administrative seizing measures originally conceived to fight the Mafia. The sequestration order may be issued with respect to any asset, resource, or item of property, provided that these are goods or resources linked to the criminal activities under investigation. Law no. 15 of January 29, 2006, gave the government authority to implement the EU's Third Money Laundering Directive and to issue provisions to make more effective the freezing of nonfinancial assets belonging to listed terrorist groups and individuals.

In Italy, the term "alternative remittance system" refers to regulated nonbank institutions such as money transfer businesses. Informal remittance systems do exist, primarily to serve Italy's significant immigrant communities, and in some cases are used by Italy-based drug trafficking organizations to transfer narcotics proceeds.

Italy does not regulate charities per se. Primarily for tax purposes, in 1997 Italy created a category of "not-for-profit organizations of social utility" (ONLUS). Such organizations can be associations, foundations or fundraising committees. To be classified as an ONLUS, the organization must register with the Finance Ministry and prepare an annual report. There are currently 19,000 registered entities in the ONLUS category.

Established in 2000, the ONLUS Agency issues guidelines and drafts legislation for the nonprofit sector, alerts other authorities of violations of existing obligations, and confirms de-listings from the ONLUS registry. The ONLUS Agency cooperates with the Finance Ministry in reviewing the conditions for being an ONLUS. The ONLUS Agency has reviewed 1,500 entities and recommended the dissolution of several that were not in compliance with Italian law. Italian authorities believe that there is a low risk of terrorism financing in the Italian nonprofit sector.

Italian cooperation with the United States on money laundering has been exemplary. The United States and Italy have signed a customs assistance agreement, as well as extradition and mutual legal assistance treaties. Both in response to requests under the mutual legal assistance treaty (MLAT) and on an informal basis, Italy provides the United States records related to narcotics trafficking, terrorism and terrorist financing investigations and proceedings. Italy also cooperates closely with U.S. law enforcement agencies and other governments investigating illicit financing related to these and other serious crimes. Currently, assets can only be shared bilaterally if agreement is reached on a case-specific basis. In May 2006, however, the U.S. and Italy signed a new bilateral instrument on mutual legal assistance as part of the process of implementing the U.S./EU Agreement on Mutual Legal Assistance, signed in June 2003. Once ratified, the new U.S./Italy bilateral instrument on mutual legal assistance will provide for asset forfeiture and sharing.

Italy is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Italy ratified the UN Convention against Transnational Organized Crime with the passage of Law no. 146 of March 16, 2006.

Italy is a member of the Financial Action Task Force (FATF) and held the FATF presidency in 1997-98. As a member of the Egmont Group, Italy's UIC shares information with other countries' FIUs. The UIC has been authorized to conclude information-sharing agreements concerning suspicious financial transactions with other countries. To date, Italy has signed memoranda of understanding with France, Spain, the Czech Republic, Croatia, Slovenia, Belgium, Panama, Latvia, the Russian Federation, Canada, and Australia. Italy also is negotiating agreements with Japan, Argentina, Malta, Thailand, Singapore, Hong Kong, Malaysia, and Switzerland. Italy has a number of bilateral agreements with foreign governments in the areas of investigative cooperation on narcotics trafficking and organized crime. There is no known instance of refusal to cooperate with foreign governments.

The Government of Italy is firmly committed to the fight against money laundering and terrorist financing, both domestically and internationally. However, given the relatively low number of STRs being filed by nonbank financial institutions, the GOI should improve its training efforts and supervision in this sector. Italian law enforcement agencies should take additional steps to understand and identify underground finance and value transfer methodologies employed by Italy's burgeoning immigrant communities. The GOI should also continue its active participation in multilateral fora dedicated to the global fight against money laundering and terrorist financing.

## Jamaica

Jamaica, the foremost producer and exporter of marijuana in the Caribbean, is also a major transit country for cocaine flowing from South America to the United States and other international destinations. Because of its location as a major transit center for cocaine, payments for drugs pass through Jamaica in the form of cash shipments back to South America. The profits from these heavy illegal drug flows must be legitimated and therefore make Jamaica susceptible to money laundering activities and other financial crimes. In 2006, there was not a significant increase in the occurrence of financial crimes; however, there was a noticeable upsurge in advance fee scams and other related fraud schemes.

Jamaica is neither an offshore financial center, nor is it a major money laundering country. The Government of Jamaica (GOJ) does not encourage or facilitate money laundering, nor has any senior official been investigated or charged with the laundering of proceeds from illegal activity. The majority of funds being laundered in Jamaica are from drug traffickers and elements of organized crime, mainly the profits obtained in their overseas criminal activities. Jamaican banking authorities do not license offshore banks or other forms of exempt or shell companies. However, nominee or anonymous directors and trustees are allowed for companies registered in Jamaica.

Due to scrutiny by banking regulators, Jamaican financial instruments are considered an unattractive mechanism for laundering money. As a result, much of the proceeds from drug trafficking and other criminal activity are used to acquire tangible assets such as real estate or luxury cars, as well as legitimate businesses. There is a significant black market for smuggled goods, which is due to tax evasion. Further complicating the ability of the GOJ to track and prevent money laundering and the transit of illegal currency through Jamaica are the hundreds of millions of U.S. dollars in remittances sent home by the substantial Jamaican population overseas.

The two free trade zones that operate in Jamaica are in Montego Bay and Kingston. Due to the demise of the garment industry, the Kingston Free Zone is essentially dormant and only a small amount of warehouse space remains. The Montego Bay Free Zone has a small cluster of information technology companies. There is no indication that either free zone is being used for trade-based money laundering or terrorist financing. There is one gaming entity operating in the free zone; its license does not permit local betting. Domestic casino gambling is permitted in Jamaica.

The Money Laundering Act (MLA), as amended in February 2000, currently governs Jamaica's anti-money laundering regime. The MLA criminalizes money laundering related to narcotics offenses, fraud, firearms trafficking and corruption. Bank secrecy laws exist; however, there are provisions under GOJ law to enable law enforcement access to banking information.

Under the MLA, banks and a wide range of financial institutions (including wire-transfer companies, exchange bureaus, building societies, insurance companies and securities dealers) are required to report suspicious transactions of any amount to Jamaica's financial intelligence unit, the Financial Investigations Division (FID) of the Ministry of Finance. The MLA establishes a five-year record-keeping requirement and requires financial institutions to report all currency transactions over

$50,000. Exchange bureaus have a reporting threshold of $8,000. Jamaica's central bank, the Bank of Jamaica, supervises the financial sector for compliance with anti-money laundering provisions.

The FID has operated as the de facto FIU since 2001. Under the draft Proceeds of Crime Act, which is currently being debated before Parliament, the FID will be named as Jamaica's official FIU. Companion legislation to the Act has been drafted to allow the sharing of information with other FIUs. In preparation for its expanded investigative role once the Act is passed, the FID has embarked on a five-stage plan to enhance its capacity in 2006. This includes the installation of a new computer system to process and track cases.

The FID consists of 14 forensic examiners, six police officers who have full arrest powers, a director and five administrative staff. Suspicious transaction reports (STRs) or cash transaction reports (CTRs) that are deemed to warrant further investigation are referred to the Financial Intelligence Division within the FID. Efforts are underway to improve the cooperation between the Tax authorities (TAAD) and the FID. Both the FID and the TAAD units suffer from a lack of adequate resources; therefore, the TAAD's competing priorities—such as revenue collection obligations, a main focus of the GOJ—take precedence over assisting the FID with money laundering investigations.

Jamaica has an ongoing education program to ensure compliance with the mandatory STR requirements. Reporting individuals are protected by law with respect to their cooperation with law enforcement entities. The FID reports that nonbanking financial institutions have a 70 percent compliance rate with money laundering controls. In 2006, 18,311 STRs were filed; of these, 14 were referred to law enforcement for investigation. Since January 2006, seven persons have been arrested and charged with money laundering.

The Jamaican Parliament's 2004 amendments to the Bank of Jamaica Act, the Banking Act, the Financial Institutions Act, and the Building Societies Act improved the governance, examination and supervision of commercial banks and other financial institutions by the Bank of Jamaica. Amendments were also passed to the Financial Services Commission Act, which governs financial entities supervised by the Financial Services Commission. These measures expanded the powers of the authorities to share information, particularly with overseas regulators and law enforcement agencies. The amended Acts provide the legal and policy parameters for the licensing and supervision of financial institutions, and lay the foundation to complement the proposed reforms to the MLA through the enactment of the draft Proceeds of Crime Act.

The GOJ requires customs declaration of currency or monetary instruments over $10,000 (or its equivalent). The Airport Interdiction Task Force, a joint law enforcement effort by the United States, United Kingdom, Canada and Jamaica, will begin operation in early 2007. The Task Forces focuses, in part, on efforts to combat the movement of large amounts of cash often in shipments totaling hundreds of thousands of U.S. dollars through Jamaica.

Currently, the FID and the Jamaica Constabulary Force (JCF) are the entities responsible for tracing and seizing assets. Law enforcement authorities are hampered by the fact that Jamaica has no civil forfeiture law. Under the 1994 Drug Offenses (Forfeiture of Proceeds) Act, a criminal drug-trafficking conviction is required prior to forfeiture. This often means that even when police discover illicit funds, the money cannot be seized or frozen and must be returned to the criminals. Assets that are eventually forfeited are deposited into a fund shared by the Ministries of National Security, Justice and Finance.

The Proceeds of Crime Act, when passed, would incorporate the existing provisions of the MLA and would allow for the civil forfeiture of assets related to criminal activity. The Act would expand the confiscation powers of the GOJ and permit, upon conviction, the forfeiture of benefits assessed to have been received by the convicted party within the six years preceding the conviction. The Act would include a provision allowing for the forfeiture of assets related to human trafficking and terrorist financing, and would apply to all property or assets associated with an individual convicted or

suspected of involvement with a crime. This includes legitimate businesses used to launder drug money or support terrorist activity. Under the Act, the proposed division of forfeited assets would distribute one-third of assets to the Ministry of National Security, one-third to the Ministry of Finance, and one-third to the Ministry of Justice.

There was an increase in the amount of both seizures and forfeitures of assets for 2006. In 2006, over $2 million was seized and $1.5 million was forfeited, a significant increase over the $646,000 seized and $476,000 forfeited in 2005. Nondrug related assets go to a consolidated or general fund, while drug related assets—which totaled $560,000 in 2006—are placed into a forfeited asset fund, which benefits law enforcement.

The draft Proceeds of Crime Act addresses many of the shortcomings of the GOJ's current legislative anti-money laundering and asset forfeiture regime. However, despite a lack of major opposition to the bill, the Act has been under consideration for a year. The GOJ intends to pass the Act in early 2007.

The Terrorism Prevention Act of 2005 criminalizes the financing of terrorism, consistent with UN Security Council Resolution 1373. Under the Terrorism Prevention Act, the GOJ has the authority to identify, freeze and seize terrorist finance related assets. The FID has the responsibility for investigating terrorist financing. The FID is currently updating its FIU database and will be implementing a system to cross-reference reports from the U.S. Treasury Department's Office of Foreign Asset Control (OFAC) and the UN Sanctions Committee. Additionally, the Ministry of Foreign Affairs and Foreign Trade circulates to all relevant agencies the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list. To date, no accounts owned by those included on the UN consolidated list have been identified in Jamaica.

The GOJ has not encountered any misuse of charitable or nonprofit entities as conduits for the financing of terrorism. The Ministry of Finance is currently finalizing its risk-assessment report on charitable organizations.

Jamaica and the United States have a Mutual Legal Assistance Treaty that entered into force in 1995. Jamaica is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the Inter-American Convention against Corruption, and the UN Convention against Transnational Organized Crime. The GOJ has signed, but not ratified, the UN Convention against Corruption. Jamaica is a member of the Caribbean Financial Action Task Force (CFATF) and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The FID is not a member of the Egmont Group of financial intelligence units.

The Government of Jamaica should ensure the swift passage of legislation to improve its anti-money laundering efforts, as well as procedures to enhance asset forfeiture. Jamaica should ensure that the proposed legislative reforms allow for a fully functioning financial intelligence unit that meets the membership criteria of the Egmont Group and other international standards. A more aggressive effort is necessary to bring Jamaica's anti-money laundering and counterterrorist financing regime into line with international standards.

## Japan

Japan is the world's second largest economy and a large and important world financial center. Although the Japanese government continues to strengthen legal institutions to permit more effective enforcement of financial transaction laws, Japan still faces substantial risk of money laundering by organized crime and other domestic and international criminal elements. The principal sources of laundered funds are drug trafficking and financial crimes: illicit gambling, loan-sharking, extortion, abuse of legitimate corporate activities, internet fraud activities, and all types of property related crimes, often linked to Japan's criminal organizations. U.S. law enforcement investigations

periodically show a link between drug-related money laundering activities in the U.S. and bank accounts in Japan. The number of Internet-related money laundering cases involving Japan is also increasing. In some cases, criminal proceeds were concealed in bank accounts obtained through an Internet market. Laws enacted in 2004 make online sales of bank accounts illegal.

On November 17, 2005, the Japanese government's headquarters for the Promotion of Measures against Transnational Organized Crime and Other Related Issues and the headquarters for International Terrorism agreed that relevant ministries would submit a bill to the 2007 ordinary session of the Diet to enhance compliance with the FATF Forty Recommendations and the FATF Nine Special Recommendations on Terrorist Financing. It is now expected that these recommendations will be promulgated by April 1, 2007, given the probable timing for the Anti-Money Laundering Law currently being drafted by the National Police Agency. In accordance with the FATF Forty Recommendations of 2003, the new Anti-Money Laundering Law will include a wider range of sectors required to submit suspicious transaction reports (STR), including accountants, real estate agents, dealers in precious metals and stones, and certain types of company service providers. The government of Japan is also considering measures to implement the FATF's Special Recommendation Nine, which recommends cross-border currency reporting requirements.

Drug-related money laundering was first criminalized under the Anti-Drug Special Law that took effect July 1992. This law also mandates the filing of STRs for suspected proceeds of drug offenses, and authorizes controlled drug deliveries. The legislation also creates a system to confiscate illegal profits gained through drug crimes. The seizure provisions apply to tangible and intangible assets, direct illegal profit, substitute assets, and criminally derived property that have been commingled with legitimate assets.

The narrow scope of the Anti-Drug Special Law and the burden required of law enforcement to prove a direct link between money and assets to specific drug activity limits the law's effectiveness. As a result, Japanese police and prosecutors have undertaken few investigations and prosecutions of suspected money laundering. Many Japanese officials in the law enforcement community, including Japanese Customs, believe that Japan's organized crime groups have been taking advantage of this limitation to launder money.

Japan expanded its money laundering law beyond narcotics trafficking to include money laundering predicate offenses such as murder, aggravated assault, extortion, theft, fraud, and kidnapping when it passed the 1999 Anti-Organized Crime Law (AOCL), which took effect in February 2000. The law extends the confiscation laws to include additional money laundering predicate offenses and value-based forfeitures. It also authorizes electronic surveillance of organized crime members, and enhances the suspicious transaction reporting system.

The AOCL was partially revised in June of 2002 by the "Act on Punishment of Financing to Offences of Public Intimidation," which specifically added the financing of terrorism to the list of money laundering predicates. An amendment to the AOCL was submitted on February 20, 2004 to the Diet for approval, was resubmitted to the Diet in October 2005, and remains under consideration. The amendment would expand the predicate offenses for money laundering from approximately 200 offenses to nearly 350 offenses, with almost all offenses punishable by imprisonment.

Japan's Financial Services Agency (FSA) supervises public-sector financial institutions and the Securities and Exchange Surveillance Commission supervises securities transactions. The FSA classifies and analyzes information on suspicious transactions reported by financial institutions, and provides law enforcement authorities with information relevant to their investigation. Japanese banks and financial institutions are required by law to record and report the identity of customers engaged in large currency transactions. There are no secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement authorities.

To facilitate the exchange of information related to suspected money laundering activity, the FSA established the Japan Financial Intelligence Office (JAFIO) on February 1, 2000, as Japan's financial intelligence unit. Financial institutions in Japan forward STRs to JAFIO, which analyzes and disseminates them as appropriate. At the end of 2005, Japan announced plans to transfer JAFIO from the FSA to the National Policy Agency, possibly on April 1, 2007, pending the successful passage of the new Anti-Money Laundering Law.

In 2006, JAFIO received 113,860 STRs, up from the 98,935 STRs received in 2005. In 2006, some 82 percent of the reports were submitted by banks, 7 percent by credit cooperatives, 9 percent from the country's large postal savings system, 0.7 percent from nonbank money lenders, and almost none from insurance companies. In 2006, JAFIO disseminated to law enforcement 71,241 STRs, up from 66,812 STRs disseminated in 2005.

JAFIO concluded international cooperation agreements during 2006 with the FIU's of Australia, Thailand, Hong Kong, Canada and Indonesia. In 2004, JAFIO concluded such cooperation agreements with Singapore's Financial Intelligence Unit (FIU) and with FinCEN, establishing cooperative frameworks for the exchange of financial intelligence related to money laundering and terrorist financing. JAFIO already had similar agreements in place with the FIUs of the United Kingdom, Belgium, and South Korea. Japanese financial institutions have cooperated with law enforcement agencies, including U.S. and other foreign government agencies investigating financial crimes related to narcotics. In 2006, Japan concluded a Mutual Legal Assistance Treaty (MLAT) with the Republic of Korea. In 2003, the United States and Japan concluded a Mutual Legal Assistance Treaty (MLAT).

Although Japan has not adopted "due diligence" or "banker negligence" laws to make individual bankers legally responsible if their institutions launder money, there are administrative guidelines that require due diligence. In a high-profile 2006 court case, however, the Tokyo District Court ruled to acquit a Credit Suisse banker of knowingly assisting an organized crime group to launder money despite doubts about whether the banker performed proper customer due diligence. Japanese law protects bankers and other financial institution employees who cooperate with law enforcement entities.

In April 2002, the Diet enacted the Law on Customer Identification and Retention of Records on Transactions with Customers by Financial Institutions (a "know your customer" law). The law reinforced and codified the customer identification and record-keeping procedures that banks had practiced for years. The Foreign Exchange and Foreign Trade law was also revised so that financial institutions are required to make positive customer identification for both domestic transactions and transfers abroad in amounts of more than two million yen (approximately $16,950). Banks and financial institutions are required to maintain customer identification records for seven years.

In 2004, the FSA cited Citibank Japan's failure to properly screen clients under anti-money laundering mandates as one of a list of problems that caused the FSA to shut down Citibank Japan's private banking unit. In February 2004, the FSA disciplined Standard Chartered Bank for failing to properly check customer identities and for violating the obligation to report suspicious transactions. In January 2007, the Federal Reserve ordered Japan's Sumitomo Mitsui Banking Corp.'s New York branch to address anti-money laundering deficiencies, only a month after similarly citing Bank of Tokyo-Mitsubishi UFJ for anti-money laundering shortcomings.

The Foreign Exchange and Foreign Trade Law requires travelers entering and departing Japan to report physically transported currency and monetary instruments (including securities and gold weighing over one kilogram) exceeding one million yen (approximately $8,475), or its equivalent in foreign currency, to customs authorities. Failure to submit a report, or submitting a false or fraudulent one, can result in a fine of up to 200,000 yen (approximately $1,695) or six months' imprisonment. In January 2007, an amendment to the rule on Customer Identification by Financial Institutions came into

force, whereby financial institutions are now required to identify the originators of wire transfers of over 100,000 yen.

In response to the events of September 11, 2001 the FSA used the anti-money laundering framework provided in the Anti-Organized Crime Law to require financial institutions to report transactions where funds appeared either to stem from criminal proceeds or to be linked to individuals and/or entities suspected to have relations with terrorist activities. The 2002 Act on Punishment of Financing of Offenses of Public Intimidation, enacted in July 2002, added terrorist financing to the list of predicate offenses for money laundering, and provided for the freezing of terrorism-related assets. Japan signed the UN International Convention for the Suppression of the Financing of Terrorism on October 30, 2001, and became a party on June 11, 2002.

After September 11, 2001, Japan has regularly searched for and designated for asset freeze any accounts that might be linked to all the suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list.

Underground banking systems operate widely in Japan, especially in immigrant communities. Such systems violate the Banking Law and the Foreign Exchange Law. There have been a large number of investigations into underground banking networks. Reportedly, substantial illicit proceeds have been transferred abroad, particularly to China, North and South Korea, and Peru. In November 2004, the Diet approved legislation banning the sale of bank accounts, in a bid to prevent the use of purchased accounts for fraud or money laundering.

Japan has not enacted laws that allow for sharing of seized narcotics assets with other countries. However, the Japanese government fully cooperates with efforts by the United States and other countries to trace and seize assets, and makes use of tips on the flow of drug-derived assets from foreign law enforcement efforts to trace funds and seize bank accounts.

Japan is a party to the 1988 UN Drug Convention and has signed but not ratified the UN Transnational Organized Crime Convention. Ratification of this convention would require amendments to Japan's criminal code to permit charges of conspiracy, which is not currently an offense. Minority political parties and Japan's law society have blocked this amendment on at least three occasions. Japan is a member of the Financial Action Task Force. JAFIO joined the Egmont Group of FIUs in 2000. Japan is also a member of the Asia/Pacific Group against Money Laundering. In 2002, Japan's FSA and the U.S. Securities and Exchange Commission and Commodity Futures Trading Commission signed a nonbinding Statement of Intent (SOI) concerning cooperation and the exchange of information related to securities law violations. In January 2006 the FSA and the U.S. SEC and CFTC signed an amendment to their SOI to include financial derivatives.

The government of Japan has many legal tools and agencies in place to successfully detect, investigate, and combat money laundering. In order to strengthen its money laundering regime, Japan should stringently enforce the Anti-Organized Crime Law. Japan should also enact penalties for noncompliance with the Foreign Exchange and Trade Law, adopt measures to share seized assets with foreign governments, and enact banker "due diligence" provisions. Japan should continue to combat underground financial networks. Since Japan is a major trading power and the misuse of trade is often the facilitator in alternative remittance systems, Japan should take steps to identify and combat trade-based money laundering. Japan should also become a party to the UN Transnational Organized Crime Convention.

## Jersey

The Bailiwick of Jersey (BOJ) encompasses part of the Channel Islands and is a Crown Dependency of the United Kingdom. The majority of illicit money in Jersey is derived from foreign criminal activity. Local drug trafficking and corruption of politically exposed persons (PEP) are sources of

illicit proceeds found in the country. Jersey's sophisticated array of offshore services is similar to that of international financial services centers worldwide. Money laundering mostly occurs with Jersey's banking system, investment companies, and local trust companies. As of September 2006, the financial services industry consists of 47 banks, 908 trust companies, 175 insurance companies (largely captive insurance companies), and 1086 collective investment funds. Other services include investment advice, dealing, and management companies, and mutual fund companies. In addition the financial services companies offer corporate services, such as special purpose vehicles for debt restructuring and employee share ownership schemes. For high net worth individuals, there are many wealth management services.

The International Monetary Fund (IMF) conducted an assessment of the anti-money laundering regime of Jersey in October 2003. The IMF team found Jersey's Financial Services Commission (JFSC), the financial services regulator, to be in compliance with international standards, but provided recommendations for improvement.

The Jersey Finance and Economics Committee administers the law regulating, supervising, promoting, and developing the Jersey finance industry. The IMF report noted that the Finance and Economics Committee's power to give direction to the JFSC might appear to be a conflict of interest between the two agencies, and suggested that the BOJ establish a separate body to speak for the industry's consumers. The report proposed that Jersey authorities establish rules for banks dealing with market risk, along with a code of conduct for collective investment funds. The IMF report also recommended that the BOJ institute a contingency plan for the failure of a major institution.

Jersey is working to address the issues raised in the report. The JFSC reportedly intends to continue to strengthen its existing regulatory powers and amend the Financial Services Commission Law 1998 to provide legislative support for its inspections. The JFSC also plans to introduce monetary fines for administrative and regulatory breaches. Improvements will also include stricter industry guidelines and tighter enforcement of anti-money laundering and terrorist financing controls.

Jersey's main anti-money laundering laws are the Drug Trafficking Offenses (Jersey) Law of 1988, which criminalizes money laundering related to narcotics trafficking, and the Proceeds of Crime (Jersey) Law, 1999, which broadens the predicate offenses for money laundering to all offenses punishable by at least one year in prison. The Prevention of Terrorism (Jersey) Law 1996, which criminalizes money laundering related to terrorist activity, was replaced by the Terrorism (Jersey) Law 2002 that came into force in January 2003. The Terrorism (Jersey) Law 2002 is a response to the events of September 11, 2001, and enhances the powers of BOJ authorities to investigate terrorist offenses, to cooperate with law enforcement agencies in other jurisdictions, and to seize assets. Jersey passed the Corruption Law 2005 in alignment with the Council of Europe Criminal Law Convention on Corruption. Although the law was registered in May 2006, by the end of 2006 it had not yet come into force.

Suspicious transaction reporting is mandatory under the narcotics trafficking, terrorism, and anti-money laundering laws. There is no threshold for filing a suspicious transaction report, and the reporting individual is protected from criminal and civil charges by safe harbor provisions in the law. Record keeping requirements mandate that banks and other financial service companies maintain financial records of their customers for a minimum of 10 years. The JFSC has issued anti-money laundering (AML) Guidance Notes that the courts consider when determining whether or not an offense has been committed under the Money Laundering Order. Penalties for a money laundering conviction include imprisonment for a minimum of one year.

After consultation with the financial services industry, the JFSC issued a joint paper with Guernsey and the Isle of Man that recommended proposals to tighten the essential due diligence requirements for financial institutions with regard to their customers. The position paper states the JFSC's insistence on the responsibility of all financial institutions to verify the identity of their customers, regardless of

any intermediary. The paper also outlines a program to obtain verification documentation for customer relationships preceding the Proceeds of Crime (Jersey) Law. Working groups review specific portions of these principles annually and draft AML Guidance Notes to incorporate changes and improvements.

Approximately 31,162 Jersey companies are registered with the Registrar of Companies. In addition to public filings relating to shareholders, the JFSC requires each Jersey-registered company to file details regarding the ultimate beneficial owners. That information is held confidentially but is available to domestic and foreign investigators under appropriate circumstances and in accordance with the law.

A number of companies registered in other jurisdictions are administered in Jersey. "Exempt companies" do not pay Jersey income tax and are only available to nonresidents. Jersey does not provide offshore licenses. All financial businesses must have a presence in Jersey and their management must be located in Jersey. Alternate remittance systems reportedly are not prevalent.

Jersey has established a Financial Intelligence Unit (FIU) known as the Joint Financial Crime Unit (JFCU). This unit receives, investigates, and disseminates suspicious transaction reports (STRs). The unit includes a financial crime analyst as well as officers from Jersey's Police and Customs services. The JFCU received 1,034 STRs in 2006, and 1,162 in 2005. Approximately twenty-five percent of the STRs filed in 2005 and 2006 resulted in further police investigations.

The FIU, in conjunction with the Attorney General's Office, can trace, seize and freeze assets. It can obtain a confiscation order with a proven link to a crime. If the criminal has benefited from a crime, legitimate assets may be forfeited to meet a confiscation order. There is no maximum interval between the freezing of assets and when the assets are released. The Attorney General's Office may apply to the Court to confiscate assets previously frozen. Seized and forfeited proceeds from drug trafficking are placed in a separate fund which is then used to assist law enforcement in the fight against drug trafficking and to support harm reduction programs and education initiatives. Jersey allows limited civil forfeiture relating to cash proceeds of drug trafficking located at the ports and is considering introducing and implementing civil asset forfeiture powers.

Authorities in Jersey do not circulate the names of suspected terrorists and terrorist organizations listed on the United Nations Security Council Resolution (UNSCR) 1267 Sanctions Committee's consolidated list, nor do they circulate the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, the EU designated list, or any other designated list. Institutions in the BOJ are expected to gather information of designated entities from the internet and other public sources. Jersey authorities have implemented sanction orders freezing accounts of individuals connected with terrorist activity.

Jersey's authorities have extensive license to cooperate with other domestic and international law enforcement and regulatory agencies. The JFSC cooperates with regulatory authorities to ensure that financial institutions meet anti-money laundering obligations. In 2005, the JFSC and the Jersey FIU worked together to deny the licensing of a Trust company and close a medium size business for failure to adhere to the AML legislation and guidance issued by the regulator. Internationally, the JFSC has reached agreements on information exchange with securities regulators in Germany, France, and the United States. The JFSC has a memorandum of understanding for information exchange with Belgium. The 1988 U.S.-UK Agreement Concerning the Investigation of Drug Trafficking Offenses and the Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking, as amended in 1994, was extended to Jersey in 1996. Jersey shares forfeited assets with the U.S. pursuant to this agreement, and its laws enable Jersey to share assets in nondrug cases as well. Application of the 1988 UN Drug Convention was extended to Jersey on July 7, 1997. Jersey's FIU is a member of the Egmont Group.

The Bailiwick of Jersey has established an anti-money laundering program that in some instances exceeds international standards, and addresses its particular vulnerabilities to money laundering.

However, Jersey should establish reporting requirements for the cross-border transportation of currency and monetary instruments, and set penalties for violations. Jersey should also take steps to force its obligated entities to obtain verification documents for customers preceding the 1999 requirements. The BOJ should introduce civil asset forfeiture, and implement its new corruption law. Jersey should also ensure that supervisory authorities exist to apply standards and regulations to its port activity and "exempt companies" that are identical to those used in the rest of the jurisdiction. Jersey should take steps toward a more proactive role in fighting terrorism financing by circulating the UNSCR 1267 list as well as other lists, instead of relying on the entities to research names through online public sources. Jersey should continue to demonstrate its commitment to fighting financial crime by enhancing its anti-money laundering/counterterrorist financing regime in these areas of vulnerability.

## Jordan

Despite significant growth in its financial services sector, Jordan is neither a regional nor offshore financial center, and is not considered a major venue for international criminal activity. The banking and financial sectors, including money service businesses, are supervised by competent authorities.

The Government of Jordan (GOJ) has yet to enact a comprehensive anti-money laundering law (AML). A draft law has been approved by the legal committee of the lower house of Parliament and there is hope that Parliament will pass the law during the 2006-2007 winter session. Currently, the Central Bank's suspicious transaction follow-up unit receives reports of suspicious financial activity from banks under the authority of Article 93 of the Banking Law of 2000, which obligates covered persons to notify the Central Bank of any transaction suspected of being related to any "crime or illegitimate act." In order to comply with international best practices, the Central Bank issued Instructions No. 29/2006 for banks in May 2006 which include important obligations concerning customer due diligence, politically exposed persons, wire transfers, record keeping, suspicious activity reporting, and internal policies and procedures, including the mandatory designation of a money laundering reporting officer. Instructions No.10/2001 impose similar, though less stringent, obligations on money service businesses. Article 52 of the Insurance Regulatory Act of 1999 criminalizes money laundering using insurance instruments. The Banking Law of 2000 (as amended in 2003) allows judges to waive banking secrecy provisions in any number of criminal cases, including suspected money laundering and terrorism financing.

In November 2006, Jordan's Parliament enacted an Anti-Terrorism law that prohibits the collection of funds with the intent that they be used in terrorist acts, and Article 147 of the Jordanian Penal Code prohibits banking transactions related to terrorist activity. However, Jordan does not yet have a statutory basis for the administrative freezing of the assets of designated terrorists listed on the UNSCR 1267 Sanctions Committee's consolidated list. Assets can be frozen and ultimately confiscated as part of a criminal investigation. In December 2004, the United States and Jordan signed an Agreement regarding Mutual Assistance between their Customs Administrations that provides for mutual assistance with respect to customs offenses and the sharing and disposition of forfeited assets.

Jordanian officials report that financial institutions file suspicious transaction reports and cooperate with prosecutors' requests for information related to narcotics trafficking and terrorism cases. There have not been any prosecutions or convictions for money laundering or terrorist finance. Legislation creating a Financial Intelligence Unit (FIU) is pending.

Charitable organizations are regulated by the Ministry of Social Development, and are governed by the Charitable Associations and Social Organizations Act of 1966. In accordance with this Act, organizations must register with the Ministry, which has the right to accept or reject the registration and conduct on-site inspections and review financial records. Furthermore, the Collection of Charitable Donations Regulation No. 1 of 1957 requires that all donations must be deposited in a bank

as soon as the collection process ends, and that the Ministry must be informed of the deposit. According to Central Bank Instructions No. 29/2006, banks must verify the identity of any charitable organization wishing to open an account. Moreover, the Penal Code stipulates that whoever collects donations, subscriptions, or contributions for an illicit organization shall be imprisoned for a period not to exceed six months.

There are six public free trade zones (FTZs) operating in Jordan, as well as 26 private FTZs. The FTZs operate under the supervision of the Free Zones Corporation as well as the Customs Department and are governed by the Free Zones Corporation Investment Regulation No. 43 of 1987 as well as the Customs Law. Both the Law and the Regulation prohibit the entrance of illegal material into the zones. The Customs Law grants the Minister of Finance the right to form joint committees comprised of staff from the Customs Department and the Free Zones Corporation to verify and inspect goods to ensure that no contraband is found in free zones. The Customs Law considers removal of goods from the free zones without the necessary customs clearances a smuggling offence. Currently, there is no cross border cash declaration requirement, although such a provision is contained in the draft AML law.

Jordan is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. Jordan has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Jordan is a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004. In January 2007, Jordan assumes the presidency of this FATF-style regional body.

The Government of Jordan should enact a comprehensive anti-money laundering law that adheres to international standards including criminalizing money laundering from all serious crimes. The legislation should establish a Financial Intelligence Unit capable of sharing financial information with foreign counterparts. Jordan should develop a rigorous regime for the freezing, seizing and forfeiture of criminal assets and assets related to the financing of terrorism. The GOJ should become a party to the UN Convention against Transnational Organized Crime. Jordanian law enforcement and customs should examine forms of trade-based money laundering.

## Kenya

Kenya does not have an effective legal regime to address money laundering. The Government of Kenya (GOK) has no regulations to freeze/seize criminal or terrorist accounts, and has not passed a law that explicitly outlaws money laundering and creates a financial intelligence unit (FIU). As a regional financial and trade center for Eastern, Central, and Southern Africa, Kenya's economy has large formal and informal sectors. Many entities in Kenya are involved in exporting and importing goods, including a reported 800 registered international nongovernmental organizations (NGOs) managing approximately $1 billion annually. Annual remittances from expatriate Kenyans are estimated at $680 -780 million. Individual Kenyans and foreign residents also transfer money out of Kenya. Many transfers are executed via formal channels such as wire services and banks, but there is also a thriving network of cash-based, unrecorded transfers.

Kenya's use as a transit point for international drug traffickers is increasing. Domestic drug abuse is also increasing, especially in Coast Province. Narcotics proceeds are being laundered in Kenya, although the volume has not yet been determined.

Kenya has no offshore banking or Free Trade Zones. Kenya has a large informal sector and a thriving network of cash-based, unrecorded transfers, primarily used by expatriates to send and receive remittances internationally. The large Somali refugee population in Kenya uses a hawala system to send and receive remittances; however, the GOK has no means to monitor hawala transfers.

Section 49 of the Narcotic Drugs and Psychotropic Substance Control Act of 1994 criminalizes money laundering related to narcotics trafficking and makes it punishable by a maximum prison sentence of

14 years. However, no cases of the laundering of funds from narcotics trafficking have ever been successfully prosecuted. The Act, together with Legal Notice No. 4 of 2001, the Central Bank of Kenya (CBK) Guidelines on Prevention of Money Laundering and enabling provisions of other laws, make money laundering a criminal offense but do not create an effective anti-money laundering (AML) regime.

In November 2006, the GOK published a proposed Proceeds of Crime and Anti-Money Laundering Bill. This bill is a revised version of a draft law introduced in 2004. It declares itself to be "An act of Parliament to provide for the offence of money laundering and to introduce measures for combating the offence, to provide for the identification, tracing, freezing, seizure and confiscation of the proceeds of crime." It defines "proceeds of crime" as any property or economic advantage derived or realized, directly or indirectly, as a result of or in connection with an offence. The draft legislation provides for both criminal and civil restraint, seizure and forfeiture. In addition, the proposed bill would authorize the establishment of an FIU and require financial institutions and nonfinancial businesses or professions, including casinos, real estate agencies, precious metals and stones dealers, and legal professionals and accountants, to file suspicious transaction reports above a certain threshold.

The bill also identifies 30 other statutes to be amended so that they will be consistent with the new bill when it is passed.

The new bill has some deficiencies. It does not mention terrorism, nor does it specifically define "offense" or "crime." The proposed legislation does not explicitly authorize the seizing of legitimate businesses used to launder money. The requirement that only suspicious transactions above a certain threshold are reported is inconsistent with international standards, which call for suspicious transaction reports to have no monetary threshold. The bill generated more support than the 2004 draft legislation, and senior GOK officials have claimed it is a high priority. However, the GOK did not table the bill in Parliament until November 22, and the bill lapsed when Parliament recessed on December 8. The bill will likely be tabled early in 2007.

The CBK is the regulatory and supervisory authority for Kenya's deposit-taking institutions and has responsibility for over 51 such entities, 95 foreign exchange bureaus, and mortgage companies and other financial institutions. Casinos are regulated by the Minister of Home Affairs, although its supervision of this sector is believed to be ineffective.

Forex bureaus were established and first licensed in January 1995 to foster competition in the foreign exchange market and to narrow the exchange rate spread in the market. As authorized dealers, forex bureaus conduct business and are regulated under the provisions of the Central Bank of Kenya Act (Cap 491). The CBK subsequently recognized that several bureaus were violating the Forex Bureau Guidelines, including dealing in third party checks and doing telegraphic transfers without the approval of the Central Bank. Those checks and transfers may have been used for fraud, tax evasion and money laundering. The CBK's Banking Supervision Department therefore issued Central Bank circular No. 1 of 2005 instructing all forex bureaus to cease immediately dealing in telegraphic transfers and third party checks. These new guidelines are issued under Section 33K of the Central Bank of Kenya Act, and took effect on January 1, 2007. They address third party checks and telegraphic transfers, and are also expected to enhance competition among bureaus.

In October 2000, the CBK issued regulations that require deposit-taking institutions to verify the identity of new customers opening an account or conducting a transaction. The Banking Act amendment of December 2001 authorizes disclosure of financial information by the CBK to any monetary authority or financial regulatory authority within or outside Kenya. In 2002, the Kenya Bankers Association (KBA) issued guidelines requiring banks to report suspicious transactions to the CBK. These guidelines do not have the force of law, and only a handful of suspicious transactions have been reported so far. There have been no arrests or prosecutions for money laundering or terrorist financing. Under the regulations, banks must maintain records of transactions over $100,000 and

international transfers over $50,000, and report them to the CBK. These regulations do not cover nonbank financial institutions such as money remitters, casinos, or investment companies, and there is no enforcement mechanism behind the regulations. Some commercial banks and foreign exchange bureaus do file suspicious transaction reports voluntarily, but they run the risk of civil litigation, as there are no adequate "safe harbor" provisions for reporting such transactions to the CBK. A law enforcement agency can demand information from any financial institution, if it has obtained a court order. However, a court ruling to penalize a commercial bank in 2002 for disclosing information to the CBK, in response to a court order, made banks wary of reporting suspicious transactions. The contradiction highlights the need for "safe harbor" provisions and a robust anti-money laundering law.

Kenya has little in the way of cross-border currency controls. GOK regulations require that any amount of cash above $5,000 be disclosed at the point of entry or exit for record-keeping purposes only, but this provision is rarely enforced. The CBK guidelines call for currency exchange bureaus to furnish reports on a daily basis on any single foreign exchange transaction above $10,000, and on cumulative daily foreign exchange inflows and outflows above $100,000. Under September 2002 guidelines, foreign exchange dealers are required to ensure that cross-border payments are not connected with illegal financial transactions.

Kenya's vulnerability to money laundering was recently demonstrated by investigations revealing that Charterhouse Bank managers had conspired with depositors to evade import duties and taxes and launder the proceeds totaling approximately $500 million from 1999 to 2006. In June 2006, a member of Parliament tabled a 2004 initial investigation report on Charterhouse Bank by a special CBK investigations team indicating account irregularities, tax evasion and money laundering by some of the bank's clients. The Ministry of Finance temporarily closed the bank to prevent a run, and the CBK placed Charterhouse Bank under statutory management to preserve records and prevent removal of funds. Subsequent audits and investigations covering the period 1999-2006 found that Charterhouse Bank had violated the CBK's know-your-customer procedures in over 80 percent of its accounts, and were missing basic details such as the customer's name, address, ID photo, or signature cards.

Charterhouse Bank also violated the Banking Act and the CBK's Prudential Guidelines by not properly maintaining records for foreign currency transactions. The bank management's continual violation of CBK prudential guideline CBK/PG/08 requirements to report suspicious transactions, and its efforts to conceal them from CBK examiners, indicate strongly that bank officials were complicit in these suspicious transactions. Available evidence makes clear that the bank management had, on a large scale, consistently evaded and ignored normal internal controls by allowing many irregular activities to occur. The transfers of funds to the United States and the United Kingdom were done in increments just below reporting thresholds of the receiving banks for large currency transactions, indicating a clear understanding of anti-money laundering controls.

The CBK Governor recommended in October 2006 that the Ministry of Finance revoke Charterhouse Bank's license so that CBK could liquidate the bank and compensate the innocent account holders. Charterhouse management and depositors filed numerous lawsuits to remove the statutory manager and reopen the bank. The Minister of Finance advised Charterhouse and the CBK that the Ministry would not renew the bank's license to operate after December 31, 2006. (Bank licenses are annual and expire automatically at the end of each year if not renewed.) Charterhouse's owners are expected to mount a legal challenge to the bank's closure.

The Charterhouse Bank investigations revealed the proceeds of large-scale evasion of import duties and taxes had been laundered through the banking system since at least 1999. In addition, the smuggled and/or under-invoiced goods may have been marketed through the normal wholesale and retail sectors. This case indicates that criminals have been taking advantage of Kenya's inadequate anti-money laundering regime for years by evading oversight and/or by paying off enforcement officials, other government officials, and politicians. There are strong indications that other Kenyan

banks are also involved in similar activities. Reportedly, Kenya's financial system may be laundering over $100 million each year. However, in 2006 there was not any reported money laundering related arrests, prosecutions, or convictions.

Kenya has not criminalized the financing of terrorism as required by the United Nations Security Council Resolution 1373 and the UN Convention for the Suppression of Financing of Terrorism, to which it is a party. In April 2003, the GOK introduced the Suppression of Terrorism Bill into Parliament. After objections from some public groups that the bill unfairly targeted the Muslim community and unduly restricted civil rights, the GOK withdrew the bill. The GOK redrafted the Anti-Terrorism Bill in 2006 to revise the rejected texts, but Muslim and human rights groups remain convinced the government could use it to commit human rights violations. The draft bill contains provisions that would strengthen the GOK's ability to combat terrorism; however, the GOK has yet to publish the bill or submit it to Parliament.

The CBK does not circulate the list of individuals and entities that have been included on the United Nations (UN) 1267 Sanctions Committee's consolidated list or the United States Office of Foreign Asset Control (OFAC) designated list to the financial institutions it regulates. Instead, it uses its bank inspection process to search for names on the OFAC list of designated people/entities. The CBK and the GOK have no authority to seize or freeze accounts without a court warrant. To date, the CBK has not notified the United States Government of any bank customers identified on the OFAC list.

All charitable and nonprofit organizations are required to register with the government and submit annual reports to the GOK's oversight body, the National Non-Governmental Organization Coordination Bureau. NGOs that are noncompliant with the annual reporting requirements can have their registrations revoked; however, such penalties are rarely imposed. The government revoked the registration of some NGOs with Islamic links in 1998 after the bombing of the U.S. Embassy in Nairobi, only to later re-register them. The Non-Governmental Organization Coordination Bureau lacks the capacity to monitor NGOs and it is suspected that charities and other nonprofit organizations handling millions of dollars are filing inaccurate or no annual reports. The Bureau plans to strengthen its capacity to review NGO registrations and annual reports for suspicious activities in 2007.

Drug trafficking-related asset seizure/forfeiture laws and their enforcement are weak and disjointed. Some underlying money laundering activities are criminalized under various Acts of Parliament. Apart from the seizure of intercepted drugs and narcotics, seizures of assets are rare. At present, the government entities responsible for tracing and seizing assets include the Central Bank of Kenya Banking Fraud Investigation Unit, the Kenya Police (through the Anti-Narcotics Unit and the Anti-Terrorism Police Unit), the Kenya Revenue Authority (KRA), and the Kenya Anti-Corruption Commission (KACC). Police must obtain a court warrant to demand bank account records or to seize an account. The police must present evidence linking the deposits to a criminal violation. This process is difficult to keep confidential, and as a result of leaks, serves to warn account holders of investigations. Account holders then move their accounts or contest the warrants. Although the KACC Director claimed that KACC had obtained court warrants to seize billions of shillings in 78 bank accounts belonging to corrupt politicians, businessmen and former senior civil servants in September 2006, no action was taken. There is currently no law specifically authorizing the seizure of the financial assets of terrorists.

Kenya is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. In the 2006 Transparency International Corruption Perceptions Index, Kenya is ranked 144 out of 163 countries measured. In 2004, Kenya acceded to the UN Convention against Transnational Organized Crime. Kenya is an active member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a Financial Action Task Force (FATF)-style regional body. Kenya has an informal arrangement with the United States for the

exchange of information regarding narcotics, terrorism financing, and other serious crime investigations. Kenya has cooperated with the United States and the United Kingdom, but lacks the institutional capacity, investigative skills, and equipment to conduct complex investigations independently.

Kenya is developing into a major money laundering country. The Government of Kenya should pass the proposed Proceeds of Crime and Anti-Money Laundering bill that includes the creation of a FIU. The Central Bank, law enforcement agencies, and the Ministry of Finance should work together more closely to enforce existing laws and regulations to combat money laundering, tax evasion, corruption, and smuggling. The Minister of Finance should revoke or refuse to renew the license of any bank found to have knowingly laundered money, and encourage the CBK to tighten its examinations and audits of banks.

Kenyan law enforcement and customs authorities should be trained to recognize and investigate trade-based money laundering methodologies and informal value transfer systems. Kenya should criminalize the financing of terrorism. Kenya should pass a law specifically authorizing the seizure of the financial assets of terrorists. Kenyan authorities should take steps to ensure that NGOs and suspect charities and nonprofit organizations follow international recognized norms regarding transparency and file complete and accurate annual reports.

## Korea, Democratic Peoples Republic of

*This is a reprint of last year's report as we have received no new information for 2006.*

For decades, citizens of the Democratic Peoples Republic of Korea (DPRK) have been apprehended trafficking in narcotics and engaged in other forms of criminal behavior, including passing counterfeit U.S. currency and trade in counterfeit products, such as cigarettes.

Substantial evidence exists that North Korean governmental entities and officials have laundered the proceeds of narcotics trafficking and have been engaged in counterfeit and other illegal activities through a network of front companies that use financial institutions in Macau for their operations. On September 20, the U.S. Department of Treasury designated Banco Delta Asia SARL in Macau as a "primary money laundering concern" under Section 311 of the USA PATRIOT Act. The Department of the Treasury noted that the bank "…has been a willing pawn for the North Korean Government to engage in corrupt financial activities through Macau." The Federal Register Notice designating the bank cited "the involvement of North Korean Government agencies and front companies in a wide variety of illegal activities, including drug trafficking and the counterfeiting of goods and currency" and noted that North Korea has been positively linked to nearly 50 drug seizures in 20 different countries since 1990, a significant number of which involved the arrest or detention of North Korean diplomats or officials.

In addition, indictments in the United States and the work of several corporate investigative teams employed by the holders of major United States and foreign cigarette and pharmaceutical trademarks have provided further compelling evidence of DPRK involvement in a wide range of criminal activities carried out in league with criminal organizations around the world, including trafficking in counterfeit branded items (cigarettes, Viagra), and high-quality counterfeit U.S. currency ("supernotes").

## Korea, Republic of

The Republic of Korea (ROK) has not been considered an attractive location for international financial crimes or terrorist financing due to foreign exchange controls, although these are gradually being phased out by 2009. Most money laundering appears to be associated with domestic criminal activity

or corruption and official bribery. Still, criminal groups based in South Korea maintain international associations with others involved in human and contraband smuggling and related organized crime. As law enforcement authorities have gained more expertise investigating money laundering and financial crimes, they have become more cognizant of the problem.

On the whole, the South Korean government has been a willing partner in the fight against financial crime, and has pursued international agreements toward that end. The Financial Transactions Reports Act (FTRA), passed in September 2001, requires financial institutions to report suspicious transactions to the Korea Financial Intelligence Unit (KoFIU), which operates within the Ministry of Finance and Economy. KoFIU was officially launched in November 2001, and is composed of 60 experts from various agencies, including the Ministry of Finance and Economy, the Justice Ministry, the Financial Supervisory Commission, the Bank of Korea, the National Tax Service, the National Police Agency, and the Korea Customs Service. KoFIU analyzes suspicious transaction reports (STRs) and forwards information deemed to require further investigation to the Public Prosecutor's office, and, as of 2006, also to the Korean police.

In 2006, the government implemented several measures to further strengthen its anti-money laundering regime by introducing mandatory currency transaction reporting (CTRs) for high-value cash transactions, on top of continued suspicious transaction reporting. Beginning in January 2006, financial institutions have been required to report within 24 hours all cash transactions of 50 million won ($49,213) or more by individuals to KoFIU. That reporting threshold will be lowered to 30 million won ($29,528) in 2008 and to 20 million won ($19,685) in 2010. Since January 2006, financial institutions have also been required to perform enhanced customer due diligence (CDD), thereby strengthening customer identification requirements set out in the Real Name Financial Transaction and Guarantee of Secrecy Act. Under the enhanced CDD guidelines, financial institutions must identify and verify customer identification data, including address and telephone numbers, when opening an account or conducting transactions of 20 million won ($19,685) or more.

The STR system was strengthened in 2004 with the introduction of a new online electronic reporting system and the lowering of the monetary threshold under which financial institutions must file STRs from 50 to 20 million won (from $49,213 to $19,685). Improper disclosure of financial reports is punishable by up to five years imprisonment and a fine of up to 30 million won ($29, 528). Between January 1, 2002, and June 30, 2006, KoFIU received a total of 30,544 STRs from financial institutions. The number of such cases has continued to climb noticeably each year, from 275 STRs in 2002, to 1,744 in 2003, 4,680 in 2004, and 13,459 in 2005. In the first half of 2006, there were 10,386 STRs submitted to KoFIU, a 10 percent increase over the same period in 2005. Since 2002 through the first half of 2006, KoFIU has analyzed 29,626 of these reports and provided 4,268 reports to law enforcement agencies, including the Public Prosecutor's Office (PPO), National Police Agency (NPA), National Tax Service (NTS), Korea Customs Service (KCS), and the Financial Supervisory Commission (FSC). Of the 4,268 cases referred to law enforcement agencies, investigations have been completed in 1,643 cases, with nearly half of those (806 cases) resulting in indictments and prosecution for money laundering.

In addition, KoFIU supervises and inspects the implementation of internal reporting systems established by financial institutions and is charged with coordinating the efforts of other government bodies. Officials charged with investigating money laundering and financial crimes are beginning to widen their scope to include crimes related to commodities trading and industrial smuggling, and continue to search for possible links of such illegal activities to international terrorist activity. In 2006, KoFIU continued to strengthen advanced anti-money laundering measures (such as the STR and CTR systems) to meet global standards such as Clause 5.8 of the Methodology for Assessing Compliance with the Financial Action Task Force (FATF) 40 Recommendations. KoFIU encouraged financial institutions including small-scale credit unions and cooperatives to adopt a differentiated risk-based

CDD system, focusing on types of customers and transactions, by offering them comprehensive training programs.

Money laundering controls are applied to nonbanking financial institutions, such as exchange houses, stock brokerages, casinos, insurance companies, merchant banks, mutual savings, finance companies, credit unions, credit cooperatives, trust companies, and securities companies. Following the late-2005 arrest of a Korean business executive charged with laundering 8.3 billion won ($8.17 million) to be used to bribe politicians and bureaucrats, KoFIU in 2006 began considering revisions to the Financial Transaction Reports Act to impose anti-money laundering obligations on casinos. Intermediaries such as lawyers, accountants, or broker/dealers are not covered by Korea's money laundering controls. Any traveler carrying more than $10,000 or the equivalent in other foreign currency is required to report the currency to the Korea Customs Service.

Money laundering related to narcotics trafficking has been criminalized since 1995, and financial institutions have been required to report transactions known to be connected to narcotics trafficking to the Public Prosecutor's Office since 1997. All financial transactions using anonymous, fictitious, and nominee names have been banned since the 1997 enactment of the Real Name Financial Transaction and Guarantee of Secrecy Act. The Act also requires that, apart from judicial requests for information, persons working in financial institutions are not to provide or reveal to others any information or data on the contents of financial transactions without receiving a written request or consent from the parties involved. However, secrecy laws do not apply when such information must be provided for submission to a court or as a result of a warrant issued by the judiciary.

In a move designed to broaden its anti-money laundering regime, the ROK also criminalized the laundering of the proceeds from 38 additional offenses, including economic crimes, bribery, organized crime, and illegal capital flight, through the Proceeds of Crime Act (POCA), enacted in September 2001. The POCA provides for imprisonment and/or a fine for anyone receiving, disguising, or disposing of criminal funds. The legislation also provides for confiscation and forfeiture of illegal proceeds.

South Korea still lacks specific legislation on terrorism financing. As of late 2006, two versions of a new counterterrorism bill are pending in Korea's unicameral legislature, the National Assembly. Previous attempts to pass similar bills have not succeeded. Many politicians and nongovernmental organizations (NGOs), recalling past civil rights abuses in Korea by former administrations, oppose the passage of counterterrorism legislation because of fears about possible misuse by the National Intelligence Service. The proposed legislation is crafted to allow the Korean Government additional latitude in fighting terrorism, though general financial crimes and money laundering have already been criminalized in previously enacted laws. The pending counterterrorism bill, if passed, would permit the government to seize legitimate businesses that support terrorist activity. Currently, under the special act against illicit drug trafficking and other related laws, legitimate businesses can be seized if they are used to launder drug money, but businesses supporting terrorist activity cannot be seized unless other crimes are committed. At this time, there are no known charitable or nonprofit entities operating in Korea that are used as conduits for the financing of terrorism.

Through KoFIU, the government circulates to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 and those listed by the European Union under relevant authorities. Korea implemented regulations on October 9, 2001, to freeze financial assets of Taliban-related authorities designated by the UN Security Council. The government then revised the regulations, agreeing to list immediately all U.S. Government-requested terrorist designations under U.S. Executive Order 13224 of December 12, 2002. No listed terrorists are known to be maintaining financial accounts in Korea at this time. Korean

banks have not identified any terrorist assets. There have been no cases of terrorism financing identified since January 1, 2002.

Korean government authorities continue to investigate the underground "hawala" system used primarily to send illegal remittances abroad by South Korea's approximately 30,000 foreigners from the Middle East as well as thousands of undocumented foreign workers (mainly ethnic Koreans from Mongolia, Uzbekistan, and Russia). Currently, gamblers who bet abroad often use alternative remittance and payment systems; however, government authorities have criminalized those activities through the Foreign Exchange Regulation Act and other laws. According to an October 2006 Korea Customs Service report, 1,159 hawala cases worth 5. 26 trillion won ($4.2 billion) were recorded in 2002; 1,311 cases amounting to 2.2 trillion won ($1.84 billion) in 2003; 1,917 cases totaling 3.66 trillion ($3.2 billion) in 2004, and 1,901 cases worth 3.56 trillion won ($3.47 billion) in 2005. The majority of early hawala cases were related to the U.S. through 2004, but in 2005 the bulk of cases involved Japan (45 percent or $1.56 billion), followed by the U.S. (25 percent or $867 million) and the PRC (19 percent or $674 million).

South Korea actively cooperates with the United States and other countries to trace and seize assets. The Anti-Public Corruption Forfeiture Act of 1994 provides for the forfeiture of the proceeds of assets derived from corruption. In November 2001, Korea established a system for identifying, tracing, freezing, seizing, and forfeiting narcotics-related and/or other assets of serious crimes. Under the system, KoFIU is responsible for analyzing and providing information on STRs that require further investigation. The Bank Account Tracing Team under the Narcotics Investigation Department of the Seoul District Prosecutor's Office (established in April 2002) is responsible for tracing and seizing drug-related assets. The Korean Government established six additional new bank account tracking teams in 2004 to serve out of the District Prosecutor's offices in the metropolitan cities of Busan, Daegu, Kwangju, Incheon, Daejon, and Ulsan, to expand its reach. Its legal framework does not allow civil forfeiture.

Korea continues to address the problem of the transportation of counterfeit international currency. The Bank of Korea reported that through September 2006, there were 371 reported cases of counterfeit dollars worth $36,450, compared to 1060 cases of $105,440 worth in the first nine months of 2005. Bank experts confirm that the amount of forged U.S. currency is on a sharp decline, reflecting local bank findings that the number of counterfeit $100 notes found during the first nine months of 2006 - about $36,100-fell to about one third of that found in the same period of 2005. In April 2005, the local press reported that police arrested a Korean who had smuggled $140,000 in $100 "supernotes" from China-a record amount for South Korea. However, no similar incidents were reported as of late 2006.

South Korea has a number of free economic zones (FEZs) that enjoy certain tax privileges. However, companies operating within them are subject to the same general laws on financial transactions as companies operating elsewhere, and there is no indication these FEZs are being used in trade-based money laundering schemes or for terrorist financing. Korea mandates extensive entrance screening to determine companies' eligibility to participate in FEZ areas, and firms are subject to standard disclosure rules and criminal laws. As of November 2006, Korea had seven FEZs, as a result of the June 2004 recategorization of the three port cities of Busan, Incheon, and Kwangyang as FEZs. They were recategorized from their previous designation of "customs-free areas" in order to avoid confusion from the earlier dual system of production-focused FEZs, and logistics-oriented "customs-free zones." Incheon International Airport is slated to become the eighth FEZ.

Korea is a party to the 1988 UN Drug Convention and, in December 2000, signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. Korea is a party to the UN International Convention for Suppression of the Financing of Terrorism. The ROK also signed in

December 2003, but has not ratified, the UN Convention against Corruption. Korea is an active member of the Asia/Pacific Group on Money Laundering (APG), and in 2004 hosted the APG annual

meeting. Korea also became a member of the Egmont Group in 2002. In August, 2006, the FATF invited Korea to become an Observer to the organization- the first step in gaining full membership. An extradition treaty between the United States and the ROK entered into force in December 1999. The United States and the ROK cooperate in judicial matters under a Mutual Legal Assistance Treaty, which entered into force in 1997. In addition, the FIU continues to actively pursue information-sharing agreements with a number of countries, and had signed memoranda of understanding with 31 countries/jurisdictions-the latest being Hong Kong-in November 2006.

The Government of the Republic of Korea should criminalize the financing and support of terrorism and should continue to move forward to adopt and implement its pending legislation. Among other priorities, the government should extend its anti-money laundering regime to nonfinancial institutions such as casinos and informal lending mechanisms widely recognized as potential blind spots. Just as importantly, the Republic of Korea should continue its policy of active participation in international anti-money laundering efforts, both bilaterally and in multilateral fora. Spurred by enhanced local and international concern, Korean law enforcement officials and policymakers now understand the potential negative impact of such activity on their country, and have begun to take steps to combat its growth. Their efforts will become increasingly important due to the rapid growth and greater integration of Korea's financial sector into the world economy.

## Kuwait

Kuwait continues to experience unprecedented economic growth that is enhancing the country's regional financial influence. Money laundering is not believed to be a significant problem, and reportedly that which does take place is generated largely as revenues from drug and alcohol smuggling into the country and the sale of counterfeit goods. The potential for the financing of terrorism through the misuse of charities continues to be a concern.

Kuwait has ten private local commercial banks, including two Islamic banks, all of which provide traditional banking services comparable to Western-style commercial banks. Kuwait also has two specialized banks, the Kuwait Real Estate Bank (KREB), which is in the process of converting to an Islamic bank, and the government-owned Industrial Bank of Kuwait. Both of these banks provide medium and long-term financing. With the conversion of KREB, there will be three Islamic banks, including the Kuwait Finance House (KFH) and Boubyan Islamic Bank.

The Kuwaiti banking sector opened to foreign competition under the 2001 Direct Foreign Investment Law, and the Central Bank of Kuwait (CB) has already granted licenses to four foreign banks: BNP Paribas, HSBC, Citibank, and the National Bank of Abu Dhabi; at present, the National Bank of Abu Dhabi has a license but no office in Kuwait. However, while foreign banks may now operate in Kuwait, they are only allowed to open one branch.

On March 10, 2002, the Emir (Head of State) of Kuwait signed Law No. 35/2002, commonly referred to as Law No. 35, which criminalized money laundering. Law 35 does not specifically cite terrorist financing as a crime. The law stipulates that banks and financial institutions may not keep or open anonymous accounts or accounts in fictitious or symbolic names, and that banks must require proper identification of both regular and occasional clients. The law also requires banks to keep all records of transactions and customer identification information for a minimum of five years, conduct anti-money laundering and terrorist financing training to all levels of employees, and establish proper internal control systems.

Law No. 35 also requires banks to report suspicious transactions to the Office of Public Prosecution (OPP). The OPP is the sole authority that has been designated by law to receive suspicious transaction reports (STRs) and to take appropriate action on money laundering operations. Reports of suspicious transactions are then referred to the CB for analysis. The anti-money laundering law provides for a

penalty of up to seven years' imprisonment in addition to fines and asset confiscation. The penalty is doubled if an organized group commits the crime, or if the offender took advantage of his influence or his professional position. Moreover, banks and financial institutions may face a steep fine (approximately $3.3 million) if found in violation of the law.

The law includes articles on international cooperation and the monitoring of cash and precious metals transactions. Currency smuggling into Kuwait is also outlawed under Law No. 35, although cash reporting requirements are not uniformly enforced at ports of entry. Provisions of Article 4 of Law No. 35 require travelers to disclose to the customs authorities, upon entering the country, of any national or foreign currency, gold bullion, or other precious materials in their possession valued in excess of 3,000 Kuwaiti dinars (approximately $10,000). However, the law does not require individuals to file declaration forms when carrying cash or precious metals out of Kuwait. Several cases have been opened under Law No. 35, but only two cases have gone to court. The cases reportedly involved money smuggling and failure to report currency transactions, and did not involve banks.

The National Committee for Anti-Money Laundering and the Combating of Terrorist Financing is responsible for administering Kuwait's AML/CTF regime. In April 2004, the Ministry of Finance issued Ministerial Decision No. 11 (MD No. 11/224), which transferred the chairmanship of the National Committee, formerly headed by the Minister of Finance, to the Governor of the Central Bank of Kuwait. The Committee is comprised of representatives from the Ministries of Interior, Foreign Affairs, Commerce and Industry, Finance, and Labor and Social Affairs; the Office of Public Prosecution; the Kuwait Stock Exchange; the General Customs Authority; the Union of Kuwaiti Banks; and CB.

Since its inception, the National Committee has pursued its mandate of drawing up the country's strategy and policy with regard to anti-money laundering and terrorist financing; drafting the necessary legislation and amendments to Law No. 35, along with pertinent regulations; coordinating between the concerned ministries and agencies in matters related to combating money laundering and terrorist financing; following up on domestic, regional, and international developments and making needed recommendations in this regard; setting up appropriate channels of communication with regional and international institutions and organizations; and representing Kuwait in domestic, regional, and international meetings and conferences. In addition, the Chairman is entrusted with issuing regulations and procedures that he deems appropriate for the Committee's duties, responsibilities, and organization of its activities.

Kuwait, however, has been unable to implement fully its current anti-money laundering law due in part to structural inconsistencies within the law itself. Kuwait's Financial Intelligence Unit is not an independent body in accordance with the current international standards, but rather is under the direct supervision of the Central Bank of Kuwait. In addition, vague delineations of the roles and responsibilities of the government entities involved continue to hinder the overall effectiveness of Kuwait's anti-money laundering regime. Cognizant of these shortcomings, the National Committee is currently drafting a revision of Law No. 35 that would bring Kuwait into compliance with international standards, and would criminalize terrorist financing.

In addition to Law No. 35, anti-money laundering reporting requirements and other rules are contained in CB instructions No. (2/sb/92/2002), which took effect on December 1, 2002, superseding instructions No. (2/sb/50/97). The revised instructions provide for, *inter alia*, customer identification and the prohibition of anonymous or fictitious accounts (Articles 1-5); the requirement to keep records of all banking transactions for five years (Article 7); electronic transactions (Article 8); the requirement to investigate transactions that are unusually large or have no apparent economic or lawful purpose (Article 10); the requirement to establish internal controls and policies to combat money laundering and terrorism finance, including the establishment of internal units to oversee compliance with relevant regulations (Article 14 and 15); and the requirement to report to the CB all

cash transactions in excess of $10,000 (Article 20). In addition, the CB distributed detailed instructions and guidelines to help bank employees identify suspicious transactions. At the Central Bank's instructions, banks are no longer required to block assets for 48 hours on suspected accounts in an effort to avoid "tipping off" suspected accountholders. The Central Bank, upon notification from the Ministry of Foreign Affairs (MFA), issues circulars to units subject to supervision requiring them to freeze the assets of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list. Financial entities are instructed to freeze any such assets immediately and for an indefinite period of time, pending further instructions from the Central Bank, which in turn receives its designation guidance from the MFA.

On June 23, 2003, the CB issued Resolution No. 1/191/2003, establishing the Kuwaiti Financial Inquiries Unit as an independent financial intelligence unit (FIU) within the Central Bank. The FIU is comprised of seven part-time CB officials and headed by the Central Bank Governor. The responsibilities of the FIU are to receive and analyze reports of suspected money laundering activities from the OPP, establish a database of suspicious transactions, conduct anti-money laundering training, and carry out domestic and international exchanges of information in cooperation with the OPP. Although the FIU should act as the country's financial intelligence unit, Law No. 35/2002 did not mandate the FIU to act as the central or sole unit for the receipt, analysis, and dissemination of STRs; instead, these functions were divided between the FIU and OPP.

Banks in Kuwait are required to file STRs with the OPP, rather than directly with the FIU. However, based on an MOU with the Central Bank, STRs are referred from the OPP to the FIU for analysis. The FIU conducts analysis and reports any findings to the OPP for the initiation of a criminal case, if necessary. The FIU's access to information is limited, due to its inability to share information abroad without prior approval from the OPP. Reportedly, Kuwaiti officials agree that the current limits on information sharing by the FIU will have to be addressed by amending the law, which is currently under revision by the National Committee.

There are about 130 money exchange businesses (MEBs) operating in Kuwait that are authorized to exchange foreign currency only. None of these MEBs are formal financial institutions, and therefore are under the supervision of the Ministry of Commerce and Industry (MOCI) rather than the Central Bank. The CB has reached an agreement that tasks the MOCI with the enforcement of all anti-money laundering (AML) laws and regulations in supervising such businesses. Furthermore, MOCI will work diligently to encourage MEBs to apply for and obtain company licenses, and to register with the CB.

The MOCI's Office of Combating Money Laundering Operations was established in 2003, and supervises approximately 2,500 insurance agents, brokers and companies; investment companies; exchange bureaus; jewelry establishments (including gold, metal and other precious commodity traders); brokers in the Kuwait Stock Exchange; and other financial brokers. All new companies seeking a business license are required to receive AML awareness training from the MOCI before a license is granted. These firms must abide by all regulations concerning customer identification, record keeping of all transactions for five years, establishment of internal control systems, and the reporting of suspicious transactions. MOCI conducts both mandatory follow-up visits and unannounced inspections to ensure continued compliance. The Office of Combating Money Laundering Operations is also actively engaged in a public awareness campaign to increase understanding about the dangers of money laundering.

Businesses that are found to be in violation of the provisions of Law No. 35/2002 receive an official warning from MOCI for the first offense. The second and third violations result in closure for two weeks and one month respectively. The fourth violation results in revocation of the license and closure of the business. Reportedly, three exchange houses were closed in 2005: one for operating without a license, and the other two for violating MOCI's instructions.

In August 2002, the Kuwaiti Ministry of Social Affairs and Labor (MOSAL) issued a ministerial decree creating the Department of Charitable Organizations (DCO). The primary responsibilities of the new department are to receive applications for registration from charitable organizations, monitor their operations, and establish a new accounting system to insure that such organizations comply with the law both at home and abroad. The DCO has established guidelines for charities explaining donation collection procedures and regulating financial activities. The DCO is also charged with conducting periodic inspections to ensure that charities maintain administrative, accounting, and organizational standards according to Kuwaiti law. The DCO mandates the certification of charities' financial activities by external auditors, and limits the ability to transfer funds abroad only to select charities approved by MOSAL. MOSAL also requires all transfers of funds abroad to be made between authorized charity officials. Banks and money exchange businesses (MEBs) are not allowed to transfer any charitable funds outside of Kuwait without prior permission from MOSAL. In addition, any such wire transactions must be reported to the CB, which maintains a monthly database of all transactions conducted by charities. Unauthorized public donations, including Zakat (alms) collections in mosques, are also prohibited.

In 2005, the MOSAL introduced a pilot program requiring charities to raise donations through the sale of government-provided coupons during the Muslim holy-month of Ramadan. MOSAL continued this program in 2006, and plans are underway to encourage the electronic collection of funds using a combination of electronic kiosks, hand-held collection machines, and text messaging. These devices will generate an electronic record of the funds collected, which will then be subject to MOSAL supervision.

Kuwait is a member of the Gulf Cooperation Council (GCC), which is itself a member of the Financial Action Task Force (FATF). In November 2004, Kuwait signed the memorandum of understanding governing the establishment of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body. Kuwait has played an active role in the MENAFATF through its participation in the drafting of regulations and guidelines pertaining to charities oversight and cash couriers. In December 2005, the CB hosted a training seminar for mutual evaluation assessors of MENAFATF members.

Kuwait is a party to the 1988 UN Drug Convention. In May 2006, Kuwait ratified the UN Convention against Transnational Organized Crime. It has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Kuwait should significantly accelerate its ongoing efforts to revise Law No. 35/2002 to criminalize terrorist financing; strengthen charity oversight; develop an independent Financial Intelligence Unit that meets international standards including the sharing of information with foreign FIUs; and improve international information sharing, as well as sharing between the government and financial institutions. Kuwait should implement and enforce a uniform cash declaration policy for inbound and outbound travelers. Kuwait, like many other countries in the Gulf, relies on STRs to initiate money laundering investigations. Rather, Kuwaiti law enforcement and customs authorities should be more active in identifying suspect behavior that could be indicative of money laundering, such as underground financial systems. Kuwait should become a party to both the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism.

## Laos

Laos is on the fringe of mainland Southeast Asia's banking network. Laos is neither an important regional financial center, nor an offshore financial center, nor is it considered significant in terms of money laundering However, illegal timber sales, corruption, cross-border smuggling of goods, and illicit proceeds from the methamphetamine (ATS) known

locally as "ya ba" (crazy medicine), and domestic crime are sources of laundered funds. The Lao banking sector is dominated by state-owned commercial banks in need of extensive reform. The small scale and poor financial condition of Lao banks may make them more likely to be venues for certain kinds of illicit transactions. These banks are not optimal for moving large amounts of money in any single transaction, due to the visibility of such movements in a small, low-tech environment. Reportedly, there is no notable increase in financial crime. While there is smuggling of consumer goods across the Mekong, this is not generally associated with money laundering. Rather, it is an easy way to avoid paying custom's duties and the inconvenience of driving across the bridge between Vientiane and Thailand. A special economic zone exists in the south. It is not considered particularly successful and there is no indication it is currently used to launder money or finance terrorism.

Money laundering is a criminal offense in Laos and covered in at least two separate decrees. The penal code contains a provision adopted in November 2005 that criminalizes money laundering and provides sentencing guidelines. In March of 2006, the Prime Minister's Office issued a detailed decree on anti-money laundering, based on a model law provided by the Asian Development Bank. Because of the unique nature of Lao governance, the decree is roughly equivalent to a law and is much easier to change than a law passed by the National Assembly. One provision of the decree criminalizes money laundering in relation to all crimes with a prison sentence of a year or more. In addition, the decree specifically criminalizes money laundering with respect to: terrorism; financing of terrorism; human trafficking and smuggling; sexual exploitation; human exportation or illegal migration; the production, sales, and possession of narcotic drugs; illicit arms and dynamite trafficking; concealment and trafficking of people's property; corruption; the receipt and giving of bribes; swindling; embezzlement; robbery; property theft; counterfeiting money and its use; murder and grievous bodily injury; illegal apprehension and detention; violation of state tax rules and regulations; extortion; as well as check forgery and the illicit use of false checks, bonds, and other financial instruments.

The current Financial Intelligence Unit, a committee located within the Bank of Laos, was established in 2004 and supervises financial institutions for their compliance with anti-money laundering/counter terrorist financing decrees and regulations. The Bank of Laos expects that this committee will be replaced by an operational unit with dedicated staff by early 2007. The FIU has no criminal investigative responsibilities, and is currently working with partner commercial banks to develop a standardized suspicious transaction report (STR). The bank estimates STRs will begin in 2007. There were none in 2006, nor were there any arrests for terrorist financing or money laundering. A revision to the penal law in November 2005 includes Article 58/2 which makes financing terrorism punishable by fines of 10 to 50 million Kip (approximately $10,000-$50,000,), prison sentences from 10 to 20 years, and includes the death penalty. The Bank of Laos has circulated lists of individuals and entities on the UN 1267 sanction's coordinated list.

Lao law prohibits the export of the national currency, the Kip. It is likely that the currency restrictions and undeveloped banking sector encourage the use of alternative remittance systems. When carrying cash across international borders, Laos requires a declaration for amounts over $2000. Cash must be declared when brought into the country and when departing. Failure to show declaration of incoming cash when exporting could lead to seizure

of the money or a fine. The Prime Minister's decree on money laundering specifically authorizes asset seizures when connected to money laundering and related crimes. The authority is broadly worded. It is not clear which government authority has responsibility for asset seizures, although indications are that the Ministry of Justice would take the lead. The Lao continue to build a framework of law and institutions; however, at this stage of development, enforcement of enacted legislation and decrees is weak.

Laos' decree on money laundering authorizes the government to cooperate with foreign governments to deter money laundering of any sort, with caveats for the protection of national security and sovereignty. There are no specific agreements with the United States relating to money laundering.

The GOL is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. The GOL participates in Association of Southeast Asian Nations (ASEAN) regional conferences on money laundering. Laos also has observer status in the Asia Pacific Anti-Money Laundering Group, and plans to join in 2007. In order to comport with international standards, the Government of Laos should enact comprehensive anti-money laundering legislation, as decrees are not recognized by international organizations as the force of law. Laos should become a party to the UN Convention for the Suppression of Financing of Terrorism and ratify the UN Convention against Corruption.

## Latvia

Latvia is a growing regional financial center that has a large number of commercial banks with a sizeable nonresident deposit base. Sources of laundered money in Latvia primarily involve tax evasion, but also include counterfeiting, corruption, white-collar crime, extortion, financial/banking crimes, stolen cars, contraband smuggling, and prostitution. Casinos provide another source of laundered money. A significant amount of the proceeds of tax evasion are believed to originate from outside of Latvia. A portion of domestically-obtained criminal proceeds is thought to be derived from organized crime. Reportedly, Russian organized crime is active in Latvia. State Narcotics Police have reportedly not found a significant link between smuggled goods on the black market and narcotics proceeds. Although currency transactions involving international narcotics trafficking proceeds do not include significant amounts of United States currency and apparently do not derive from illegal drug sales in the United States, there are ties between U.S.-derived drug money and the Latvian financial sector, and criminals have reportedly set up shell companies to launder drug money though the country.

Latvia currently is not considered to be an offshore financial center. Four special economic zones exist in Latvia providing a variety of significant tax incentives for the manufacturing, outsourcing, logistics centers, and trans-shipment of goods to other free trade zones. These zones are located at the free ports of Ventspils, Riga, and Liepaja, and in the inland city of Rezekne near the Russian and Belarusian Borders. Though there have been instances of reported cigarette smuggling to and from warehouses in the free trade zones, there have been no confirmed cases of the zones being used for money laundering schemes or by the financiers of terrorism. Latvia's Financial and Capital Market Commission states that the zones are covered by the same regulatory oversight and enterprise registration regulations that exist for nonzone areas.

The Government of Latvia (GOL) criminalized money laundering for all serious crimes in 1998. Latvia's anti-money laundering (AML) law, the Law on the Prevention of Laundering of Proceeds Derived from Criminal Activity, requires all institutions engaging in financial transactions to report suspicious activity to the financial intelligence unit (FIU). The legislation institutes customer

identification and record keeping requirements, as well as mandates the reporting of large cash transactions to the FIU. On February 1, 2004, Latvia adopted amendments to the AML law that expand the scope of reporting institutions to include auditors, lawyers, and high-value dealers, as well as credit institutions. The law lists four categories of entities obligated to report suspicious activities: participants in financial and capital markets (credit institutions, insurance companies, private pension funds, stock exchanges, brokerage companies, investment companies, credit unions, and investment consultants); organizers and holders of lotteries and gambling enterprises; companies engaged in foreign currency exchange; and individuals and companies who perform professional activities and services associated with financial transactions (money transfer services, tax consultants, auditors, auditing companies, notaries, attorneys, real estate companies, art dealers, and commodities traders). Another 2004 amendment provides for the inclusion of all offenses listed in the criminal law, including terrorism, as predicate offenses for money laundering. The amendments also provide the FIU with authority to block transactions for 45 days.

In addition to suspicious transactions, the law also mandates institutions to report unusual transactions to the FIU. Financial institutions receive a list of indicators that, when present, activate the reporting requirement for a financial institution. Many of the indicators are similar to those used to ascertain suspicious activities, and financial institutions are reportedly often uncertain which report is required to be filed. Most financial institutions rely on the list of indicators rather than evaluating transactions for suspicious activity. There is also a currency reporting requirement: obligated entities must report cash transactions, whether one large or several smaller, if the amount is equal to or exceeds 40,000 lats (approximately $73,000). Reporting is also required if, due to indicators that suggest unusual transactions, there is cause for suspicion regarding laundering or attempted laundering of the proceeds from crime. Financial institutions must keep transaction and identification data for at least five years after ending a business relationship with a client. If money laundering or terrorist financing is suspected, financial institutions have the ability to freeze accounts. If a financial institution finds the activity of an account questionable, it may close the account on its own initiative. Negligent money laundering is illegal in Latvia.

In January 2005, the Council of Ministers adopted Regulation 55 that created a Council for the Prevention of Laundering of Proceeds Derived from Criminal Activity, a state-level AML body chaired by the Prime Minister. In April 2005, Latvia criminalized the misrepresentation of the beneficial owner. In May 2005, additional amendments to the AML and the criminal law were adopted that significantly enhanced the ability of Latvian law enforcement agencies to share information with one another and with Latvia's banking regulator, the Financial and Capital Markets Commission (FCMC). In 2005, Latvia also passed a new Criminal Procedures Law, which removed many procedural hurdles that had served as obstacles to law enforcement agencies when they attempted to aggressively investigate and prosecute financial crimes. For example, prosecutors no longer need to prove willful blindness of the criminal origin of funds before charging a person or institution with a financial crime.

In November 2005, Latvia passed legislation instituting a cross-border currency declaration requirement, which took effect on July 1, 2006. The law stipulates that all persons transporting more than 10,000 euros (approximately $12,787) in cash or monetary instruments into or out of Latvia, with the exception of into or out of other European Union member states, is obligated to declare the money to a customs officer, or, where there is no customs checkpoint, to a Border Guard. Because Latvia is part of the customs territory of the EU, people moving within the EU are not required to declare. Completing a declaration is mandatory for all who are transferring between Latvia and territory outside of the EU who have the requisite amount of cash or monetary instruments. Declarations are shared between Latvian government agencies.

Banks are not allowed to open accounts without conducting customer due diligence and obtaining client identification documents for both residents and nonresidents. When conducting due diligence on

legal entities, banks must collect additional information on incorporation and registration. In June 2005, the GOL increased sanctions against banks for noncompliance, providing for fines up to $176,000. Latvia does not have secrecy laws that prevent the disclosure of client and ownership information to bank supervisors or law enforcement officers. Reporting individuals are protected by safe harbor provisions in the law.

Since July 2001, the Finance and Capital Market Commission (FCMC) has served as the GOL's unified public financial services regulator, overseeing commercial banks and nonbank financial institutions, the Riga Stock Exchange, and insurance companies. The Bank of Latvia supervises the currency exchange sector. The FCMC conducts regular audits of credit institutions and applies sanctions to companies that fail to file mandatory reports of unusual transactions. The FIU also works to ensure accurate reporting by determining if it has received corresponding STRs when suspicious transactions occur between Latvian banks.

The FCMC has distributed regulations for customer identification and detecting unusual and suspicious transactions, as well as regulations regarding internal control mechanisms that financial institutions should have in place. The May 2005 amendments to the AML law gave the FCMC the authority to share information with Latvian law enforcement agencies and receive data on potential financial crime patterns uncovered by police or prosecutors. The June 2005 amendments to the Criminal Procedures Law added an article criminalizing the deliberate provision of false information about a beneficiary to a credit or a financial institution.

In addition to the legislative and regulatory requirements in place, the Association of Latvian Commercial Banks (ALCB) plays an active role in setting standards on AML issues for Latvian banks. In May 2004, the ALCB adopted the regulations on the Prevention of Money Laundering as guidance. Under the leadership of the ALCB and at the urging of the FCMC, Latvian banks collectively reviewed existing customer relationships in the first half of 2005, which resulted in the closure of more than 100,000 accounts connected to customers unwilling or unable to comply with the enhanced due diligence requirements. In June 2005, the ALCB adopted a Declaration on Taking Aggressive Action against Money Laundering, which was signed by all Latvian banks. In 2005, the ACLB also adopted a voluntary measure, which all of the banks observed, to limit cash withdrawals from automated teller machines to 1,000 lats (approximately $1,834) per day. Member banks respect the ACLB guidelines. In addition to acting as an industry representative to government and the regulator, the ACLB organizes regular education courses on anti-money laundering/ counter terrorism financing (AML/CTF) issues for bank employees.

The Office for the Prevention of the Laundering of Proceeds Derived from Criminal Activity, known as the Control Service, is Latvia's FIU. Although it is part of the Latvian Prosecutor General's Office, its budget is separate. The Control Service the overall responsibility for coordination, application and assessment of Latvia's AML policy and its effectiveness. During 2006, the Control Service received more than 27,000 reports of suspicious and unusual transactions. The Control Service received 26,302 reports in 2005 and 16,479 reports in 2004. Approximately 53 percent of the reports received in 2005 and 2006 were for suspicious transactions and 47 percent were classified as unusual transactions.

The Control Service conducts a preliminary investigation of the suspicious and unusual reports and then may forward the information to law enforcement authorities that investigate money laundering cases. The Control Service can disseminate case information to a specialized Anti-Money Laundering Investigation Unit of the State Police; the Economic Police; and the Office for the Combat of Organized Crime. The FIU can also disseminate information to the Financial Police (under the State Revenue Service of the Ministry of Finance); the Bureau for the Prevention and Combat of Corruption (Anti-Corruption Bureau, ACB) for crimes committed by public officials; the Security Police (for cases concerning terrorism and terrorism financing); and other law enforcement authorities.

The Control Service has access to all state and municipal databases. It does not have direct access to the databases of financial institutions, but requests data as needed. The Control Service shares data with other FIUs and has cooperation agreements on information exchange with FIUs in thirteen countries. Latvia has also signed multilateral agreements with several EU countries to automatically exchange information with the EU financial intelligence units using FIU.NET.

The Prosecutor General's Office maintains a staff of seven prosecutors to prosecute cases linked to money laundering. The individuals comprising the staff have been subjected to a special clearance process. In the first eight months of 2006, the Prosecutor General's Office received nine new money laundering cases for prosecution; of these, it referred six cases to court for the criminal offense of money laundering. Three individuals received convictions, and sentences including time in jail, in two cases.

The adoption of Latvia's new Criminal Procedures Law in 2005 provided additional measures for the seizure and forfeiture of assets. The law allows law enforcement authorities to better identify, trace, and confiscate criminal proceeds. Investigators have the ability to initiate an action for the seizure of assets recovered during a criminal investigation concurrently with the investigation itself (previously this was possible only when the investigation was complete).

In 2006, the Latvian FIU issued 125 orders to freeze assets, freezing a total of 12,645,000 Lats (approximately $23.5 million). Proceeds from any seizures or forfeitures pass to the State budget. Latvia's FIU reports that cooperation from the banking community to trace and freeze assets has been excellent.

The GOL has initiated a number of measures aimed at combating the financing of terrorism. It has issued regulations to implement the sanctions imposed by United Nations Security Council Resolution (UNSCR) 1267. The regulations require that financial institutions report to the Control Service transactions related to any suspected terrorists or terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list or on other terrorist lists, including those shared with Latvia by international partners. The Control Service maintains consolidated terrorist finance and watch-lists and regularly sends these to financial and nonfinancial institutions, as well as to their supervisory bodies. On several occasions, Latvian financial institutions have temporarily frozen monetary funds associated with names on terrorist finance watch lists, including those issued by the U.S. Office of Foreign Assets Control (OFAC), although authorities have found no confirmed matches to names on the list. Article 17 of the AML law authorizes the Control Service to freeze the funds of persons included on one of the terrorist lists for up to six months. Freezing of terrorist assets falls under the same mechanism as with other crimes, but includes involvement by the Latvian Security Police. Any associated investigations, asset or property seizures, and forfeitures are handled in accordance with the new Criminal Procedures Law. On June 1, 2005, Latvia amended its Criminal Law supplementing it with a new Article 88-1 that specifically criminalizes the financing of terrorism, meeting the requirements of UNSCR 1373.

Latvia took swift action to improve its AML/CTF regime after the United States outlined concerns in a Notices of Proposed Rulemaking against two Latvian banks on April 26, 2005, under Section 311 of the USA PATRIOT Act. Reportedly, there are some concerns regarding the willingness of the banking sector to comply with the government, as evidenced by the banking sector's response to the 2005 action. The United States issued a final rule imposing a special measure against only one of the two banks, VEF Banka, as a financial institution of primary money laundering concern, on August 14, 2006.

Only conventional money remitters (such as Western Union and Moneygram) are permitted in Latvia. The remitters work through the banks and not as separate entities. Alternative remittance services are reportedly prohibited in Latvia. The Control Service has not detected any cases of charitable or nonprofit entities used as conduits for terrorism financing in Latvia.

Latvia is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). Latvia underwent a joint International Monetary Fund (IMF)/MONEYVAL evaluation in March 2006 which assessed the country's AML regulatory and legal framework. This assessment was approved as MONEYVAL's third-round evaluation of Latvia in September 2006. The Control Service is a member of the Egmont Group and has agreements on information exchange with sixteen counterpart FIUs.

Latvia is a party to the UN International Convention for the Suppression of the Financing of Terrorism and eleven other multilateral counterterrorism conventions. Latvia is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. A Mutual Legal Assistance Treaty (MLAT) has been in force between the United States and Latvia since 1999.

The GOL should enact additional amendments to its legislation to tighten its AML framework. It should continue to implement and make full use of the 2005 amendments to its AML law and Criminal Procedures Law, taking steps to increase information sharing and cooperation between law enforcement agencies at the working level. The GOL should lower the threshold for the reporting of currency transactions. The GOL should also strengthen its ability to aggressively prosecute and convict those involved in financial crimes. Latvian authorities should also clarify the distinction between unusual transaction reports and suspicious transaction reports in its guidance to the obliged entities.

## Lebanon

Lebanon is a financial hub for banking activities in the Middle East and eastern Mediterranean. It has one of the more sophisticated banking sectors in the region. The banking sector continues to record an increase in deposits. As of September 2006, there were 63 banks (54 commercial banks and nine investment banks) operating in Lebanon with total deposits of $59.7 billion. Four U.S. banks and bank representative offices operate in Lebanon: Citibank, American Express Bank, the Bank of New York, and JP Morgan Chase Bank.

The Central Bank (Banque du Liban) (CBL) regulates all financial institutions and money exchange houses. Banking sources emphasize their belief that Lebanon is not a significant financial center for money laundering, but acknowledge that it does have a number of vulnerabilities. Lebanon imposes no controls on the movement of capital. It has a substantial influx of remittances from expatriate workers and family members, estimated by banking sources to reach $3.5-4 billion yearly.

Laundered criminal proceeds come primarily from domestic criminal activity. Money laundering proceeds are largely controlled by organized crime. During 2006, the banking sector has seen two cases of bank fraud consisting of embezzlement by bank employees in branch offices and one case of fraud by a money dealer. There is some smuggling of cigarettes and pirated software, but this does not generate large amounts of funds that are laundered through the banking system. There is a black market for counterfeit goods and pirated software, CDs, and DVDs. Lebanese customs officials have had some recent success in combating counterfeit and pirated goods. The illicit narcotics trade is not a principal source of money laundering proceeds.

Offshore banking is not permitted in Lebanon, nor are offshore trusts or offshore insurance companies. Legislative Decree No. 46, dated June 1983, governs offshore companies. It restricts offshore companies' activity to negotiating and signing agreements concerning business conducted outside of Lebanon or in the Lebanese Customs Free Zone; thus, offshore companies are barred from engaging in activities such as industry, banking, and insurance. All offshore companies must register with the Beirut Commercial Registry, and the owners of an offshore company must submit a copy of their identification. Moreover, the Registrar of the Beirut Court keeps a special register, in which all

information about the offshore company is retained. A draft law amending legislation on offshore companies to make it WTO compliant was still pending in Parliament as of early November 2006.

There are currently two free trade zones operating in Lebanon, at the Port of Beirut and at the Port of Tripoli. The free trade zones fall under the supervision of Customs. Exporters moving goods into and out of the free zones submit a detailed manifest to Customs. If Customs suspects trade-based money laundering or terrorism finance, it reports it to Lebanon's financial intelligence unit (FIU), the Special Investigation Commission (SIC). Companies using the free trade zone must be registered and must submit appropriate documentation, which is kept on file for a minimum of five years. Lebanon has no cross-border currency reporting requirements. However, since January 2003, Customs checks travelers randomly and notifies the SIC when large amounts of cash are found.

In 2004, Lebanon passed a law requiring diamond traders to seek proper certification of origin for imported diamonds; the Ministry of Economy and Trade is in charge of issuing certification for re-exported diamonds. This law was designed to prevent the traffic in conflict diamonds, and allowed Lebanon to join the Kimberley Process on September 20, 2005. In August 2003, Lebanon passed a decree prohibiting imports of rough diamonds from countries that are not members of the Kimberley Process. However, in 2005, investigations by Global Witness, a nongovernmental organization, discovered that according to Lebanese customs data, Lebanon imported rough diamonds worth $156 million from the Republic of Congo (ROC), a country removed from the Kimberley Process Certification Scheme for having a "massive discrepancy" between its actual diamond production and declared exports. This documented example of suspect imports from the ROC throw serious doubts on Lebanon's commitment to counter the trade in conflict diamonds. Moreover, there have been consistent reports that many Lebanese diamond brokers in Africa are engaged in the laundering of diamonds—the most condensed form of physical wealth in the world.

Lebanon has a large expatriate community that is found throughout the Middle East, Africa, and parts of Latin America. They often work as brokers and traders. Many Lebanese "import-export" concerns are found in free trade zones. Reportedly, many of these Lebanese brokers network via family ties and are involved with underground finance and trade-based money laundering. Informal remittances and value transfer in the form of trade goods add substantially to the remittance flows from expatriates via official banking channels. There are also reports that many in the Lebanese expatriate business community willingly or unwillingly give "charitable donations" to representatives of Hezbollah. The funds are then repatriated or laundered back to Lebanon.

Lebanon has continued to make progress toward developing an effective money laundering and terrorism finance regime by incorporating the Financial Action Task Force (FATF) Recommendations. In 2002, Lebanon was removed from the FATF's Non-Cooperative Countries and Territories list (NCCT), after Lebanon enacted Law No. 318 in 2001. Law No. 318 created a framework for lifting bank secrecy, broadening the criminalization of money laundering beyond drugs, mandating suspicious transaction reporting, requiring financial institutions to obtain customer identification information, and facilitating access to banking information and records by judicial authorities. Under this law, money laundering is a criminal offense and punishable by imprisonment for a period of three to seven years and by a fine of no less than twenty million Lebanese pounds (approximately $13,270). The provisions of Law No. 318 expand the type of financial institutions subject to the provisions of the Banking Secrecy Law of 1956, to include institutions such as exchange offices, financial intermediation companies, leasing companies, mutual funds, insurance companies, companies promoting and selling real estate and construction, and dealers in high-value commodities. In addition, Law No. 318 requires companies engaged in transactions for high-value items (i.e., precious metals, antiquities) and real estate to also report suspicious transactions.

These companies are also required to ascertain, through official documents, the identity and address of each client, and must keep photocopies of these documents as well as photocopies of the operation-

related documents for a period of no less than five years. The CBL regulates private couriers who transport currency. Western Union and Money Gram are licensed by the CBL and are subject to the provisions of this law. Charitable and nonprofit organizations must be registered with the Ministry of Interior, and are required to have proper corporate governance, including audited financial statements. These organizations are also subject to the same suspicious reporting requirements.

All financial institutions and money exchange houses are regulated by the CBL. Law No. 318 clarified the CBL's powers to: require financial institutions to identify all clients, including transient clients; maintain records of customer identification information; request information about the beneficial owners of accounts; conduct internal audits; and exercise due diligence in conducting transactions for clients.

Law No. 318 also established an FIU, called the Special Investigation Commission (SIC), which is an independent entity with judicial status that can investigate money laundering operations and monitor compliance of banks and other financial institutions with the provisions of Law No. 318. The SIC serves as the key element of Lebanon's anti-money laundering regime and has been the critical driving force behind the implementation process. The SIC is responsible for receiving and investigating reports of suspicious transactions. The SIC is the only entity with the authority to lift bank secrecy for administrative and judicial agencies, and it is the administrative body through which foreign FIU requests for assistance are processed. In spring 2006, the SIC started work on a self-assessment in order to further enhance compliance with FATF Recommendations, and to prepare for a potential assessment by international bodies, expected in late 2007 or early 2008.

Since its inception, the SIC has been active in providing support to international criminal case referrals. From January through October 2006, the SIC investigated 118 cases involving allegations of money laundering and terrorist financing activities. Of these cases, five were originated at U.S. Government request. Two of the 118 cases were related to terrorist financing. Bank secrecy regulations were lifted in 56 instances. Ten cases were transmitted by the SIC to the general state prosecutor for further investigation. As of early November 2006, no cases were transmitted by the general state prosecutor to the penal judge. The general state prosecutor reported three cases to the SIC for the freezing of assets. One case involved individuals convicted of terrorism charges, another case involved individuals related to Iraq's former regime, and the third case involved individuals convicted of drug charges. From January to October 2006, the SIC froze the accounts of 17 individuals in five of the 118 cases investigated. Total dollar amounts frozen by the SIC in these five cases is about $1.4 million. The SIC has also worked with the UN International Independent Investigation's Commission (UNIIC) investigation into the assassination of Rafiq Hariri, helping the international inquiry lift bank secrecy laws on certain accounts and freeze the assets of suspects. As a result, dollar amounts frozen by the SIC amounted to $22 million in 2005.

During 2003, Lebanon adopted additional measures to strengthen efforts to combat money laundering and terrorism financing, such as establishing anti-money laundering units in customs and the police. In 2003, Lebanon joined the Egmont Group of financial intelligence units. The SIC has reported increased inter-agency cooperation with other Lebanese law enforcement units, such as Customs and the police, as well as with the office of the general state prosecutor. In 2005, a SIC Remote Access Communication (SRAC) system was put in place for the exchange of information between the SIC, Customs, the Internal Security Forces (ISF) anti-money laundering and terrorist finance unit, and the general state prosecutor. The cooperation led to an increase in the number of suspicious transactions reports (STRs), and as a result, the SIC initiated several investigations in 2006.

In order to more effectively combat money laundering and terrorist financing, Lebanon also adopted two important laws in 2003: Laws 547 and 553. Law 547 expanded Article One of Law No. 318, criminalizing any funds resulting from the financing or contribution to the financing of terrorism or terrorist acts or organizations, based on the definition of terrorism as it appears in the Lebanese Penal

Code (which distinguishes between "terrorism" and "resistance"). Law 547 also criminalized acts of theft or embezzlement of public or private funds, as well as the appropriation of such funds by fraudulent means, counterfeiting, or breach of trust by banks and financial institutions for such acts that fall within the scope of their activities. It also criminalized counterfeiting of money, credit cards, debit cards, and charge cards, or any official document or commercial paper, including checks. Law 553 added an article to the Penal Code (Article 316) on terrorist financing, which stipulates that any person who voluntarily, either directly or indirectly, finances or contributes to terrorist organizations or terrorists acts is punishable by imprisonment with hard labor for a period not less than three years and not more than seven years, as well as a fine not less than the amount contributed but not exceeding three times that amount.

Lebanese law allows for property forfeiture in civil as well as criminal proceedings. The Government of Lebanon (GOL) enforces existing drug-related asset seizure and forfeiture laws. Current law provides for the confiscation of assets the court determines to be related to or proceeding from money laundering or terrorist financing. In addition, vehicles used to transport narcotics can be seized. Legitimate businesses established from illegal proceeds after passage of Law 318 are also subject to seizure. Forfeitures are transferred to the Lebanese Treasury. In cases where proceeds are owed to a foreign government, the GOL returns the proceeds to the concerned government.

Lebanon was one of the founding members of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body that promotes best practices to combat money laundering and terrorist financing in the region. It was inaugurated on November 30, 2004, in Bahrain. As it assumed its presidency for the first year, Lebanon hosted the second MENAFATF plenary in September 2005. A third MENAFATF plenary was held in March 2006 in Cairo where, at Lebanon's initiative, the U.S.-MENA Private Sector Dialogue (PSD) was launched. Lebanon assumed the presidency of the U.S-MENA PSD for the first year.

Lebanon has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision" and is compliant on 24 out of the 25 "Core Principles." Compliance with the pending "Core Principle" is being addressed, and a draft law providing legal protection to bank supervisors awaits cabinet approval. On October 31, 2006, the Banking Control Commission performed a self-assessment, to be completed before the end of January 2007. Banks are compliant with the Basel I Capital Accords and are preparing to comply with the three pillars of the Basel II recommendations. The CBL and the Banking Control Commission are issuing circulars to ensure the banking sector is compliant with Basel II recommendations by January 1, 2008.

The SIC circulates to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224 and those that European Union have designated under their relevant authorities. The SIC as of early November 2006 had signed fifteen memoranda of understanding with other FIUs concerning international cooperation in anti-money laundering and combating terrorist financing. The SIC cooperates with competent U.S. authorities on exchanging records and information within the framework of Law 318.

Lebanon is a party to the 1988 UN Drug Convention, although it has expressed reservations to several sections relating to bank secrecy. It has signed and ratified the UN Convention against Transnational Organized Crime. Lebanon is not a party to the UN Convention against Corruption or the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Lebanon continues to improve its efforts to develop an effective anti-money laundering and counterterrorism finance regime. Yet prosecutions and convictions are still lacking. The end of the Syrian military occupation in April 2005 and the gradual decline of Syrian influence over the economy (both licit and illicit), security services, and political life in Lebanon may present an opportunity for the GOL to further strengthen its efforts against money laundering, corruption and

terrorist financing. The GOL should encourage more efficient cooperation between financial investigators and other concerned parties, such as police and Customs, which could yield significant improvements in initiating and conducting investigations. It should become a party to the UN Convention against Corruption and the UN International Convention for the Suppression of Terrorist Financing. Per Financial Action Task Force Special Recommendation Nine, the GOL should mandate and enforce cross-border currency reporting. Lebanese law enforcement authorities should examine domestic ties to the international network of Lebanese brokers and traders that are commonly found in underground finance, trade fraud, and trade-based money laundering.

## Libya

Libya is not considered to be an important financial sector in the Middle East and northern Africa. The Libyan economy depends primarily upon revenues from the oil sector, which contribute practically all export earnings and about one-quarter of GDP. Oil revenues and a small population give Libya one of the highest per capita GDPs in Africa, but little of this income flows down to the lower levels of society. Libya has a cash-based economy and large underground markets. Libya is a destination for smuggled goods, particularly alcohol and black market/counterfeit goods from sub-Saharan Africa and from Egypt. Contraband smuggling includes narcotics, particularly hashish/cannabis and heroin. Libya is not considered to be a production location for illegal drugs, although its geographic position, long borders and lax immigration policies make it a transit point. Libya is also a transit and destination country for human trafficking originating in sub-Saharan Africa and Asia. Many victims willingly migrate to Libya en route to Europe with the help of smugglers. Reportedly, human smuggling networks force some victims into prostitution or to work as laborers and beggars to pay off their smuggling debts. Profits are laundered. Hawala and informal value transfer networks are present.

The Libyan banking system consists of a Central Bank, six state-owned commercial banks, forty-eight national banks and a handful of privately-owned Libyan banks. Libyan banks suffer from a lack of modern equipment and trained personnel, and substantial investment in both will be required to bring Libyan banks up to international standards. Libyan banks offer little in the way of services for their customers, and most Libyans make little use of the banking system. The Libyan Banking Law No. 1 of 2005 allows for the entry of foreign banks into Libya although with difficult entry and operating terms and requirements that, combined with a history of Libyan government policy reversals, have precluded foreign bank entry to date. Libya is not considered to be an offshore financial center. Offshore banks, international business companies and other forms of exempt/shell companies are not licensed by the Libyan government.

Libya has shown some commitment to privatize its public banks. During the past year, the ongoing privatization of Sahara Bank has resulted in the sale of approximately 40 percent of its shares to individual investors The Central Bank continues to formulate a program of banking sector modernization and has hired western consulting firms to assist in reforms. Libya is also cooperating with both the IMF and World Bank by soliciting their advice and assistance for economic reforms. In general, training and resources are lacking for anti-money laundering awareness and countermeasure implementation. A considerable transition time is anticipated while Libya's banking system is reformed and gradually brought back into the international system following the lifting of UN and U.S. sanctions.

The Central Bank is responsible for the establishment of regulations relevant to combating money laundering and terrorist finance under the terms of Article 57 of Banking Law No. 1 of 2005. Money laundering is illegal in Libya, and terms and penalties are clearly laid out in Banking Law No. 2 of 2005 on Combating Money Laundering. This law does not make specific mention of drug-related money laundering. These crimes are dealt with under Libya's Penal Code, Criminal Procedures Law, and related supplementary laws. Penalties for money laundering under Law No. 2 include

imprisonment (for an unspecified duration) and a fine equal to the amount of relevant illegal goods/property. An increased penalty is used if the malefactor participated in the predicate offense, whether as a perpetrator or accomplice. Penalties ranging from 1,000 to 10,000 Libyan dinars (approximately $770 to $7,700) are also imposed on persons withholding information on money laundering offenses, persons warning offenders of an ongoing investigation and persons in violation of foreign currency importation regulations. The offense of falsely accusing others of money laundering offenses is punishable by imprisonment of no less than a year.

Banking Law No. 2 directs the Central Bank to establish a Financial Information Unit (FIU). It also establishes a National Committee for Combating Money Laundering to be chaired by the Governor or Deputy of the Central Bank. The National Committee will also include representatives from the Secretariat of the General People's Committee for Financial and Technical Supervision, the Secretariat of the General People's Committee for Justice, the Secretariat of the General People's Committee for Public Security, the Secretariat of the General People's Committee for Finance, the Secretariat of the General People's Committee for Economy and Trade, the Secretariat of the General People's Committee for Foreign Liaison and International Cooperation, the Customs Authority and the Tax Authority.

Libyan banks are required to record and report the identity of customers engaged in all transactions. Records of transactions are retained for a considerable (but indeterminate) period, although a lack of computerized records and systems, particularly among Libya's more than forty-eight regional banks and branches in remote areas of the country, negate reliable record-keeping and data retrieval.

Libya's Banking Law No.1 forbids "possessing, owning, using, exploiting, disposing of in any manner, transferring, transporting, depositing, or concealing illegal property in order to disguise its unlawful source." The broad scope of the law, and its complimentary relationship to existing criminal law, extends the scope of money laundering controls and penalties to nonbanking financial institutions. All entities, either financial or nonfinancial in nature, are required by law to report money laundering activity to Libyan authorities under penalty of law. The Central Bank is responsible for supervision of all banks, financial centers and money changing institutions. All banks are required to undergo an annual audit and establish an administrative unit called the "compliance unit" which is directly subordinate to the board of directors. The Central Bank's Banking Supervision Division is also responsible for examining banks to ensure that they are operating in compliance with law.

Libya established a Financial Information Unit (FIU) under the terms of Banking Law No. 2. The Central Bank is responsible for establishing and housing the Libyan FIU. The most recent reporting available indicates that the FIU is still in its formative stages, and individuals seconded by the Central Bank to the FIU require additional training in order to be fully effective.

The FIU is tasked to gather all reports on suspicious transactions from all financial and commercial establishments and individual persons. The FIU is authorized by law to exchange information and reports on cases suspected of being linked to money laundering activities with its counterparts in other countries, in accordance with Libya's international commitments. All banks operating in Libya are required by law to establish a "Subsidiary Unit for Information on Combating Money Laundering" responsible for monitoring all activities and transactions suspected of being linked to money laundering activities. The FIU is responsible for reporting this information to the Governor of the Central Bank for appropriate action. However, given the limitations of the Libyan banking sector both in terms of human and technological resources and the lead time necessary to establish new internal mechanisms, these subsidiary units are either non-existent or nonfunctional in most cases. All entities cooperating with the FIU and/or law enforcement entities are granted confidentiality. Furthermore, anyone reporting acts of money laundering before they are discovered by Libyan authorities is exempted from punishment under the law (safe harbor). There is no reliable information on the

number of suspicious transaction reports (STRs) issued in 2006, nor information on the scope of prosecutions and convictions on the part of Libyan government authorities.

It is illegal to transfer funds outside of Libya without the approval of the Central Bank. Cash courier operations are in clear violation of Libyan law. It is estimated that up to ten percent of foreign transfers are made through illegal means (i.e., not through the Central Bank). Libya is seeking foreign assistance to bring tighter control over these transactions. However, fund transfers by illegal immigrants (mainly from sub-Sahara Africa) are difficult for the Libyan government to monitor, particularly transfers by criminal organizations. It is estimated that there are currently up to two million illegal immigrants in Libya. It is illegal for these workers to take cash out of the country, however some do engage in smuggling and there are illicit transfers of goods and currency across Libya's long land borders.

Informal hawala money dealers (hawaladars) exist in Libya, and are often used to facilitate trade and small project finance. Libyan officials have indicated that they intend to require registration of all hawaladars in the near future. Many payments and transactions take place outside the banking system, often using cash, so as to avoid the scrutiny of the Libyan government. This is done largely for practical reasons, as Libya's socialist practices and commercial rivalries among regime insiders discourage disclosure of income and business transactions. Until the recent revision of the tax code, rates of up to 80-90 percent encouraged off-the-book transactions.

Reportedly, there is no evidence of extensive money laundering or terrorist financing taking place in the Free Trade Zone (FTZ) in the city of Misurata. Misurata, 210 kilometers east of Tripoli, is currently Libya's sole operating FTZ. Projects in the free zone enjoy standard "Five Freedoms" privileges, including tax and customs exemptions. At present, the zone occupies 430 hectares, including a portion of the Port of Misurata.

Libya is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Libya is a party to all 12 of the UN Conventions and Protocols dealing with terrorism, including the International Convention for the Suppression of the Financing of Terrorism. However, Libya has not criminalized terrorist financing. Nor is there any indication that Libya has circulated UN or U.S. lists of terrorist entities or made any effort to freeze, seize or forfeit assets of suspected terrorists or financiers of terrorism.

In 2006, the Department of State rescinded Libya's designation as a State Sponsor of Terrorism. The Government of Libya (GOL) should enact counterterrorist financing legislation and adopt anti-money laundering and counterterrorist finance policies and programs that adhere to world standards. Joining the Middle East and North Africa Financial Action Task Force would assist Libya in that regard. Libya should continue to modernize its banking sector and adopt full transparency procedures. Tax reform should continue so as to shrink the underground economy. Working with the international community, the Libyan FIU and financial police should avail themselves of training. Appropriate entities should become familiar with money laundering and terrorist finance methodologies. In particular, Libyan law enforcement and customs authorities should examine the underground economy, including smuggling networks, and informal value transfer systems. The GOL should adopt measures that combat corruption in government and commerce. Government statistics on the number of money laundering investigations, prosecutions, and convictions should be made publicly available.

## Liechtenstein

The Principality of Liechtenstein's well-developed offshore financial services sector, relatively low tax rates, liberal incorporation and corporate governance rules, and tradition of strict bank secrecy have contributed significantly to the ability of financial intermediaries in Liechtenstein to attract funds from abroad. These same factors have historically made the country attractive to money launderers and

tax evaders. Although the principality has made progress in its efforts against money laundering, accusations of misuse of Liechtenstein's banking and financial services sectors persist.

Liechtenstein's financial services sector includes 16 banks, three nonbank financial companies, 16 public investment companies, and a number of insurance and reinsurance companies. The three largest banks account for slightly less than ninety percent of the market. Liechtenstein's 230 licensed fiduciary companies and 60 lawyers serve as nominees for or manage more than 75,000 entities (mostly corporations or trusts) available primarily to nonresidents of Liechtenstein. Approximately one third of these entities hold controlling interests in separate entities chartered outside of Liechtenstein. Laws permit corporations to issue bearer shares.

Narcotics-related money laundering has been a criminal offense in Liechtenstein since 1993, and the number of predicate offenses for money laundering has increased over time. The Government of Liechtenstein (GOL) is reviewing the Criminal Code in order to further expand the list of predicate offenses. Article 165 criminalizes laundering one's own funds and imposes penalties for money laundering. However, negligent money laundering is not addressed.

The first general anti-money laundering legislation was added to Liechtenstein's laws in 1996. Although the 1996 law applied some money laundering controls to financial institutions and intermediaries operating in Liechtenstein, the anti-money laundering regime at that time suffered from serious systemic problems and deficiencies. In response to international pressure, beginning in 2000, the GOL took legislative and administrative steps to improve its anti-money laundering regime.

Liechtenstein's primary piece of anti-money laundering legislation, the Due Diligence Act (DDA) of November 26, 2004, entered into force on February 1, 2005. The act repealed a number of prior laws, including the 1996 Due Diligence Act and its amendments. The DDA applies to banks, e-money institutions, casinos, dealers in high-value goods, and a number of other classes of entities. Along with the January 2005 Due Diligence Ordinance, the DDA sets out the basic requirements of the anti-money laundering regime: customer identification, suspicious transaction reporting, and record keeping. The act mandates that banks and postal institutions not engage in business relationships with shell banks nor maintain passbooks, accounts, or deposits payable to the bearer. The legislative revision also focused on the inclusion of measures to combat terrorist financing. For instance, the DDA expanded the scope of STR (suspicious transaction reporting) to including terrorist financing.

The GOL announced that by 2008 it would implement a new set of EU regulations requiring that money transfers above 15,000 euro (approximately $17,680) be accompanied by information on the identity of the sender, including his or her name, address, and account number. The proposed measures will ensure that this information will be immediately available to appropriate law enforcement authorities and will assist them in detecting, investigating, and prosecuting terrorists and other criminals.

The Financial Market Authority (FMA) serves as Liechtenstein's central financial supervisory authority. Beginning operations on January 1, 2005, FMA assumed the responsibilities of several former administrative bodies, including the Financial Supervisory Authority and the Due Diligence Unit, both of which once exercised responsibility over money laundering issues. FMA reports exclusively to the Liechtenstein Parliament, making it independent from Liechtenstein's government. It oversees a large variety of financial actors, including banks, finance companies, insurance companies, currency exchange offices, and real estate brokers. FMA works closely with Liechtenstein's financial intelligence unit (FIU), the Office of the Prosecutor, and the police.

Liechtenstein's FIU, known as the Einheit fuer Finanzinformationen (EFFI), receives STRs relating to money laundering and terrorist financing. The EFFI became operational in March 2001 and a member of the Egmont Group three months later. The EFFI has set up a database to analyze its STRs and has access to various governmental databases, although it cannot seek additional financial information

unrelated to a filed STR. The suspicious transaction reporting requirement applies to banks, insurers, financial advisers, postal services, exchange offices, attorneys, financial regulators, casinos, and other entities. The GOL has reformed its suspicious transaction reporting system to permit reporting for a much broader range of offenses than in the past and based on a suspicion, rather than the previous standard of "a strong suspicion."

In 2005, the number of STRs decreased by 17.5 percent from the previous year to 193. Of these 193 reports, the majority were submitted by banks (54 percent) and professional trustees (38 percent). As in 2004, fraud and money laundering remained the most prevalent types of offenses indicated by the entities submitting STRs to the FIU. The share of STRs involving fraud decreased from 48 percent to 45 percent, while the share of STRs involving money laundering increased from 20 percent to 27 percent. There is no similar data available for 2006.

In 2005, the FIU forwarded 72 percent of the total number of STRs it received to prosecution authorities, compared with 79 percent in 2004 and 72 percent in 2003. In the reporting year, 22.3 percent of the beneficial owners indicated in STRs were German nationals, followed by Swiss and U.S. nationals with 14.5 percent each. Austrian, British, and Dutch citizens each accounted for 4.1 percent of beneficial owners indicated in STRs, and Liechtenstein nationals made up only 3 percent of beneficial owners mentioned. In terms of the location of the suspected predicate offense (as mentioned in STRs), Canada and the United States accounted for the most funds, with about $403 million (500 million Swiss francs) and $360 million (450 million Swiss francs) respectively.

In 2005, the EFFI received 89 inquiries from 13 foreign FIUs, 25 percent fewer than in 2004. In the same period, the EFFI submitted 103 inquiries to 18 different countries, down from 134 inquiries in 2004. The most frequent judicial cooperation requests originated from or were directed to the U.S., Germany, Switzerland, and Austria.

Liechtenstein has in place legislation to seize, freeze, and share forfeited assets with cooperating countries. The Special Law on Mutual Assistance in International Criminal Matters gives priority to international agreements. Money laundering is an extraditable offense, and legal assistance is granted on the basis of dual criminality—the offense must be a criminal offense in both jurisdictions. Article 235A provides for the sharing of confiscated assets, and this has been used in practice. Liechtenstein has not adopted the EU-driven policy of reversing the burden of proof by making it necessary for the defendant to prove that he had acquired assets legally (instead of the state having to prove he had acquired them illegally).

A series of amendments to Liechtenstein law, adopted by Parliament on May 15, 2003, include a new criminal offense for terrorist financing along with amendments to the Criminal Code and the Code of Criminal Procedure. Liechtenstein also has issued ordinances to implement United Nations Security Council Resolutions (UNSCRs) 1267 and 1333. Amendments to the ordinances in October and November 2001 allow the GOL to freeze the accounts of individuals and entities that were designated pursuant to these UNSCRs. The GOL updates these ordinances regularly.

The GOL has also improved its international cooperation provisions in both administrative and judicial matters. A mutual legal assistance treaty (MLAT) between Liechtenstein and the United States entered into force on August 1, 2003 and was reaffirmed through an exchange of diplomatic notes on July 14, and October 27, 2006. The U. S. Department of Justice has acknowledged Liechtenstein's cooperation in the Al-Taqwa Bank case and in other fraud and narcotics cases. The EFFI has in place memoranda of understanding (MOUs) with the FIUs in Belgium, Monaco, Croatia, Poland, Russia, Switzerland, and Georgia. Further MOUs are being prepared with France, Italy, Canada, Malta, and San Marino.

Liechtenstein is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The GOL is a party to the Council of Europe

Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and the UN International Convention for the Suppression of the Financing of Terrorism. Liechtenstein has also signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Liechtenstein has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision" and has adopted the EU Convention on Combating Terrorism.

The Government of Liechtenstein has made progress in addressing shortcomings in its anti-money laundering regime. It should continue to build upon the foundation of its evolving anti-money laundering and counterterrorist financing regime. Liechtenstein should become a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Per FATF Special Recommendation Nine, Liechtenstein should require reporting of cross-border currency movements. The data should be shared with EFFI, the financial intelligence unit. Authorities should ensure that trustees and other fiduciaries comply fully with all aspects of the new anti-money laundering legislation and attendant regulations, including the obligation to report suspicious transactions. The EFFI should be given access to additional financial information. While Liechtenstein recognizes the rights of third parties and protects uninvolved parties in matters of confiscation, the government should distinguish between bona fide third parties and others. There appears to be an over-reliance on STRs to initiate money laundering and financial crimes investigations; Liechtenstein law enforcement entities should become more pro-active in this regard. The GOL should criminalize "negligent money laundering" and should publish the annual number of arrests, prosecutions, and convictions for money laundering.

## Luxembourg

Despite its standing as the second-smallest member of the European Union (EU), Luxembourg is one of the largest financial centers in the world. Its strict bank secrecy laws allow international financial institutions to benefit from and operate a wide range of services and activities. With nearly $ 2.2 trillion in domiciled assets, Luxembourg is the second largest mutual fund investment center in the world, after the United States. Luxembourg is considered an offshore financial center, with foreign-owned banks (many of which enjoy ring-fenced tax benefits) accounting for a majority of the nation's total bank assets. Although there are a handful of domestic banks operating in the country, the majority of banks registered in Luxembourg are foreign subsidiaries of banks in Germany, Belgium, France, Italy, and Switzerland. For this reason (and also due to the proximity of three of these nations to Luxembourg), a significant share of Luxembourg's suspicious transaction reports (STRs) are generated from transactions involving clients in these countries. While Luxembourg is not a major hub for illicit drug distribution, the size and sophistication of its financial sector create opportunities for money laundering, tax evasion, and other financial crimes.

As of September 2006, 154 banks, with a balance sheet total reaching 824 billion euros (approximately $1.05 trillion), were registered within Luxembourg. In addition, as of September 2006, a total of 2,158 "undertakings for collective investment" (UCIs), or mutual fund companies, whose net assets had reached over 1.7 trillion euros (approximately $2.18 trillion) by the end of September 2006, were operating out of Luxembourg. Luxembourg has about 15,000 holding companies, 95 insurance companies, and 260 reinsurance companies. As of January 2006, the Luxembourg Stock Exchange listed over 36,000 securities issued by nearly 4,100 entities from about 100 different countries. Legislation passed in June 2004 permits the registration of venture capital funds (Societe d'investissement en capital a risqué, or "SICAR"). As of September 2006, 82 SICARs had been registered.

Luxembourg's financial sector laws are modeled to a large extent on EU directives. The Law of July 7, 1989, updated in 1998 and 2004, serves as Luxembourg's primary anti-money laundering (AML) and terrorist financing law, criminalizing the laundering of proceeds for an extensive list of predicate

offenses, including narcotics trafficking. The Law of April 5, 1993 implements the EU's 1991 First Anti-Money Laundering Directive and includes among its provisions customer identification, record keeping, and suspicious transaction reporting requirements. The Act of August 1, 1998 expands the list of covered entities and adds corruption, weapons offenses, and organized crime to the list of predicate offenses for money laundering. The Act of June 10, 1999 further expands anti-money laundering provisions. On May 23, 2005, a new law was passed which added corruption in the private sector to the list of money laundering predicate offenses. Fraud committed against the European Union has also been added to the list of offenses. Although only natural persons are currently subject to the law, the government has been preparing a draft bill that would add legal persons to its jurisdiction.

In an effort to bring Luxembourg into full compliance with the requirements of the EU's Second Money Laundering Directive, on November 12, 2004, Parliament approved legislation updating the nation's anti-money laundering laws. These legislative amendments formally transferred the requirements of the EU's Second Money Laundering Directive into domestic law. In October 2005, the Commission de Surveillance du Secteur Financier (CSSF) distributed a circular to the financial industry publicizing the November 2004 law and offering advice on suggested best practices. The 2004 amendments also broaden the scope of institutions subject to money laundering regulations. Under the current law, banks, pension funds, insurance brokers, UCIs, management companies, external auditors, accountants, notaries, lawyers, casinos and gaming establishments, real estate agents, tax and economic advisors, domiciliary agents, insurance providers, and dealers in high-value goods, such as jewelry and cars, are now considered covered institutions. AML law does not cover SICAR entities.

All covered entities are required to file STRs with the financial intelligence unit (FIU) and, though not legally required, are expected to send copies of their reports to their respective oversight authorities. The banking community generally cooperates with enforcement efforts to trace funds and seize or freeze bank accounts; the track record of cooperation by notaries and others is still being tested, given the legislation has only been in effect for the past year. Financial institutions are required to retain pertinent records for a minimum of five years; additional commercial rules require that certain bank records be kept for up to ten years. The AML law also contains "safe harbor" provisions that protect obliged individuals and entities from legal liability when filing STRs or assisting government officials during the course of a money laundering investigation. The 2004 amendments also contain new requirements regarding financial institutions' internal AML programs. They impose strict "know your customer" requirements, mandating their application to all new and existing customers, including beneficial owners, trading in goods worth at least 15,000 euros. If the transaction or business relationship is remotely based, the law details measures required for customer identification. Financial institutions must ensure adequate internal organization and employee training, and must also cooperate with authorities, proactively monitoring their customers for potential risk. "Tipping off" has also been prohibited.

Under Luxembourg law the secrecy rules are waived in the prosecution of money laundering and other criminal cases. No court order is required to investigate otherwise secret account information in suspected money laundering cases or when a STR is filed. Financial professionals are obliged to cooperate with the public prosecutor in investigating such cases.

The Commission de Surveillance du Secteur Financier (CSSF) is an independent government body under the jurisdiction of the Ministry of Finance that serves as the prudential oversight authority for banks, credit institutions, the securities market, some pension funds, and other financial sector entities covered by the country's anti-money laundering and terrorist financing laws. The Luxembourg Central Bank oversees the payment and securities settlement system, and the Commissariat aux Assurances (CAA), also under the Ministry of Finance, is the regulatory authority for the insurance sector. The identities of the beneficial owners of accounts are available to all entities involved in oversight functions, including registered independent auditors, in-house bank auditors, and the CSSF.

Under the direction of the Ministry of the Treasury, the CSSF has established a committee, the Comite de Pilotage Anti-Blanchiment (COPILAB), composed of supervisory and law enforcement authorities, the FIU, and financial industry representatives. The committee meets monthly to develop a common public-private approach to strengthen Luxembourg's AML regime.

No distinctions are made in Luxembourg's laws and regulations between onshore and offshore activities. Foreign institutions seeking establishment in Luxembourg must demonstrate prior establishment in a foreign country and meet stringent minimum capital requirements. Companies must maintain a registered office in Luxembourg, and background checks are performed on all applicants. A ministerial decree published in July 2004 modified the Luxembourg Stock Exchange's internal regulations to make it easier to list offshore funds, provided the fund complies with CSSF requirements as detailed in Circular 04/151. Also, a government registry publicly lists company directors. Although nominee (anonymous) directors are not permitted, bearer shares are permitted. Officials contend that bearer shares do not present a problem for money laundering because of know-your-customer laws, requiring banks to know the identity of the beneficial owner. Banks must undergo annual audits under the supervision of the CSSF (CSSF reg. No. 27). Independent auditors have established a peer review procedure in compliance with an EU recommendation on quality control for external audit work to assure the adherence to international standards on auditing.

Established within Luxembourg's Ministry of Justice, the Cellule de Renseignement Financier (FIU-LUX) consists of two full and one part-time officials and serves as Luxembourg's FIU, receiving and analyzing STRs and seizing and freezing assets when necessary. As part of modifications made in 2004 to Luxembourg's money laundering law, the FIU's official status as a division within the Ministry of Justice Public Prosecutor's Office was formalized. As a result, FIU officials spend a fair proportion of their time on nonfinancial crime cases. Some members of the financial community continue to call for the creation of an administrative FIU body separate from the Office of the Public Prosecutor. The FIU is responsible for providing members of the financial community with access to updated information on money laundering and terrorist financing practices. It also works closely with various regulatory bodies such as the CSSF and the CAA. The FIU and CSSF work together in investigations involving significant money laundering cases. The FIU does not have direct access to the records or databases of other government entities, but the response to its requests have proven to be efficient.

In order to obtain a conviction for money laundering, prosecutors must now prove criminal intent rather than negligence. Negligence, however, is still scrutinized by the appropriate sector oversight authority, with sanctions for noncompliance varying from 1,250 to 1,250,000 euros.

In 2005, covered institutions filed a total of 831 STRs, compared to a total of 943 in 2004. This figure represents a slight decrease in comparison to the past two years (832 STRs were filed in 2003, 631 in 2002, and 431 in 2001). The rate of STR filings began to decrease as legislation was being introduced in 2004 to add professional obligations covered by the anti-money laundering and terrorist financing law. The majority of STRs still originate from banks. Of 388 confirmed cases of suspicious activity in 2005, including those received by international rogatory commission, 55 specifically related to money laundering, 30 to organized crime, 11 to drug-related money laundering, 5 to corruption, and 9 to other offenses. Among the 2,471 individuals involved in STRs in 2004, 383 were residents in Luxembourg, 350 in France, 333 in Belgium, 250 in Germany, 221 in Italy, 111 in the United Kingdom, 132 in Russia, and 71 in the United States. Statistics for 2006 are not available.

There has only been one money laundering case prosecuted in Luxembourg. The case is still pending. There is one additional money laundering case scheduled for trial in 2007.

Luxembourg law only allows for criminal forfeitures and public takings. Drug-related proceeds are pooled in a special fund to invest in anti-drug abuse programs. Funds found to be the result of money laundering can be confiscated even if they are not the proceeds of a crime. The GOL can, on a case-

by-case basis, freeze and seize assets, including assets belonging to legitimate businesses used for money laundering. The government has adequate police powers and resources to trace, seize, and freeze assets without undue delay. Luxembourg has a comprehensive system not only for the seizure and forfeiture of criminal assets, but also for the sharing of those assets with other governments. On October 17, 2006, the United States and Luxembourg announced a sharing agreement in which they would divide equally €11,366,265.44 (approximately $ 14,548,820) of seized assets of two convicted American narcotics traffickers which had been domiciled in Luxembourg bank accounts. Reportedly, there is a consistently high level of cooperation between Luxembourg and other foreign countries' law enforcement authorities on money laundering investigations.

Luxembourg authorities have been actively involved in bilateral and international fora and training in order to become more effective at fighting the financing of terrorism. In July 2003, Luxembourg's parliament passed a multifaceted counterterrorism financing law known as Projet de Loi 4954, designed to strengthen Luxembourg's ability to fight terrorism and terrorist financing. The law defines terrorist acts, terrorist organizations, and terrorism financing in the Luxembourg Criminal Code. In addition, the specific crimes, as defined, will carry penalties of 15 years to life. The law also extends the definition of money laundering to incorporate new terrorism-related crimes and provides an exception to notification requirements in selected wiretapping cases. The November 2004 amendments bring Luxembourg into compliance with the FATF's Special Recommendation IV by extending the reporting obligations of the financial sector to terrorist financing, independently from any context of money laundering. Covered institutions now are required to report any transaction believed to be related to terrorist financing, regardless of the source of the funds.

The Ministry of Justice studies and reports on potential abuses of charitable and nonprofit entities to protect their integrity. Justice and Home Affairs ministers from Luxembourg and other EU member states agreed in early December 2005 to take into account five principles with regard to implementing FATF Special Recommendation VIII on nonprofit organizations: safeguarding the integrity of the sector; dialogue with stakeholders; continuing knowledge development of the sector; transparency, accountability and good governance; and effective, proportional oversight. Luxembourg authorities have not found evidence of the widespread use in Luxembourg of alternative remittance systems such as hawala, black market exchanges, or trade-based money laundering. Officials comment that existing AML rules would apply to such systems, and no separate legislative initiatives are being formally considered to address them.

In an effort to identify and freeze the assets of suspected terrorists, the GOL actively disseminates to its financial institutions information concerning suspected individuals and entities on the United Nations Security Council Resolution 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. Luxembourg does not have legal authority to independently designate terrorist groups or individuals. The government has been working on legislation with regard to this issue for some time now; however, the legislation remains in the early drafting process. Luxembourg's authorities can and do take action against groups targeted through the EU designation process and the UN.

Under the 2004 amendments to Luxembourg's AML law, bilateral freeze requests are limited to a new maximum of three months; designations under the EU, UN, or international investigation processes continue to be subject to freezes for an indefinite time period. Upon request from the United States, Luxembourg froze the bank accounts of individuals suspected of involvement in terrorism. Luxembourg has also independently frozen several accounts, resulting in court challenges by the account holders. Since 2001, over $200 million in suspect accounts have been frozen by Luxembourg authorities pending further investigations (most of the assets were subsequently released).

Luxembourg cooperates with and provides assistance to foreign governments in their efforts to trace, freeze, seize and forfeit assets. Dialogue and other bilateral proceedings between Luxembourg and the

United States have been extensive. Luxembourg held the EU Presidency from January through June 2005. As part of its presidency agenda, Luxembourg placed a priority on making progress on the additional legal instruments the United States had signed with the European Union covering extradition and mutual legal assistance. The extradition agreement will modernize existing bilateral extradition treaties with each of the EU member states. The mutual legal assistance agreement contains cutting-edge provisions for future legal cooperation, including the ability to informally identify the existence of bank accounts in terrorism-related cases. To implement the EU-wide agreements, supplemental treaties between the U.S. and each EU member states are required. On February 1, 2005, bilateral instruments were signed to implement the U.S.-EU extradition and mutual legal assistance agreements between Luxembourg and the United States. Luxembourg was instrumental in using its EU presidency to push this process closer to completion with four additional EU members as well.

In its 2005 EU Presidency capacity, Luxembourg also oversaw new milestones in the recently-established U.S.-EU dialogue on terrorist finance issues. Prosecutors and investigators from the United States and the EU's Eurojust met for the first time in March 2005 at The Hague to discuss a suspect terrorist group that operated in a number of countries. The Luxembourg EU Presidency hosted a two-day workshop in April 2005 for U.S. and EU member state terrorist finance prosecutors, investigators, and designators (who met for the first time at this event). The dialogue continued throughout 2005 to expand U.S.-Luxembourg and U.S.-EU cooperation between experts dedicated to countering terrorist financing. This forum was determined to be quite useful, and was continued by the Finnish EU Presidency as the second workshop was held 27-28 September 2006.

As of September 2005, over $22 million in illegal drug proceeds was frozen in Luxembourg at the request of U.S. authorities. Luxembourg worked with the United States Department of Justice throughout the year on several outstanding drug-related money laundering and asset forfeiture cases. On September 7, 2005, Luxembourg repatriated to the United States nearly $1 million, based on a U.S. legal assistance request, to victims of a fraud involving a former Vice President of Riggs Bank in Washington, D.C.

Luxembourg laws facilitating international cooperation in money laundering include the Act of August 8, 2000, which enhances and simplifies procedures on international judicial cooperation in criminal matters; and the Law of June 14, 2001, which ratifies the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. During its EU Presidency, Luxembourg shepherded the draft of the Third Money Laundering and Terrorist Financing Directive through the EU's legislative process. The directive was published in the EU's Official Journal on November 25, 2005. EU member states must transpose this legislation into national law within the next two years.

Luxembourg is a party to the 1988 UN Drug Convention and but has not yet ratified the UN Convention against Transnational Organized Crime. In November 2003, Luxembourg ratified the UN International Convention for the Suppression of the Financing of Terrorism.

Luxembourg is a member of the European Union and the FATF. The Luxembourg FIU is a member of the Egmont Group and has negotiated memoranda of understanding with several countries, including Belgium, Finland, France, Korea, Monaco, and Russia. Luxembourg and the United States have had a mutual legal assistance treaty (MLAT) since February 2001. Luxembourg's Agency for the Transfer of Financial Technology (ATTF) has consistently provided training and acted as a consultant in money laundering matters to government and banking officials in countries whose regimes are in the development stage. Since 2001, ATTF has provided assistance to government and banking officials from Bosnia-Herzegovina, Bulgaria, Croatia, Cape Verde, China, the Czech Republic, Egypt, Macedonia, Romania, Russia, Ukraine, Cyprus, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia, El Salvador, Kazakhstan, Laos, Moldova, Mongolia, Serbia and Montenegro,

Tunisia, Turkey, Uzbekistan, and Vietnam. Georgia was added to this list in 2006 and the hope is to add Azerbaijan in 2007.

According to the December 2004 International Monetary Fund (IMF) report Luxembourg: Report on the Observance of Standards and Codes—FATF Recommendations for Anti-Money Laundering and Combating the Financing of Terrorism, Luxembourg has "a solid criminal legal framework and supervisory system" to counter money laundering and terrorist financing and is "broadly compliant with almost all of the Financial Action Task Force (FATF) Recommendations." The report also notes that Luxembourg's high level of cross-border business, obligatory banking secrecy, private banking, and "certain investment vehicles" create a challenging environment for countering money laundering and terrorist financing

The Government of Luxembourg has enacted laws and adopted practices that help to prevent the abuse of its bank secrecy laws, and it has enacted a comprehensive legal and supervisory anti-money laundering regime. However, further action should be taken to address the lack of a distinct legal framework for the financial intelligence unit. The financial intelligence unit staff should have its other judicial responsibilities curtailed and be freed to focus solely on financial crimes. Regarding regulations, Luxembourg should continue to strengthen enforcement to prevent abuse of its financial sector. Specifically, Luxembourg should pass legislation creating the authority for it to independently designate those who finance terrorism. Luxembourg should also enact legislation to address the continued use of bearer shares. Per FATF Special Recommendation Nine, Luxembourg should initiate and enforce cross-border currency reporting requirements and the data should be shared with the financial intelligence unit. Luxembourg's anti-money laundering regime may be relying too heavily on the filing of suspicious transaction reports to generate investigations. Although Luxembourg has steadily enacted anti-money laundering and terrorist finance laws, policies, and procedures, the lack of prosecutions and convictions is telling, particularly for a country that boasts such a large financial sector.

## Macau

Under the one country-two systems principle that underlies Macau's 1999 reversion to the People's Republic of China, Macau has substantial autonomy in all areas except defense and foreign affairs. Macau's free port, lack of foreign exchange controls, and significant gambling industry create an environment that can be exploited for money laundering purposes. In addition, Macau is a gateway to China, and can be used as a transit point to remit funds and criminal proceeds to and from China. Macau has a small economy heavily dependent on gaming, but is emerging as a financial center. Its offshore financial sector is not fully developed.

Main money laundering methods in the financial system are wire transfers; currency exchange/cash conversion; the use of casinos to remit or launder money; and the use of nominees, trusts, family members, or third parties to transfer cash. Macau has taken several steps over the past three years to improve its institutional capacity to tackle money laundering. On March 23, 2006, the Macau Special Administrative Region (MSAR) Government passed a 12-article bill on the prevention and repression of money laundering that incorporates aspects of the revised FATF Forty Recommendations. The law expands the number of sectors covered by Macau's previous anti-money laundering (AML) legislation, calls for the establishment of a financial intelligence unit (FIU), and includes provisions on due diligence. The 2006 anti-money laundering law broadened the definition of money laundering to include all serious predicate crimes. The law provides for 2-8 years imprisonment for money laundering offenses, and if a criminal is involved in organized crime or triad-related money laundering, the penalties would increase by one-half. The new law also allows for fines to be added to the time served and eliminated a provision reducing time served for good behavior.

The 2006 law also extended the obligation of suspicious transaction reporting to lawyers, notaries, accountants, auditors, tax consultants and offshore companies. Covered businesses and individuals must meet various obligations, such as the duty to confirm the identity of their clients and the nature of their transactions. Businesses must reject clients that refuse to reveal their identities or type of business dealings. The law obliges covered entities to send suspicious transaction reports (STRs) to the relevant authorities and cooperate in any follow-up investigations. This law also requires casinos to submit STRs.

On March 30, 2006, the MSAR also passed new counterterrorism legislation aimed at strengthening measures to combat the financing of terrorism (CFT). The law generally complies with UNSCR 1373, making it illegal to conceal or handle finances on behalf of terrorist organizations. Individuals are liable even if they are not members of designated terrorist organizations themselves. The legislation also allows prosecution of persons who commit terrorist acts outside of Macau in certain cases, and would mandate stiffer penalties. However, the draft legislation does not mention how to freeze without delay terrorist assets, nor does it discuss international cooperation on terrorism financing. In January 2005, the Monetary Authority of Macau issued a circular to all banks and other authorized institutions requiring them to maintain a database of suspected terrorists and terrorist organizations.

While Macau's new AML and CTF laws should create a more robust legal framework to combat money laundering, Macau will also need to enforce these laws. In an August 2002 "Assessment of the Regulation and Supervision of the Financial Sector of Macao", the IMF concluded that Macau was "materially noncompliant" with the Basel Committee's anti-money laundering principles, and recommended a number of improvements. On September 15, 2005, the U.S. Department of Treasury designated Macau-based Banco Delta Asia as a primary money laundering concern under the USA PATRIOT Act. According to the U.S. Treasury Department, Banco Delta Asia provided financial services for more than 20 years to North Korea and facilitated many of that regime's criminal activities, including circulating counterfeit U.S. currency. Macau's Monetary Authority has taken control of Banco Delta Asia and is cooperating with the U.S. Treasury Department in an ongoing investigation of the bank.

Macau's financial system is governed by the 1993 Financial System Act and amendments, which lay out regulations to prevent use of the banking system for money laundering. The Act imposes requirements for the mandatory identification and registration of financial institution shareholders, customer identification, and external audits that include reviews of compliance with anti-money laundering statutes. The 1997 Law on Organized Crime criminalizes money laundering for the proceeds of all domestic and foreign criminal activities, and contains provisions for the freezing of suspect assets and instrumentalities of crime. Legal entities may be civilly liable for money laundering offenses, and their employees may be criminally liable.

The 1998 Ordinance on Money Laundering sets forth requirements for reporting suspicious transactions to the Judiciary Police and other appropriate supervisory authorities. These reporting requirements apply to all legal entities supervised by the regulatory agencies of the MSAR, including pawnbrokers, antique dealers, art dealers, jewelers, and real estate agents. In October 2002 the Judiciary Police set up the Fraud Investigation Section. One of its key functions is to receive all suspicious transaction reports (STRs) in Macau and to undertake subsequent investigations. In November 2003, the Monetary Authority of Macau issued a circular to banks, requiring that STRs be accompanied by a table specifying the transaction types and money laundering methods, in line with the collection categories identified by the Asia/Pacific Group on Money Laundering. Macau law provides for forfeiture of cash and assets that assist in or are intended for the commission of a crime. There is no significant difference between the regulation and supervision of onshore and of offshore financial activities.

Macau is in the process of establishing a Financial Intelligence Unit (FIU). A Macau Monetary Authority official has been designated to head the FIU. As of October 2006, in addition to the FIU Head, the staff consisted of two officials (seconded from the Insurance Bureau and the Monetary Authority), a judiciary police official, and two information technology staff. The FIU is working on creating an operations manual, and is working with the Macau Police on dissemination of suspicious transaction reports (STRs) and with the Public Prosecutors Office on prosecution of cases. The FIU is currently working out of temporary office space but plans to move into permanent office space in January 2007 when it will begin accepting STRs.

The gaming sector and related tourism are critical parts of Macau's economy. Taxes from gaming comprised 73 percent of government revenue in the first eight months of 2006. Gaming revenue increased 12.6 percent during the first eight months of 2006, compared with a year earlier. The MSAR ended a long-standing gaming monopoly early in 2002 when it awarded concessions to two additional operators, the U.S.-based Venetian and Wynn Corporations. . Macau now effectively has six separate casino licenses, three concession holders Sociedade de Jogos de Macau (SJM), Galaxy and Wynn and three subconcession holders Las Vegas Sands, MGM and PBL/Melco. Las Vegas Sands opened its first casino, the Sands, on May 18, 2004. In addition, MGM began constructing a casino in conjunction with Pansy Ho, the daughter of local businessperson Stanley Ho, the largest casino operator in Macau, whose company, Sociedade de Jogos de Macau (SJM), previously held a monopoly on casino operations. Wynn opened its casino in September 2006 and MGM and the Venetian are scheduled to open casinos in 2007. A consortium between Australia's PBL and Macau's Melco, led by Stanley Ho's son Lawrence Ho, as yet operates no casinos, but runs several slot machine rooms in Macau.

Under the old monopoly framework, organized crime groups were, and continue to be, associated with the gaming industry through their control of VIP gaming rooms and activities such as racketeering, loan sharking, and prostitution. The VIP rooms catered to clients seeking anonymity within Macau's gambling establishments, and were shielded from official scrutiny. As a result, the gaming industry provided an avenue for the laundering of illicit funds and served as a conduit for the unmonitored transfer of funds out of China. Unlike SJM and new entrant Galaxy, the Sands does not cede control of its VIP gaming facilities to outside organizations. This approach impedes organized crime's ability to penetrate the Sands operation.

The MSAR's money laundering legislation includes provisions designed to prevent money laundering in the gambling industry. The legislation aims to make money laundering by casinos more difficult, improve oversight, and tighten reporting requirements. On June 7, 2004, Macau's Legislative Assembly passed legislation allowing casinos and junket operators to make loans, in chips, to customers, in an effort to prevent loan-sharking by outsiders. The law requires both casinos and junket operators to register with the government.

Terrorist financing is criminalized under the Macau criminal code (Decree Law 58/95/M of November 14, 1995, Articles 22, 26, 27, and 286). The MSAR has the authority to freeze terrorist assets, although a judicial order is required. Macau financial authorities directed the institutions they supervise to conduct searches for terrorist assets, using the consolidated list provided by the UN 1267 Sanctions Committee and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. No assets were identified in 2005.

The Macau legislature passed a counterterrorism law in April 2002 that is intended to assist with Macau's compliance with UNSCR 1373. The legislation criminalizes violations of UN Security Council resolutions, including counterterrorism resolutions, and strengthens counterterrorist financing provisions. China signed the UN International Convention for the Suppression of the Financing of Terrorism on November 13, 2001, and the Standing Committee of the 10th National People's Congress ratified it in February 2006. The Instrument of Ratification was delivered to the UN on April

21, 2006, and stipulated that in accordance with Article 138 of the Basic Law of the Macao Special Administrative Region of the People's Republic of China, the Government of the People's Republic of China had decided that the Convention shall apply to the MSAR.

The increased attention paid to financial crimes in Macau since the events of September 11, 2001, has led to a general increase in the number of suspicious transaction reports (STRs); however, the number of STRs remains low. Macau's Judiciary Police received 107 STRs in 2003, 109 in 2004, 194 in 2005, and 396 STRs from January to September of 2006, from individuals, banks, companies, and government agencies. In 2003 Macau opened two money laundering cases and prosecuted one. In 2004 Macau opened ten money laundering cases and prosecuted zero. In 2005 Macau opened nine money laundering cases and prosecuted two. In the first half of 2006 Macau opened twelve money laundering cases and prosecuted one. In May 2002, the Macau Monetary Authority revised its anti-money laundering regulations for banks to bring them into greater conformity with international practices. Guidance also was issued for banks, money changers, and remittance agents, addressing record keeping and suspicious transaction reporting for cash transactions over $2,500. For such transactions, banks, insurance companies, and moneychangers must perform customer due diligence. In 2003, the Macau Monetary Authority examined all money changers and remittance companies to determine their compliance with these regulations. The Monetary Authority of Macau, in coordination with the IMF, updated its bank inspection manuals to strengthen anti-money laundering provisions. The Monetary Authority inspects banks every two years, including their adherence to anti-money laundering regulations.

The United States has no law enforcement cooperation agreements with Macau, though informal cooperation between the United States and Macau routinely takes place. The Judiciary Police have been cooperating with law enforcement authorities in other jurisdictions through the Macau branch of Interpol, to suppress cross-border money laundering. In addition to Interpol, the Fraud Investigation Section of the Judiciary Police has established direct communication and information sharing with authorities in Hong Kong and mainland China. In July 2006, the MSAR enacted the Law on Judicial Cooperation in Criminal Matters, enabling the MSAR to enter into more formal judicial and law enforcement cooperation relationships with other countries. The law became effective in November 2006.

The Monetary Authority of Macau also cooperates internationally with other financial authorities. It has signed memoranda of understanding with the People's Bank of China, China's Central Bank, the China Insurance Regulatory Commission, the China Banking Regulatory Commission, the Hong Kong Monetary Authority, the Hong Kong Securities and Futures Commission, the Insurance Authority of Hong Kong, and Portuguese bodies including the Bank of Portugal, the Banco de Cabo Verde and the Instituto de Seguros de Portugal.

Macau's Monetary Authorities are cooperating with the U.S. Treasury Department investigation of Banco Delta Asia. The Monetary Authorities have taken control of Banco Delta Asia and have frozen accounts linked to North Korea worth approximately US$ 24 million. The Government of Macau announced in September 2006 that it would continue to maintain control over Banco Delta Asia for at least six more months as the Banco Delta Asia investigation continues.

Macau participates in a number of regional and international organizations. It is a member of the Asia/Pacific Group on Money Laundering (APG), the Offshore Group of Banking Supervisors, the International Association of Insurance Supervisors, the Offshore Group of Insurance Supervisors, the Asian Association of Insurance Commissioners, the International Association of Insurance Fraud Agencies, and the South East Asia, New Zealand and Australia Forum of Banking Supervisors (SEAZA). In 2003, Macau hosted the annual meeting of the APG, which adopted the revised FATF Forty Recommendations and a strategic plan for anti-money laundering efforts in the region from 2003 to 2006. In September 2003, Macau became a party to the UN Convention against Transnational

Organized Crime as a result of China's ratification. Macau also became a party to the 1988 UN Drug Convention through China's ratification. Macau has taken a number of steps in the past three years to raise industry awareness of money laundering. During a March 2004 IMF technical assistance mission, the IMF and Monetary Authority of Macau organized a seminar for financial sector representatives on the FATF Revised Forty Recommendations. The Macau Monetary Authority trains banks on anti-money laundering measures on a regular basis.

Macau should implement and enforce existing laws and regulations, and ensure effective implementation of its new legislation. Macau should ensure that regulations, structures, and training are put in place to prevent money laundering in the gaming industry, including implementing as quickly as possible regulations to prevent money laundering in casinos, including the VIP rooms. The MSAR should take steps to implement the new FATF Special Recommendation Nine, adopted by the FATF in October 2004, requiring countries to put in place detection and declaration systems for cross-border bulk currency movement. Macau should increase public awareness of the money laundering problem, improve interagency coordination, and boost cooperation between the MSAR and the private sector in combating money laundering. The Government of Macau should ensure that its financial intelligence unit meets Egmont Group standards for information sharing. It should expedite the drafting and issuance of implementing regulations to its new AML and CTF laws. The Government of Macau also should be more proactive in identifying and freezing accounts related to money laundering by weapons proliferators and counterfeiters.

## Malaysia

Malaysia is not a regional center for money laundering. However, its financial sectors are vulnerable to abuse by narcotics traffickers, financiers of terrorism, and criminal elements. Malaysia's relatively lax customs inspection at ports of entry and free trade zones, and its offshore financial services center serve to increase its vulnerability. Though the Government of Malaysia (GOM) has established a "drug-free by 2015" policy and cooperation with the U.S. on combating drug trafficking is excellent, Malaysia's proximity to the heroin production areas and methamphetamine labs of the Golden Triangle leads to smuggling across Malaysian borders, destined for Australia and other markets. Ecstasy from Amsterdam is flown into Kuala Lumpur International Airport for domestic use and distribution to Thailand, Singapore, and Australia.

Malaysia, having enacted laws to combat money laundering, has a developed anti-money laundering system. Malaysia has endorsed the Basel Committee's Core Principles for Effective Banking Supervision, and generally follows international standards related to money laundering, including the Financial Action Task Force (FATF) Forty Recommendations on Money Laundering and the Nine Special Recommendations on Terrorist Financing. Malaysia's National Coordination Committee to Counter Money Laundering (NCC), comprised of members from 13 government agencies, oversaw the drafting of Malaysia's Anti-Money Laundering Act 2001 (AMLA). The NCC also coordinates government-wide anti-money laundering and counterterrorist finance efforts.

Malaysia is a member of the Asia/Pacific Group on Money Laundering (APG),. In 2001, the APG conducted a Mutual Evaluation of Malaysia and its offshore financial center, Labuan. The second round of evaluations is scheduled in February 2007. In preparation for the APG's second round, the NCC has established various working groups to review Malaysia's current anti-money laundering and counter terrorist finance (AML/CTF) measures, laws, regulations, guidelines and framework in an effort to identify possible gaps and to formulate corrective measures.

Subsequent to its 2001 mutual evaluation, Malaysia enacted the AMLA in January 2002, criminalizing money laundering and lifting bank secrecy provisions for criminal investigations involving more than 122 predicate offenses. In 2005, the number of money laundering predicate offences in the Second Schedule to the AMLA was increased from 168 to 185 serious offences from 27 pieces of legislation.

The new predicate offenses were from the Customs Act, Islamic Banking Act, Payment Systems Act, Takaful Act, Futures Industry Act, Securities Commission Act and the Securities Industry Act.

The AMLA also created a financial intelligence unit (FIU), the Unit Perisikan Kewangan, located in the Central Bank, Bank Negara Malaysia (BNM). The FIU is tasked with receiving and analyzing information, and sharing financial intelligence with the appropriate enforcement agencies for further investigations. The Malaysian FIU cooperates with other relevant agencies to identify and investigate suspicious transactions. A comprehensive supervisory framework has been implemented to audit financial institutions' compliance with the AMLA. Currently, BNM maintains 300 examiners who are responsible for money laundering inspections for both onshore and offshore financial institutions. Malaysia's FIU has been a member of the Egmont Group since July 2003. This year Malaysia was elected to be the Asia Chair for the Egmont Committee.

Malaysia's financial institutions have strict "know your customer" rules under the AMLA. Every transaction, regardless of its size, is recorded. Reporting institutions must maintain records for at least six years and report any suspicious transactions to Malaysia's FIU. If the reporting institution deems a transaction suspicious it must report that transaction to the FIU regardless of the transaction size. In addition, cash threshold reporting (CTR) requirements above approximately $13,600 were invoked on banking institutions. FIU officials indicate that they receive regular reports from the AMLA reporting institutions. Reporting individuals and their institutions are protected by statute with respect to their cooperation with law enforcement. While Malaysia's bank secrecy laws prevent general access to financial information, those secrecy provisions are waived in the case of money laundering investigations.

Malaysia has adopted banker negligence (due diligence) laws that make individual bankers responsible if their institutions launder money. Both reporting institutions and individuals are required to adopt internal compliance programs to guard against any offense. Under the AMLA, any person or group that engages in, attempts to engage in, or abets the commission of money laundering, is subject to criminal sanction. All reporting institutions are subject to review by the FIU. Under the AMLA, reporting institutions include financial institutions from the conventional, Islamic, and offshore sectors as well as nonfinancial businesses and professions such as lawyers, accountants, company secretaries, and Malaysia's one licensed casino. In 2005, reporting obligations were invoked on licensed gaming outlets, notaries public, offshore trading agents and listing sponsors. Phased-in reporting requirements for stock brokers and futures brokers were expanded in 2005, and in 2006, reporting requirements were extended to money lenders, pawnbrokers, registered estate agents, trust companies, unit trust management companies, fund managers, futures fund managers, nonbank remittance service providers, and nonbank affiliated issuers of debit and credit cards.

According to a Ministry of Finance report released in September 2006, Islamic banking assets accounted for 11.8 percent of the total assets in the banking sector at the end of June 2006, up from 11.6 percent in June 2005. Malaysia's Islamic finance sector is subject to the same strict supervision to combat financial crime as the commercial banks. A combination of legacy exchange controls imposed after the 1997-98 Asian financial crisis in addition to robust regulation and supervision by BNM makes the Islamic financial sector as unattractive to financial criminals as is the conventional financial sector.

In 1998 Malaysia imposed foreign exchange controls that restrict the flow of the local currency from Malaysia. Onshore banks must record cross-border transfers over approximately $1,360. Since April 2003, an individual form is completed for each transfer above approximately $13,600. Recording is done in a bulk register for transactions between approximately $1,411 and $14,110. Banks are obligated to record the amount and purpose of these transactions.

While Malaysia's offshore banking center on the island of Labuan has different regulations for the establishment and operation of offshore businesses, it is subject to the same anti-money laundering

laws as those governing onshore financial service providers. Malaysia's Labuan Offshore Financial Services Authority (LOFSA) serves as a member of the Offshore Group of Banking Supervisors. Offshore banks, insurance companies, trust companies, trading agents and listing sponsors are required to file suspicious transaction reports under the country's anti-money laundering law. LOFSA is under the authority of the Ministry of Finance and works closely with BNM. LOFSA licenses offshore banks, banking companies, trusts, and insurance companies, and performs stringent background checks before granting an offshore license. The financial institutions operating in Labuan are generally among the largest international banks and insurers. Nominee (anonymous) directors are not permitted for offshore banks, trusts or insurance companies. Labuan had 5,408 registered offshore companies as of June 30, 2006, of which 256 had registered since January this year. Bearer instruments are strictly prohibited in Labuan.

Offshore companies must be established through a trust company. Trust companies are required by law to establish true beneficial owners and submit suspicious transaction reports. There is no requirement to publish the true identity of the beneficial owner of international corporations; however, LOFSA requires all organizations operating in Labuan to disclose information on its beneficial owner or owners, as part of its procedures for applying for a license to operate as an offshore company. LOFSA maintains financial information on licensed entities, releasing it either with the consent of those entities or upon investigation.

In November 2005, LOFSA revoked the license of the "Blue Chip Pathfinder" Private Fund for "evidence that Swift Securities & Investments Ltd had contravened the terms of the consent and acted in a manner that was detrimental to the interests of mutual fund investors." Eleven days later, LOFSA revoked the investment banking license of Swift Securities & Investments Ltd for "contravening the provisions of the license."

In April 2006, LOFSA announced that it had subscribed to a service which provides structured intelligence on high and heightened risk individuals and entities, including terrorists, money launderers, politically exposed persons, arms dealers, sanctioned entities, and others, to gather information on their networks and associates. LOFSA now uses this service as part of its licensing application process.

The Free Zone Act of 1990 is the enabling legislation for free trade zones in Malaysia. The zones are divided into Free Industrial Zones (FIZ), where manufacturing and assembly takes place, and Free Commercial Zones (FCZ), generally for warehousing commercial stock. The Minister of Finance may designate any suitable area as an FIZ or FCZ. Currently there are 13 FIZs and 12 FCZs in Malaysia. The Minister of Finance may appoint any federal, state, or local government agency or entity as an authority to administer, maintain, and operate any free trade zone. Legal treatment for such zones is also different. The time needed to obtain such licenses from the administrative authority for the given free trade zone depends on the type of approval. Clearance time ranges from two to eight weeks. There is no information available suggesting that Malaysia's free industrial and free commercial zones are being used for trade-based money laundering schemes or by the financiers of terrorism. However, the Government of Malaysia (GOM) considers these zones as areas outside the country and they receive lenient tax and customs treatment relative to the rest of the country.

In April 2002, the GOM passed the Mutual Assistance in Criminal Matters Bill, and in July 2006 concluded a Mutual Legal Assistance Treaty with the United States. Malaysia concluded a similar treaty among like-minded ASEAN member countries in November 2004. In October 2006, Malaysia ratified treaties with China and Australia regarding the provision of mutual assistance in criminal matters. An extradition treaty was also signed with Australia. The mutual assistance treaties enable States Parties to assist each other in investigations, prosecutions, and proceedings related to criminal matters, including terrorism, drug trafficking, fraud, money laundering and human trafficking.

In 2004, Malaysia made its first money laundering arrest. As of December 31, 2005, six individuals were being prosecuted for money laundering offences involving a total of 196 charges with fines amounting to approximately $19.5 million. In December 2005, one person was convicted of a money laundering offence amounting to approximately $23,423. From January through November 2006, 14 additional individuals had been charged, bringing the total number of people being prosecuted for money laundering to 20 with fines amounting to approximately $71.97 million.

Malaysia cooperates with regional, multilateral, and international partners to combat financial crimes and permits foreign countries to check the operations of their bank branches.

The FIU has signed memoranda of understanding (MOUs) on the sharing of financial intelligence with the FIUs of Australia, Indonesia, Thailand, the Philippines and China. MOUs with the United Kingdom, United States, Japan, South Korea, Netherlands Antilles, Finland, Albania, Argentina, Cook Islands, Mexico, Sri Lanka, Ukraine, Peru and India are at various stages of negotiation.

Malaysia is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. The GOM has agreed in principle to accede to the UN Convention for the Suppression of the Financing of Terrorism, and is expected to bring into force amendments to five different pieces of legislation. Parliament passed amendments to the Anti-Money Laundering Act, the Penal Code, the Subordinate Courts Act, the Courts of Judicature Act, and the Criminal Procedure Code. All five amendments have been accorded Royal Assent and are awaiting Ministerial instructions to bring these amendments into force. These amendments will increase penalties for terrorist acts, allow for the forfeiture of terrorist-related assets, allow for the prosecution of individuals who have provided material support for terrorists, expand the use of wiretaps and other surveillance of terrorist suspects, and permit video testimony in terrorist cases.

The GOM has cooperated closely with U.S. law enforcement in investigating terrorist-related cases since the signing of a joint declaration to combat international terrorism with the United States in May 2002. The GOM has the authority to identify and freeze the assets of terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, and has issued orders to all licensed financial institutions, both onshore and offshore, to do so. The Ministry of Foreign Affairs opened the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) in August 2003. The SEARCCT has hosted a series of counterterrorism courses and seminars, including training on counter terrorist finance.

BNM and SEARCCT jointly organized a series of workshops and dialogues for reporting institutions with the participation of regulatory and law enforcement agencies. Malaysia offers interactive computer-based training in anti-money laundering developed by the UN Office on Drugs and Crime and the World Bank. In addition, BNM together with members of the NCC has developed an eight-module Accreditation of Financial Investigators Program for AMLA investigators. Ongoing training enhances the capabilities of graduates of the computer-based programs, including the legal aspects of anti-money laundering, investigative procedures, analysis of net worth, forensic accounting, and computer forensics.

The GOM has rules regulating charities and other nonprofit entities. The Registrar of Societies is the principal government official who supervises and controls charitable organizations, with input from the Inland Revenue Board (IRB) and occasionally the Companies Commission of Malaysia (CCM). The Registrar mandates that every registered society of a charitable nature submits its annual returns, including its financial statements. Should activities deemed suspicious be found, the Registrar may revoke the nonprofit organization's (NPO) registration or file a suspicious transaction report. Registering as a NPO can be bureaucratic and time-consuming. One organization reported that getting registered took nine months and required multiple personal interviews to answer questions about its mission and its methods. Some NPOs reportedly register as "companies" instead, a quick and inexpensive process requiring capital of approximately 54 cents and annual financial statements. In

March 2006, the FIU completed a review of the nonprofit sector with the Registrar, the IRB, and CCM in an effort to ensure that the laws and regulations were adequate to mitigate the risks of nonprofit organizations as conduits for terrorism financing. BNM reports that the review did not show any significant regulatory weaknesses; however, the GOM is considering measures to enhance the monitoring of fundraising, including increased disclosure requirements of how funds are spent.

Malaysia's tax law allows a tax credit for contributions to mosques or Islamic charitable organizations (zakat, as required by Islam) encouraging the reporting of such contributions. There is no similar tax credit for non-Muslims. Islamic zakat contributions can be taken as payroll deductions, adding another tool to help prevent the abuse of charitable giving.

The FIU has provided capacity building and training in anti-money laundering efforts to some of its ASEAN partners, including Cambodia, Laos, and Vietnam. In February 2006, the Asian Development Bank (ADB) funded a team from Malaysia's FIU to run a workshop in Laos for two state-owned banks and to provide technical assistance in the drafting of Laos's anti-money laundering compliance procedures. This was completed in October 2006.

The Malaysian government continues to receive training towards the more effective use of existing "Aiding and Abetting" laws to prosecute drug kingpins and their organizations.

The Government of Malaysia (GOM) should enact an imminent effective date for the five recent amendments criminalizing the financing of terrorism. This also will allow Malaysia to accede to the UN International Convention for the Suppression of the Financing of Terrorism. Malaysia also should continue to enhance its cooperation with on a regional, multilateral, and international basis. The GOM should improve enforcement of regulations regarding its free trade zones, which remain vulnerable to the financing of terrorism and money laundering. Perhaps most importantly, the GOM should implement stricter border control measures.

## Mexico

Mexico is a major drug-producing and drug-transit country; it also serves as one of the major conduits for proceeds from illegal drug sales leaving the United States. The illicit drug trade is believed to be the principal source of funds laundered through the Mexican financial system. Corruption, kidnapping, trafficking in firearms and immigrants, and other crimes are other major sources of illegal proceeds being laundered. The smuggling of bulk shipments of U.S. currency into Mexico and the movement of the cash back into the United States via couriers, armored vehicles and wire transfers remain favored methods for laundering drug proceeds. Mexico's financial institutions are vulnerable to currency transactions involving international narcotics trafficking proceeds that include significant amounts of U.S. currency derived from illegal drug sales in the United States.

Currently, there are 29 commercial banks and 71 foreign financial representative offices operating in Mexico, as well as 86 insurance companies, 166 credit unions and 25 money exchange houses. Commercial banks, foreign exchange companies and general commercial establishments are allowed to offer money exchange services. Although the underground economy is estimated to account for 20-40 percent of Mexico's gross domestic product, the informal economy is considered to be much less significant with regard to money laundering than the narcotics-driven segments of the economy.

Beginning in 2005, permits were issued for casinos to operate in Mexico. Gambling is also legally allowed through national lotteries, horse races and sport pools. Casinos, offshore banks, lawyers, accountants, couriers and brokers are currently not subject to anti-money laundering (AML) reporting requirements.

In 2005, Mexico established three strategic financial zones: two in San Luis Potosi and one in Chiapas. These zones, similar to free trade zones, allow tax exemptions for inputs to exports that are imported

or produced locally. Additional strategic financial zones are planned to be established in the states of Queretaro, Quintana Roo and Lazaro Cardenas. The Mexican Customs agency certifies companies operating in these zones under the authority provided by Article 135 of the Customs Law. There is no indication that these zones are being used in trade-based money laundering or terrorist financing.

Since 2000, Mexicans have received more than $100 billion in remittances. Approximately $23.1 billion in remittances were received in 2006 alone. Many U.S. banks have partnered with their Mexican counterparts to develop systems to simplify and expedite the transfer of money, including wider acceptance by U.S. banks of the "matricula consular." The matricula consular is an identification card issued by Mexican consular offices to Mexican citizens residing in the United States that has been criticized as insecure. In some cases, the sender or the recipient can simply provide the matricula consular as identification and pay a flat fee to receive a remittance; neither is required to open a bank account in the United States or Mexico. Although these systems have been designed to make the transfer of money faster and less expensive for the customers, the rapid movement of such vast sums of money by persons of questionable identity leaves the systems open to potential money laundering and exploitation by organized crime groups. As a result of the increased availability of these electronic transfers, the U.S. embassy estimates that electronic transfers accounted for 90 percent of remittances to Mexico in 2006.

According to U.S. law enforcement officials, Mexico remains one of the most challenging money laundering jurisdictions for the United States, especially with regard to the investigation of money laundering activities involving the cross-border smuggling of bulk currency derived from drug transactions. Sophisticated and well-organized drug trafficking organizations based in Mexico are able to take full advantage of the extensive United States-Mexico border and the large flow of licit remittances. In addition, the combination of a sophisticated financial sector and weak regulatory controls facilitates the concealment and movement of drug proceeds. U.S. officials estimate that since 2003, as much as $22 billion may have been repatriated to Mexico from the U.S. by drug trafficking organizations. In April 2006, the U.S. Department of Treasury issued a warning to the U.S. financial sector on the potential use of certain Mexican financial institutions, including Mexican casas de cambio, to facilitate bulk cash smuggling. Corruption is also a concern: in recent years, various Mexican officials have come under investigation for alleged money laundering activities.

In 2006, U.S. authorities observed a significant increase in the number of complex money laundering investigations by the Financial Crimes Unit of the Office of the Deputy Attorney General Against Organized Crimes (SIEDO), including cases coordinated with U.S. officials. As a result of the cooperation of Mexican Customs, SIEDO and various U.S. agencies, Mexico seized over $25 million in 2006. As of November, SIEDO had initiated 142 criminal investigations into money laundering cases in 2006, 77 of which were brought to trial. The U.S. Treasury Department's Office of Foreign Asset Control (OFAC) announced in June 2006 the designation of the Amezcua Contreras Organization as a Tier I target involved in significant narcotics trafficking under the Foreign Narcotics Kingpin Designation Act. In July and September 2006, OFAC also announced designations of 45 Tier II targets associated with the previously-designated Arrellano Felix and Arriola Marquez drug trafficking organizations. The designations are a result of cooperation among OFAC, other U.S. government entities and SIEDO. They allow U.S. and Mexican authorities to seek the freezing of assets of Mexican drug cartels, hindering their ability to take advantage of the U.S. and Mexican financial systems.

The Government of Mexico (GOM) continues its efforts to create and implement an anti-money laundering program that meet such international standards as those of the Financial Action Task Force (FATF), which Mexico joined in June 2000. Money laundering related to all serious crimes was criminalized in 1996 under Article 400 bis of the Federal Penal Code and is punishable by imprisonment of from five to fifteen years and a fine. Penalties are increased when a government

official in charge of the prevention, investigation or prosecution of money laundering commits the offense.

In 1997, the GOM established a financial intelligence unit under the Ministry of the Treasury, which became known as the Unidad de Inteligencia Financiera (UIF) in 2004 with the consolidation of all the Treasury offices responsible for investigating financial crimes into the UIF. The UIF is responsible for receiving, analyzing and disseminating financial reports from a wide range of obligated entities. The UIF also reviews all crimes linked to Mexico's financial system and examines the financial activities of public officials. The UIF's personnel number approximately 70 and are comprised mostly of forensic accountants, lawyers and analysts. Its director reports to the Minister of Finance.

Regulations have been implemented for banks and other financial institutions (mutual savings companies, insurance companies, financial advisers, stock markets, credit institutions, exchange houses and money remittance businesses) to know and identify customers and maintain records of transactions. These entities must report to the UIF any suspicious transactions, transactions over $10,000, and transactions involving employees of financial institutions who engage in unusual activity. Financial institutions with a reporting obligation also require occasional customers performing transactions equivalent to or exceeding $3,000 in value to be identified, so that the transactions can be aggregated daily to prevent circumvention of the requirements to file cash transaction reports (CTRs) and suspicious transaction reports (STRs). Financial institutions also have implemented programs for screening new employees and verifying the character and qualifications of their board members and high-ranking officers. Real estate brokerages, attorney, notaries, accountants and dealers in precious metals and stones are required under a November 2005 provision of the tax law to report all transactions exceeding $10,000 to the UIF, via the Tax Administration Service (SAT). As of 2006, nonprofit organizations are also subject to reporting requirements on donations greater than $10,000. In 2005, the UIF received over 4 million CTRs and approximately 57,700 STRs from obligated entities; corresponding data for 2006 is not available.

In December 2000, Mexico amended its Customs Law to reduce the threshold for reporting inbound cross-border transportation of currency or monetary instruments from $20,000 to $10,000. At the same time, it established a requirement for the reporting of outbound cross-border transportation of currency or monetary instruments of $10,000 or more. These reports are also received by the UIF and cover a wider range of monetary instruments (e.g. bank drafts) than those required by the United States.

Following the analysis of CTRs, STRs and reports on the cross-border movements of currency, the UIF sends reports that are deemed to require further investigation, and have been approved by Treasury's legal counsel, to the Office of the Attorney General (PGR). As of October, the UIF had sent 45 cases to the PGR in 2006. The PGR's special financial crimes unit is part of SIEDO, which works closely with the UIF in carrying out money laundering investigations. In addition to working with SIEDO, UIF personnel have initiated working-level relationships with other federal law enforcement entities, including the Federal Investigative Agency (AFI) and the Federal Preventive Police (PFP), in order to support the investigations of criminal activities with ties to money laundering. In 2006, the UIF signed memoranda of understanding (MOUs) with the Economy Secretariat and the immigration authorities that allows the UIF access to their databases. The UIF has also signed agreements with the National Banking Commission (CNBV) and the National Commission of Insurance and Finance (CNSF) to coordinate methods to prevent money laundering and terrorist financing, and is currently finalizing similar negotiations with the Treasury and the National Savings Commission (CNSAR).

Since undergoing its second mutual evaluation by the FATF in 2003, the GOM has been subject to monitoring by FATF and has submitted several reports on the progress made since its evaluation. The evaluation team found in 2003 that the GOM had made progress since the first mutual evaluation by removing specific exemptions to customer identification obligations, implementing on-line reporting

forms and a new automated transmission process for reporting transactions to the UIF, reducing the delay in reporting transactions overall, and developing an overall anti-money laundering strategy. However, the FATF evaluation team also identified a number of deficiencies in the system. These deficiencies include the lack of a separate criminal offense of terrorist financing, and strict bank and trust secrecy, which are considered impediments to investigations and prosecutions. As a result of these deficiencies, the GOM must update the FATF on its progress, which it did at the June and October 2005 and February 2006 plenary meetings of the FATF.

While Mexico has not yet criminalized terrorist financing, it has made improvements to its bank secrecy laws. Amendments to the Banking Law approved in April and December 2005 now allow specific government entities, such as the PGR and the state attorneys general, to receive records directly from banks and credit institutions without prior approval from the CNBV. Financial institutions must respond to these requests within three days.

In November 2003, the Senate passed a bill amending the Federal Penal Code that would link terrorist financing to money laundering. However, the lower house failed to act on this bill. In 2005, the draft legislation was re-submitted as two separate draft laws: one to criminalize the financing of terrorism and one to address outstanding international cooperation issues. If passed, this legislation would bring Mexico into compliance with international standards. The proposed amendments would also create two new crimes: conspiracy to launder assets and international terrorism (when committed in Mexico to inflict damage on a foreign state). The draft legislation is still under consideration in the Senate.

While Mexico does not have a specific offense criminalizing the financing of terrorism, money laundering associated with terrorism is punishable under the existing Penal Code. The GOM has responded positively to U.S. Government efforts to identify and block terrorist-related funds. It continues to monitor suspicious financial transactions, although no assets related to terrorism have been frozen to date.

Although the United States and Mexico both have forfeiture laws and provisions for seizing assets abroad derived from criminal activity, U.S. requests of Mexico for the seizure, forfeiture and repatriation of criminal assets have not often met with success. Mexican authorities have difficulties forfeiting assets seized in Mexico if these assets are not clearly linked to narcotics. Although Mexican officials have made significant progress in modernizing their approach to asset seizure, actual asset forfeiture remains a challenge.

Mexico has developed a broad network of bilateral agreements and regularly meets in bilateral law enforcement working groups with the United States. The U.S.-Mexico Mutual Legal Assistance Treaty entered into force in 1991. Mexico and the United States also implement other bilateral treaties and agreements for cooperation in law enforcement issues, including the Financial Information Exchange Agreement (FIEA) and the Memorandum of Understanding (MOU) for the exchange of information on the cross-border movement of currency and monetary instruments. In addition to its membership in the FATF, Mexico participates in the Caribbean Financial Action Task Force as a cooperating and supporting nation. In 2006, Mexico also became a member of the South American Financial Action Task Force (GAFISUD), after previously participating in GAFISUD as an observer member. The UIF is a member of the Egmont Group, and Mexico participates in the OAS/CICAD Experts Group to Control Money Laundering. The GOM is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, the UN International Convention for the Suppression of the Financing of Terrorism and the Inter-American Convention Against Terrorism. The UIF has signed memoranda of understanding for the exchange of information with 22 other financial intelligence units, including the U.S. financial intelligence unit, FinCEN.

To create a more effective AML regime, Mexico should fully implement and improve its mechanisms for asset forfeiture and money laundering cooperation with the United States and increase efforts to

control the bulk smuggling of currency across its borders. The GOM should also closely monitor remittance systems for possible exploitation by criminal or terrorist groups. Mexico should enact its proposed legislation to criminalize the financing and support of terrorists and terrorist organizations. Despite a strengthened regulatory framework, improved cooperation among law enforcement authorities and a strong public campaign against corruption, Mexico continues to face challenges in prosecuting and convicting money launderers, and should continue to focus its efforts on improving its ability to combat money laundering, terrorist financing and other financial crimes.

## Moldova

Moldova is not considered an important regional financial center. Moldova remains predominantly a cash-based society and people reportedly have little faith in banks. Criminal proceeds laundered in Moldova are derived from both domestic and foreign criminal activity. Organized crime syndicates are active in the country. Widespread corruption in both commerce and government exacerbates the situation. There is a large underground economy in Moldova. Smuggling of consumer goods, including counterfeit items, is common. Moldova is also recognized as a major source country for trafficking in persons. A rise in internet-related fraud schemes is evident. Moldova has approximately five casinos, but they are neither well regulated nor controlled.

Additional money laundering threats are found in the separatist region of Trans-Dniester—a narrow strip of land between the Dniester River and the Ukrainian border—which proclaimed independence from Moldova in 1990. Trans-Dniester contains most of Moldova's industrial infrastructure, but its economic potential is limited by its international isolation. The region is plagued by corruption, organized crime and smuggling. There are persistent reports of Trans-Dniester illegal arms sales, narcotics trafficking, and of being the base of operations for Russian and Ukrainian organized crime syndicates.

Money laundering became a criminal offense in Moldova November 2001, and the law was amended in June 2002. It remained unchanged when the new criminal code was adopted in June 2003. The legislation applies to proceeds of "all crimes," not just narcotics activity, with banks and nonbank financial institutions (NBFIs) required to report transactions over a certain amount to the Center for Combating Economic Crimes and Corruption (CCECC). On July 1, 2004, the Law on Money Laundering was amended to raise the reporting threshold from 100,000 lei to 300,000 lei (approximately $8,040 to $24,100) for individuals, and from 200,000 lei to 500,000 (approximately $16,100 to $40,200) for legal entities. However, the amendments still require reporting transactions under the threshold if, when combined with other transactions during a one-month period, they reach a total which crosses that threshold. This amendment may actually increase the amount of reporting required. Current anti-money laundering legislation also covers gold, gems, and precious metals.

Banks must maintain transfer records for a period of five years after an account opens or after any financial transaction takes place and seven years after foreign currency contract transactions, whichever is later. They have submitted suspicious transactions reports (STRs), as required, since the law was enacted. However, Moldovan legislation exempts foreign nationals from being subject to STR reporting. Both banks and NBFIs are protected from criminal, civil, and administrative liability asserted as a result of their compliance with the reporting requirements, and no secrecy laws exist that would prevent law enforcement or banking authorities from accessing financial records. A May 2003 amendment states that forwarding such information to law enforcement entities or the courts is not a breach of confidentiality, as long as it is done in accordance with the regulations. Current legislation contains provisions authorizing sanctions of commercial banks for negligence.

Government of Moldova (GOM) efforts against the international transportation of illegal-source currency and monetary instruments largely focus on cross-border currency reporting forms, completed at ports of entry by travelers entering Moldova. It is not clear if these efforts are successful.

The CCECC houses Moldova's Financial Intelligence Unit (FIU). In 2004, the CCECC established an FIU from within, by creating a money laundering section of ten investigators to pursue suspicious financial transactions. Under Moldovan criminal procedure, cases first undergo a preliminary investigation by operative investigators before being sent to criminal investigators and prosecutors who decide whether a full investigation will be launched. The FIU is not a member of the Egmont Group, although it has been a candidate for membership since 2004. Reportedly, the FIU has drafted a new anti-money laundering/counterterrorist financing (AML/CTF) law, which is to be submitted to Parliament in early 2007. The legislation was developed with technical assistance from the Council of Europe.

Moldova is not considered an offshore financial center, and only two foreign banks exist in Moldova: "Banca Comerciala Romana," a Romanian bank; and "Unibank," in which the Russian bank "Petrocomert" holds 100 percent of the shares. These banks are regulated in the same manner as Moldovan commercial banks. Offshore banks are permitted, so long as they are licensed and background checks are conducted on shareholders and bank officials. Nominee (anonymous) directors are not allowed, and banks do not permit bearer shares. The Ministry of Finance (MOF) currently licenses five casinos, although they are reportedly not well regulated or controlled.

Reportedly, the GOM is seriously considering a package of amendments to existing legislation that would allow Moldova to emerge as a significant offshore center in the region. The GOM has indicated publicly that the proposed changes are designed to attract substantial inflows of capital and provide a much-needed economic boost to one of the poorest countries in Europe. According to the current draft of the proposed amendments, the changes call for a sharp decrease in reporting requirements and an increase in financial secrecy, including the ability to establish "anonymous" stock companies. As drafted, neither banks nor law enforcement would be able to determine the beneficial owner of legal entities, and the law would provide what would effectively equate to a fee schedule for the "legalization" of money of dubious origin. If passed in their current form, the amended laws would violate FATF recommendations and call into question Moldova's compliance with and commitment to international AML/CFT standards.

Article 106 of the Moldovan criminal code, enacted June 12, 2003, relates specifically to asset seizure and confiscation. The article, titled "Special Seizures," describes a special seizure as the forced transfer of ownership of goods used during, or resulting from, a crime to the state. The article may be applied to goods belonging to persons who knowingly accept assets acquired illegally, even when prosecution is declined. However, it remains unclear whether asset forfeiture may be invoked against those unwittingly involved in or tied to an illegal activity. Money laundering crimes are the purview of the CCECC, while narcotics-related seizures are within the jurisdiction of the Ministry of Interior (MOI). The GOM currently lacks adequate resources, training, and experience to trace and seize assets effectively. There are no accurate statistics available on seizures or confiscation.

Moldova codified the criminalization of terrorist financing in the Law on Combating Terrorism, enacted November 12, 2001. Article 2 defines terrorist financing, and Article 8/1 authorizes suspension of terrorist and related financial operations. Current GOM capabilities to identify, freeze, and seize terrorist assets are rudimentary, with investigators lacking advanced training and resources. While the NBM receives and regularly distributes the UNSCR 1267 Sanctions Committee's consolidated list of suspected terrorists, no related assets have been identified, frozen, or seized in Moldova. Investigation into misuse of charitable or nonprofit entities is non-existent, as the GOM has neither the resources nor ability to perform these tasks. In December 2004, the Parliament amended the law on money laundering to include provisions on terrorist financing. Moldova has made no arrests for terrorist financing. Moldova is a party to the UN International Convention for the Suppression of the Financing of Terrorism.

No agreements, bilateral or otherwise, exist between the USG and the GOM regarding the exchange of records in connection with narcotics, terrorism, terrorist financing, or other serious criminal

investigation. Current legislation does not prohibit cooperation on a case-by-case basis. GOM authorities continue to solicit USG assistance on individual cases and cooperate with U.S. law enforcement personnel when presented with requests for information/assistance. There are no known cases of GOM refusal to cooperate with foreign governments or of sanctions or penalties being imposed upon the GOM for a failure to cooperate.

Moldova is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime. Moldova has signed an agreement with CIS member states for the exchange of information on criminal matters, including money laundering. In 2004, the CCECC was accepted as an observer at the Eurasian Group on Combating Money Laundering and as a candidate in the Egmont Group. Moldova is a member of the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL).

In December, 2006 Moldova signed a $24.7 million Threshold Country Program with the Millennium Challenge Account that focuses on anticorruption measures. The GOM requested funding to address areas of persistent corruption including in the judiciary, health care system, and tax, customs and police agencies. Moldova is listed as 79 out of 163 countries in Transparency International's 2006 Corruption Perception Index.

The Government of Moldova should enhance its existing anti-money laundering/counterterrorist financing regime. The regime should adhere to internationally accepted standards. Moldova should improve the mechanisms for sharing information and forfeiting assets. Additionally, Moldova should provide appropriate training for its law enforcement personnel involved in the asset forfeiture program. Border enforcement and antismuggling enforcement should be priorities. Moldova should take specific steps to counter corruption and should become a party to the UN Convention on Transnational Organized Crime and the UN Convention against Corruption. Moldova should not pursue proposed legislative changes on offshores that would make Moldova's financial sector less transparent and more vulnerable to money laundering, terrorist financing, and other forms of illicit finance. As a member of MONEYVAL, the Government of Moldova has committed to adhering to the international standards set by the Financial Action Task Force to combat money laundering and terrorist financing. Establishing an offshore shore financial sector would belie that commitment.

## Monaco

The second-smallest country in Europe, the Principality of Monaco is known for its tradition of bank secrecy, network of casinos, and favorable tax regime. Money laundering offenses relate mainly to offenses committed abroad. Russian organized crime and the Italian Mafia reportedly have laundered money in Monaco. The principality reportedly does not face the ordinary forms of organized crime, and the crime that does exist does not seem to generate significant illegal proceeds, with the exception of fraud and offenses under the "Law on Checks." Monaco remains on an OECD list of so-called "noncooperative" countries in terms of provision of tax information.

Monaco has a population of approximately 32,000, of which fewer than 7,000 are Monegasque nationals. Monaco's approximately 60 banks and financial institutions hold more than 300,000 accounts and manage total assets of about 70 billion euros (approximately $91 billion). Approximately 85 percent of the banking customers are nonresident. In 2005, the financial sector represented 15 percent of Monaco's economic activity. The high prices for land throughout the principality result in a real estate sector of considerable import. There are four casinos run by the Société des Bains de Mer, in which the state holds a majority interest.

Monaco's banking sector is linked to the French banking sector through the Franco-Monegasque Exchange Control Convention signed in 1945 and supplemented periodically, most recently in 2001.

Through this convention, Monaco operates under the banking legislation and regulations issued by the French Banking and Financial Regulations Committee, including Article 57 of France's 1984 law regarding banking secrecy. The majority of entities in Monaco's banking sector concentrates on portfolio management and private banking. Subsidiaries of foreign banks operating in Monaco may withhold customer information from the parent bank.

Although the French Banking Commission supervises Monegasque institutions, Monaco shoulders the responsibility for legislating and enforcing measures to counter money laundering and terrorism financing. The Finance Counselor, located within the Government Council, is responsible for anti-money laundering (AML) implementation and policy.

Money laundering in Monaco has been criminalized by Act 1.162 of July 7, 1993, "On the Participation of Financial Institutions in the Fight against Money Laundering," and Section 218-3 of the Criminal Code, amended by Act 1.253 of July 12, 2002, "Relating to the Participation of Financial Undertakings in Countering Money Laundering and the Financing of Terrorism." On November 9, 2006, Section 218-3 of the Criminal Code was modified to adopt an "all crimes" approach.

The original AML legislation requires banks, insurance companies, and stockbrokers to report suspicious transactions and to disclose the identities of those involved. Casino operators must alert the government of suspicious gambling payments possibly derived from drug-trafficking or organized crime. The law imposes a five-to-ten-year jail sentence for anyone convicted of using illicit funds to purchase property, which itself is subject to confiscation.

The 2002 amendments to Act 1.162 expanded the scope of AML reporting requirements to include corporate service providers, portfolio managers, some trustees, and institutions within the offshore sector. The Act instituted new procedural requirements regarding internal compliance, client identification, and records retention and maintenance. Sovereign Order 16.615 of January 11, 2005, and Sovereign Order 631 of August 10, 2006, mandate additional customer identification measures.

Offshore companies are subject to the same due diligence and suspicious reporting obligations as banking institutions, and Monegasque authorities conduct on-site audits. The 2002 legislation strengthened the "know your client" obligations for casinos and obliges companies responsible for the management and administration of foreign entities not only to report suspicions to Monaco's financial intelligence unit (FIU), but also to implement internal AML and counterterrorist financing (CTF) procedures. The FIU monitors these activities.

Banking laws do not allow anonymous accounts, but Monaco does permit the existence of alias accounts, which allow account owners to use pseudonyms in lieu of their real names. Cashiers do not know the clients, but the banks know the identities of the customers and retain client identification information.

Prior approval is required to engage in any economic activity in Monaco, regardless of its nature. The Monegasque authorities issue approvals based on the type of business to be engaged in, the location, and the length of time authorized. This approval is personal and may not be re-assigned. Any change in the terms requires the issuance of a new approval.

Monaco's FIU, known in French as the Service d'Information et de Controle sur les Circuits Financiers (SICCFIN), receives suspicious transaction reports, analyzes them, and forwards them to the prosecutor when they relate to drug-trafficking, organized crime, terrorism, terrorist organizations, or the funding thereof. SICCFIN also supervises the implementation of AML legislation. Under Law 1.162, Article 4, SICCFIN may suspend a transaction for twelve hours and advise the judicial authorities to investigate. SICCFIN has received between 200 and 400 suspicious transaction reports (STRs) annually from 2000 to 2005. In 2005, SICCFIN received 375 STRs, about 60 percent of which were submitted by banks and other financial institutions. SICCFIN received 63 requests for financial information from other FIUs in 2005.

Investigation and prosecution are handled by the two-officer Money Laundering Unit (Unite de Lutte au Blanchiment) within the police. The Organized Crime Group (Groupe de Repression du Banditisme) may also handle cases. Seven police officers have been designated to work on money laundering cases. Four prosecutions for money laundering have taken place in Monaco, which have resulted in three convictions.

Monaco's legislation allows for the confiscation of property of illicit origin as well as a percentage of co-mingled illegally acquired and legitimate property. Authorities must obtain a court order in order to confiscate assets. Confiscation of property related to money laundering is restricted to the offenses listed in the Criminal Code. Authorities have seized assets exceeding 11.7 million euros (approximately $15.2 million) in value. Monaco has extradited criminals, mainly to Russia, and has largely completed negotiations with the United States on a seized asset sharing agreement.

In July and August 2002, Monaco passed Act 1.253 and promulgated two Sovereign Orders intended to implement United Nations Security Council Resolution 1373 by outlawing terrorism and its financing, as well as additional Sovereign Orders in April and August of that year importing into Monegasque law the obligations of the UN Convention for the Suppression of the Financing of Terrorism. In 2006, Monaco further amended domestic law to implement these obligations.

The Securities Regulatory Commissions of Monaco and France signed a memorandum of understanding (MOU) on March 8, 2002, on the sharing of information between the two bodies. The Government of Monaco considers this MOU an important tool to combat financial crime, particularly money laundering. SICCFIN has signed information exchange agreements with thirteen counterparts and is a member of the Egmont Group.

Monaco was admitted to the Council of Europe on October 4, 2004. In 2002, Monaco became a member of the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). Monaco is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

Monaco should amend its legislation to implement full corporate criminal liability. The Principality should continue to enhance its anti-money laundering and confiscation regimes by applying its AML reporting, customer identification, and record keeping requirements to all trustees, as well as Monegasque gaming houses. Monaco should also eliminate the ability to open and maintain accounts using an alias, and banks should include their cashiers in customer identification responsibilities. Monaco should become a party to the UN Convention against Corruption. SICCFIN should have the authority to forward reports and disseminate information to law enforcement even when the report or information obtained does not relate specifically to drug trafficking, organized crime, or terrorist activity or financing.

## Montenegro

The Republic of Montenegro declared independence from the State Union of Serbia and Montenegro on June 3, 2006. Montenegro is located on the Balkan Peninsula in southeastern Europe, bordering the Adriatic Sea to the west, and sharing land borders with Croatia, Bosnia and Herzegoviva, Serbia and Albania. Montenegro has a population of about 630,000.

Montenegro continues to have a significant black market for smuggled goods. Illegal proceeds are generated from drug trafficking, official corruption, tax evasion, organized crime and other types of financial crimes. Proceeds from illegal activities are being heavily invested in all forms of real estate. The construction and renovation of commercial buildings such as offices, apartments, high-end retail businesses as well as personal residences is evident in the capital city Podgorica as well as other major

cities. Investment by foreign individuals and businesses in expensive real estate along the Montenegro coast has raised prices and generated concerns about the source of funds used for these investments.

Tax evasion, which is a predicate crime for money laundering, and trade-based money laundering in the form of over-and-under-invoicing, are common methods used to launder money. In Montenegro, the difficulty of convicting a suspect of money laundering without a conviction for the original criminal act and the unwillingness of the courts to accept circumstantial evidence to support money laundering or tax evasion charges is hampering law enforcement and prosecutors in following the movement and investment of illegal proceeds and effectively using the anti-money laundering laws.

In August 2002, the Central Bank of Montenegro (CBCG) issued a decree that requires banks and other financial institutions to report suspicious transactions, establish anti-money laundering control programs, and train their employees to detect money laundering. The CBCG dissolved all offshore banks for failure to re-register and reestablish themselves as regular banks. The Finance Ministry has not released complete information about the actual disposition of the 400 offshore entities whose names they turned over to CBCG. Currently, neither offshore entities, nor free trade zones, are authorized by Montenegro.

Money laundering was criminalized in 2002, and the Criminal Code was amended in June 2003 to enable the government to confiscate money and property involved in criminal activity. Additionally, according to the Criminal Code, business licenses of legal or natural persons may be revoked and business activities banned if the subject is found guilty of criminal activities, including narcotics trafficking or terrorist financing. In April 2004, Montenegro further amended its Criminal Procedure Code to bring it into conformity with the standards of the Council of Europe.

The Government of Montenegro (GOM) passed anti-money laundering legislation on September 24, 2003. The law obliges banks, post offices, state entities, casinos, lotteries and betting houses, insurance companies, jewelers, travel agencies, auto and boat dealers, and stock exchange entities to file currency transaction reports (CTRs) on all transactions exceeding 15,000 euros (approximately $19,000). Financial institutions are also obliged to report suspicious transactions, regardless of the amount of the transaction. All reporting by banking institutions is forwarded electronically to Montenegro's financial intelligence unit (FIU), called the Administration for the Prevention of Money Laundering, or APML. Failure to report, according to the law, could result in fines up to $26,000 as well as sentences of up to 12 years. Legislation in force since 2005 expanded Montenegro's money laundering law to include attorneys and exchange houses as obligated entities. A newly formed interagency working group is discussing and developing relevant amendments to the anti-money laundering legislation to bring it into conformity with the third EU Directive on Money Laundering.

Montenegro's FIU, the Administration for the Prevention of Money Laundering and Terrorist Finance (APML), is an independent agency which has the authority to collect, analyze and disseminate currency reports to the competent authorities for further action. The FIU became operational in November 2003 and began receiving reports of transactions in July 2004. However, APML has developed no guidelines regarding what should be considered a suspicious transaction.

The Montenegro FIU became an Egmont member in June 2005. It has executed a number of Memoranda of Understanding to exchange information with most established FIUs in the region, as well as with counterpart nonregional states, such as Russia and Ukraine. APML has also signed memoranda of cooperation with law enforcement bodies from the ministries of Justice and Customs, the tax authority and the Central Bank. However, the European Commission found that Montenegro must "substantially upgrade" its coordination and information exchange among these entities in order to effectively address money laundering issues.

In the first nine months of 2006, Montenegro's FIU received over 100,000 CTRs and 152 reports of suspicious transactions. Over 70,000 of the CTRs were filed by the stock exchange and nearly 30,000

were filed by banks. The FIU initiated the analysis of 106 transactions and referred 20 cases to other responsible government agencies for further action. The referrals resulted in 15 cases where subject accounts were blocked for 72 hours in order to permit further investigation of the transactions. In 2005, Montenegro blocked a total of $10.9 million. During the first eight months of 2006, this figure had increased to $23.4 million.

Montenegro can seize and forfeit assets. In September 2004, the Government of Montenegro seized over $1 million in undeclared currency in connection with the arrest of two Chinese nationals attempting to enter Montenegro. Further investigation revealed that these individuals had moved over $4 million in illicit funds through bank accounts in Montenegro. The two Chinese nationals' convictions were upheld on appeal, and on September 29, 2006 each was sentenced to one year in prison.

Montenegro is vulnerable to smuggling, particularly stolen cars, narcotics, cigarettes, and counterfeit goods. Customs and law enforcement authorities have expressed concern about trade-based money laundering. Customs is required to report cross-border movements of cash, checks, securities and precious metals and stones with values exceeding 15,000 euros.

Montenegro has criminalized the financing of terrorism and in March 2005 has subsequently adopted amendments to its laws on terrorism and terrorist financing in order to bring Montenegrin law into conformance with international standards. Responsibility for the detection and prevention of terrorist financing was transferred in 2004 from the CBCG to the FIU. The FIU circulates to banks and other financial institutions the names of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanction Committee's consolidated list. Montenegro has identified a small number of terrorism financing cases. These cases, however, were not related to entities sanctioned by the UN Security Council.

Because of the demise of the State Union of Serbia and Montenegro, Serbia became the legacy member of the United Nations and the Council of Europe. Montenegro has obtained UN membership and its membership in the Council of Europe is pending. Because of these events, the GOM is now an observer in the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) rather than a member. Montenegro is working on preparing an updated progress report on its achievements since MONEYVAL's first-round evaluation that was completed in 2003. This report will be presented to the plenary once Montenegro's membership is confirmed, which is expected to occur in early 2007. Likewise, the GOM is working toward ratification of the appropriate international conventions.

By the principle of state succession to the State Union of Serbia and Montenegro, Montenegro became a party to the 1988 UN Drug Convention, the UN International Convention on the Suppression of Financing of Terrorism, the UN Convention Against Transnational Organized Crime, and the UN Convention against Corruption on October 23, 2006.

The Government of Montenegro should strengthen its legislation to establish more robust asset seizure and forfeiture regimes, as well as upgrade its capacity to strengthen its criminal intelligence and investigative techniques. Montenegro should continue to ensure that sufficient resources are available for its FIU and law enforcement agencies to work together effectively and efficiently. The GOM should continue to participate in international fora that offer training and technical assistance for police, customs, and judiciary officials involved with combating money laundering and terrorist financing.

## Morocco

Morocco is not a regional financial center, and the extent of the money laundering problem in the country is unknown. Nonetheless, according to a joint 2005 study by the United Nations Office on

Drugs and Crime (UNODC) and Morocco's Agency for Promotion of Economic and Social Development of the Northern Prefectures, Morocco remains an important producer and exporter of cannabis. The narcotics trade and the country's large informal economy are the primary catalysts of money laundering. In the past few years, the Kingdom has taken a series of steps to control the problem. A draft anti-money laundering (AML) bill was presented to the Parliament on November 20, 2006. Reportedly, passage of the AML law is expected to occur in 2007.

Remittances from abroad and cash-based transactions comprise Morocco's informal economic sector. There are unverified reports of trade-based money laundering, including bulk cash smuggling, under- and over-invoicing, and the purchase of smuggled goods; the cash-based cannabis sector is of particular concern. As in previous years, Morocco remains a principal producer of cannabis, with estimated revenues of over $13 billion annually. While some of the narcotics proceeds are laundered in Morocco, most proceeds are believed to be laundered in Europe.

Unregulated money exchanges remain a problem in Morocco and were a prime impetus for the pending Moroccan AML legislation. Although the legislation is intended to curb this practice, the country's current financial structure provides opportunities for unregulated cash transfers. The Moroccan financial sector consists of 16 banks, five government-owned specialized financial institutions, approximately 30 credit agencies, and 12 leasing companies. The monetary authorities in Morocco are the Ministry of Finance and the Central Bank, Bank Al Maghrib (CBM), which monitors and regulates the banking system. A separate Foreign Exchange Office regulates international transactions. There were no prosecutions for money laundering in Morocco in 2006. A key aspect of the pending AML legislation is the increase in responsibility for all entities, both public and private, to report suspect fund transfers, which will provide the legal basis to monitor and prosecute previously unregulated financial activity.

Morocco has a free trade zone in Tangier, with customs exemptions for goods manufactured in the zone for export abroad. There have been no reports of trade-based money laundering schemes or terrorist financing activities using the Tangier free zone or the zone's offshore banks, which are regulated by an interagency commission chaired by the Ministry of Finance.

While there have been no verified reports of international or domestic terrorist networks using the Moroccan narcotics trade to finance terrorist organizations and operations in Morocco, Moroccan security officials arrested over 50 suspects in August and September 2006 for their involvement in the Ansar Al Mahdi terrorist cell. At least two of the suspects were accused of providing financing to the cell.

Morocco has a relatively effective system for disseminating U.S. Government (USG) and United Nations Security Council Resolution (UNSCR) terrorist freeze lists to the financial sector and law enforcement. Morocco has provided detailed and timely reports requested by the UNSCR 1267 Sanctions Committee and some accounts have been administratively frozen (based on the U.S. list of Specially Designated Global Terrorists, designated pursuant to Executive Order 13224). In 1993, a mutual legal assistance treaty between Morocco and the United States entered into force.

Morocco is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Morocco has ratified or acceded to 11 of the 12 UN and international conventions and treaties related to counterterrorism. Morocco is a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004. The creation of the MENAFATF is critical for pushing the region to improve the transparency and regulatory frameworks of its financial sectors.

Morocco is in the process of tightening anti-money laundering controls. Since 2003, Morocco has taken a series of steps to control money laundering. In December 2003, the CBM issued Memorandum

No. 36, in advance of the pending AML legislation, which instructed banks and other financial institutions under its control to conduct internal analysis and investigations into financial transactions. The measures called for the reporting of suspicious transactions and the retention of suspicious activity reports, as well as mandating "know your customer" procedures. In June 2003, Morocco adopted a comprehensive counterterrorism bill. The bill provided the legal basis for lifting bank secrecy to obtain information on suspected terrorists, allowed suspect accounts to be frozen, and permitted the prosecution of terrorist finance-related crimes. The law also provided for the seizure and confiscation of terrorist assets, and called for increased international cooperation with regard to foreign requests for freezing assets of suspected terrorist entities. The law brought Morocco into compliance with UNSCR 1373 requirements for the criminalization of the financing of terrorism. Other money laundering controls include legislation prohibiting anonymous bank accounts and foreign currency controls that require declarations to be filed when transporting currency across the border.

Morocco's anti-money laundering (AML) efforts will take a significant step forward with the implementation of long-awaited AML legislation, expected to occur in the first half of 2007. The legislation draws largely from recommendations made by the Financial Action Task Force (FATF). Once signed into law, the legislation reportedly will require the reporting of suspicious financial transactions by all responsible parties, public and private, who in the exercise of their work, carry out or advise on the movement of funds possibly related to drug trafficking, human trafficking, arms trafficking, corruption, terrorism, tax evasion, or forgery.

Morocco should enact AML legislation that adheres to international standards, including the establishment of a centralized Financial Intelligence Unit (FIU). The AML legislation should provide the legal basis for the government to monitor, investigate, and prosecute all suspect financial activities. Police and customs authorities, in particular, should receive training on recognizing money laundering methodologies, including trade-based laundering and informal value transfer and underground remittance systems.

## The Netherlands

The Netherlands is a major financial center and an attractive venue for the laundering of funds generated from a variety of illicit activities. Activities involving money laundering are often related to the sale of heroin, cocaine, cannabis, or synthetic and designer drugs (such as ecstasy). As a major financial center, several Dutch financial institutions engage in international business transactions involving large amounts of United States currency. There are, however, no indications that significant amounts of U.S. dollar transactions conducted by financial institutions in the Netherlands stem from illicit activity. Activities involving financial fraud are believed to generate a considerable portion of domestic money laundering. A recent report by the University of Utrecht commissioned by the Ministry of Finance has found that much of the money laundered in the Netherlands comes from abroad, but did not find evidence that it is predominantly owned by major drug cartels and other international criminal organizations. There are no indications of syndicate-type structures in organized crime or money laundering, and there is virtually no black market for smuggled goods in the Netherlands. Although under the Schengen Accord there are no formal controls on the borders with Germany and Belgium, the Dutch authorities run special operations in the border areas to keep smuggling to a minimum. Reportedly, money laundering amounts to 18.5 million euros (approximately $24.4 million) annually, or five percent of the Dutch GDP. The Netherlands is not an offshore financial center nor are there any free trade zones in the Netherlands.

In 1994, the Government of the Netherlands (GON) criminalized money laundering related to all crimes. In December 2001, the GON enacted legislation specifically criminalizing the facilitating, encouraging, or engaging in money laundering. This eases the public prosecutor's burden of proof regarding the criminal origins of proceeds: under the law, the public prosecutor needs only to prove

that the proceeds "apparently" originated from a crime. Self-laundering is also covered. In two cases in 2004 and 2005, the Dutch Supreme Court confirmed the wide application of the money laundering offenses by stating that the public prosecutor does not need to prove the exact origin of laundered proceeds and that the general criminal origin as well as the knowledge of the perpetrator may be deducted from objective circumstances.

The Netherlands has an "all offenses" regime for predicate offenses of money laundering. The penalty for "deliberate acts" of money laundering is a maximum of four years' imprisonment and a maximum fine of 45,000 euros (approximately $59,000), while "liable acts" of money laundering (of people who do not know first-hand of the criminal nature of the origin of the money, but should have reason to suspect it) are subject to a maximum imprisonment of one year and a fine no greater than 45,000 euros (approximately $59,000). Habitual money laundering may be punished with a maximum imprisonment of six years and a maximum fine of 45,000 euros (approximately $59,000), and those convicted may also have their professional licenses revoked. In addition to criminal prosecution for money laundering offenses, money laundering suspects can also be charged with participation in a criminal organization (Article 140 of the Penal Code), violations of the financial regulatory acts, violations of the Sanctions Act, or noncompliance with the obligation to declare unusual transactions according to the Economic Offenses Act.

The Netherlands has comprehensive anti-money laundering legislation. The Services Identification Act and the Disclosure Act set forth identification and reporting requirements. All financial institutions in the Netherlands, including banks, bureaux de change, casinos, life insurance companies, securities firms, stock brokers, and credit card companies, are required to report cash transactions over 15,000 euros (approximately $19,700), as well as any less substantial transaction that appears unusual, a broader standard than "suspicious" transactions, to the Office for Disclosure of Unusual Transactions (MOT), the Netherlands' financial intelligence unit (FIU). In December 2001, the reporting requirements were expanded to include trust companies, financing companies, and commercial dealers of high-value goods. In June 2003, notaries, lawyers, real estate agents/intermediaries, accountants, business economic consultants, independent legal advisers, trust companies and other providers of trust related services, and tax advisors were added. Reporting entities that fail to file reports with the MOT may be fined 11,250 euros (approximately $14,775), or be imprisoned up to two years. Under the Services Identification Act, all those that are subject to reporting obligations must identify their clients, including the identity of ultimate beneficial owners, either at the time of the transaction or prior to the transaction, before providing financial services.

In 2004, an evaluation of the anti-money laundering reporting system, commissioned by the Minister of Justice, was published. In response to the report the GON enacted a number of measures to enhance the effectiveness of the existing system. In November 2005, the Board of Procurators General issued a National Directive on money laundering crime that included an obligation to conduct a financial investigation in every serious crime case, guidelines for determining when to prosecute for money laundering and technical explanations of money laundering offenses, case law, and the use of financial intelligence. A new set of indicators, which determine when an unusual transaction must be filed, also entered into force in November 2005. These new indicators represent a partial shift from a rule-based to a risk-based system and are aimed at reducing the administrative costs of reporting unusual transactions for the reporting institutions without limiting the preventive nature of the reporting system. The Dutch parliament has also approved amendments to the Services Identification Act and Disclosure Act that expand supervision authority and introduce punitive damages. The revised legislation, which became effective on May 1, 2006, incorporates a terrorist financing indicator in the reporting system.

Financial institutions are also required by law to maintain records necessary to reconstruct financial transactions for at least five years after termination of the relationship. There are no secrecy laws or fiscal regulations that prohibit Dutch banks from disclosing client and owner information to bank

supervisors, law enforcement officials, or tax authorities. Financial institutions and all other institutions under the reporting and identification acts, and their employees, are specifically protected by law from criminal or civil liability related to cooperation with law enforcement or bank supervisory authorities. Furthermore, current legislation requires Customs authorities to report unusual transactions to the MOT; however, the Netherlands does not currently have a currency declaration requirement for incoming travelers. Under the 2004 Dutch European Union (EU) Presidency, the EU reached agreement on a cash courier regulation, which implements the Financial Action Task Force (FATF) Special Recommendation Nine on terrorist financing. The implementation is expected to occur in the Netherlands mid-2007.

The Money Transfer and Exchange Offices Act, which was passed in June 2001, requires money transfer offices, as well as exchange offices, to obtain a permit to operate, and subjects them to supervision by the Central Bank. Every money transfer client has to be identified and all transactions totaling more than 2,000 euros (approximately $2,630) must be reported to the MOT.

The Central Bank of the Netherlands, which merged with the Pension and Insurance Chamber in April 2004, and the Financial Markets Authority, as the supervisors of the Dutch financial sector, regularly exchanges information nationally and internationally. Sharing of information by Dutch supervisors does not require formal agreements or memoranda of understanding (MOUs).

The financial intelligence unit (FIU) for the Netherlands is a hybrid administrative-law enforcement unit that in 2006 combined the traditional FIU, Meldpunt Onjebruikelijke Transacties (MOT), in English the Office for the Disclosure of Unusual Transactions, with its police counterpart, the Office of Operational Support of the National Public Prosecutor (BLOM). When MOT, established in 1994, and the BLOM merged, the resulting entity was integrated within the National Police (KLPD). The new unit is called the FIU-the Netherlands. This new FIU structure provides an administrative function that receives, analyzes, and disseminates the unusual and currency transaction reports filed by banks and financial institutions. It also provides a police function that serves as a point of contact for law enforcement. It forwards suspicious transaction reports with preliminary investigative information to the Police Investigation Service and to the FIU. This new organization responds to requests from foreign FIUs for financial and law enforcement information. Over the last five years, the MOT and the BLOM cooperated closely in responding to international requests for information, so this merger has not changed the nature of the Dutch reporting system. FIU-the Netherlands is part of the Egmont Group.

The MOT receives over 98 percent of unusual transaction reports electronically through its secure website. In 2004, the MOT received 174,835 unusual transaction reports, totaling over 3.2 billion euros (approximately $4 billion) and forwarded 41,003 to the BLOM and other police services as suspicious transactions for further investigation. In 2005, the MOT received 181,623 reports, totaling over 1.1 billion euros (approximately $1.4 billion), and forwarded 38,481to the BLOM and other police services. The average amount reported was 29,000 euros (approximately $36,500) in 2005, a decrease from the 79,000 euros (approximately $94,500) average reported in 2004. Reportedly, this significant decrease was due to a few large transactions in the previous year.

In order to facilitate the forwarding of suspicious transactions, the MOT and BLOM created an electronic network called Intranet Suspicious Transactions (IST). Fully automatic matches of data from the police databases are included with the unusual transaction reports forwarded to the BLOM. On January 1, 2003, the MOT and BLOM formed a special unit (the MBA-unit) to work together to analyze data generated from the IST. Once the data is analyzed by the MBA-unit, it forwards reports to the police. Since the money laundering detection system also covers areas outside the financial sector, the system is used for detecting and tracing terrorist financing activity. MOT/BLOM provides the anti-money laundering division of Europol with suspicious transaction reports, and Europol applies the same analysis tools as BLOM.

The Netherlands has enacted legislation governing asset forfeiture. The 1992 Asset Seizure and Confiscation Act enables authorities to confiscate assets that are illicitly obtained or otherwise connected to criminal acts. The GON amended the legislation in 2003 to improve and strengthen the options for identifying, freezing, and seizing criminal assets. The police and several special investigation services are responsible for enforcement in this area. These entities have adequate powers and resources to trace and seize assets. All law enforcement investigations into serious crime may integrate asset seizure.

Authorities may seize any tangible assets, such as real estate or other conveyances that were purchased directly with the proceeds of a crime tracked to illegal activities. Property subject to confiscation as an instrumentality may consist of both moveable property and claims. Assets can be seized as a value-based confiscation. Asset seizure and confiscation legislation also provides for the seizure of additional assets controlled by a drug trafficker. Legislation defines property for the purpose of confiscation as "any object and any property right." Proceeds from narcotics asset seizures and forfeitures are deposited in the general fund of the Ministry of Finance. Dutch authorities have not identified any significant legal loopholes that allow drug traffickers to shield assets.

In order to promote the confiscation of criminal assets, the GON has instituted special court procedures. These procedures enable law enforcement to continue financial investigations in order to prepare confiscation orders after the underlying crimes have been successfully adjudicated. All police and investigative services in the field of organized crime rely on the real time assistance of financial detectives and accountants, as well as on the assistance of the Proceeds of Crime Office (BOOM), a special bureau advising the Office of the Public Prosecutor in international and complex seizure and confiscation cases. To further international cooperation in this area, the Camden Asset Recovery Network (CARIN) was set up in The Hague in September 2004. BOOM played a leading role in the establishment of this informal international network of asset recovery specialists, whose aim is the exchange of information and expertise in the area of asset recovery.

Statistics provided by the Office of the Public Prosecutor show that the amount of assets seized in 2005 amounted to 11 million euros (approximately $14.5 million). The United States and the Netherlands have had an asset-sharing agreement in place since 1994. The Netherlands also has an asset-sharing treaty with the United Kingdom, and an agreement with Luxembourg.

In June 2004, the Minister of Justice sent an evaluation study to the Parliament on specific problems encountered with asset forfeiture in large, complex cases. In response to this report, the GON announced several measures to improve the effectiveness of asset seizure enforcement, including steps to increase expertise in the financial and economic field, assign extra public prosecutors to improve the coordination and handling of large, complex cases, and establish a specific asset forfeiture fund. The Office of the Public Prosecutor has designed a new centralized approach for large confiscation cases and a more flexible approach for handling smaller cases. Both took effect in 2006 and significantly increase BOOM's capacity to handle asset forfeiture cases.

Terrorist financing is a crime in the Netherlands. In August 2004, the Act on Terrorist Crimes, implementing the 2002 EU framework decision on combating terrorism, became effective. The Act makes recruitment for the Jihad and conspiracy with the aim of committing a serious terrorist crime separate criminal offenses. In 2004, the government created a National Counterterrorism Coordinator's Office to streamline and enhance Dutch counterterrorism efforts.

UN resolutions and EU regulations form a direct part of the national legislation on sanctions in the Netherlands. The "Sanction Provision for the Duty to Report on Terrorism" was passed in 1977 and amended in June 2002 to implement European Union (EU) Regulation 2580/2001. United Nations Security Council Resolution (UNSCR) 1373 is implemented through Council Regulation 2580/01; listing is through the "Clearing-House" procedure. The ministerial decree provides authority to the Netherlands to identify, freeze, and seize terrorist finance assets. The decree also requires financial

institutions to report to the MOT all transactions (actually carried out or intended) that involve persons, groups, and entities that have been linked, either domestically or internationally, with terrorism. Any terrorist crime will automatically qualify as a predicate offense under the Netherlands "all offenses" regime for predicate offenses of money laundering. Involvement in financial transactions with suspected terrorists and terrorist organizations listed on the United Nations (UN) 1267 Sanctions Committee's consolidated list or designated by the EU has been made a criminal offense. The Dutch have taken steps to freeze the assets of individuals and groups included on the UNSCR 1267 Sanctions Committee's consolidated list. UNSCR 1267/1390 is implemented through Council Regulation 881/02. Sanctions Law 1977 also addresses this requirement parallel to the regulation in the Netherlands.

The Netherlands does not require a collective EU decision to identify and freeze assets suspected of being linked to terrorism nationally. In these cases, the Minister of Foreign Affairs and the Minister of Finance make the decision to execute the asset freeze. Decisions take place within three days after identification of a target. Authorities have used this instrument several times in recent years. In three cases, national action followed the actions taking place on the EU level. In one case, the entity was included on the UN 1267 list and was automatically included in the list that is part of EU regulation 2002/881. In two other cases, the Netherlands successfully nominated the entity/individual for inclusion on the autonomous EU list that is compiled pursuant to Common Position 2001/931.

The Act on Terrorist Offenses took effect on August 10, 2004. The Act introduces Article 140A of the Criminal Code, which criminalizes participation in an organization when the intent is to commit acts of terrorism, and defines participation as membership or providing provision of monetary or other material support. Article 140A carries a maximum penalty of fifteen years' imprisonment for participation in and life imprisonment for leadership of a terrorist organization. The GON is considering new legislation that would expand, among other things, investigative powers and the use of coercive measures in antiterrorist inquiries. In June 2004, the Dutch for the first time successfully convicted two individuals of terrorist activity allowing use of intelligence of the General Intelligence and Security Service (AIVD) as evidence. Nine individuals were convicted in March 2006 on charges of membership in a terrorist organization.

Unusual transaction reports by the financial sector act as the first step against the abuse of religious organizations, foundations and charitable institutions for terrorist financing. No individual or legal entity using the financial system (including churches and other religious institutions) is exempt from the identification requirement. Financial institutions must also inquire about the identity of the ultimate beneficial owners. The second step, provided by Dutch civil law, requires registration of all active foundations in the registers of the Chambers of Commerce. Each foundation's formal statutes (creation of the foundation must be certified by a notary of law) must be submitted to the Chambers. Charitable institutions also register with, and report to, the tax authorities in order to qualify for favorable tax treatment. Approximately 15,000 organizations (and their managements) are registered in this way. The organizations must file their statutes, showing their purpose and mode of operations, and submit annual reports. Samples are taken for auditing. Finally, many Dutch charities are registered with or monitored by private "watchdog" organizations or self-regulatory bodies, the most important of which is the Central Bureau for Fund Raising. In April 2005, the GON approved a plan to replace the current initial screening of founders of private and public-limited partnerships and foundations with an ongoing screening system. The new system will be introduced in 2007 to improve Dutch efforts to fight fraud, money laundering, and terrorist financing.

Data about alternative remittance systems such as hawala or informal banking as a potential money laundering/terrorist financing source is still scarce. Initial research by the Dutch police and Internal Revenue Service and Economic Control Service (FIOD/ECD) indicates that the number of informal banks and hawaladars in the Netherlands is rising. The Dutch Government plans to implement improved procedures for tracing and prosecuting unlicensed informal or hawala-type activity, with the

Dutch Central Bank, FIOD/ECD, the Financial Expertise Center, and the Police playing a coordinating and central role. The Dutch Finance Ministry has participated in a World Bank-initiated international survey on money flows by immigrants to their native countries, with a focus on relations between the Netherlands and Suriname. The Dutch Central Bank will also initiate a study into the number of informal banking institutions in the Netherlands. In Amsterdam, a special police unit has been investigating underground bankers. These investigations have resulted in the disruption of three major underground banking schemes.

The Netherlands is in compliance with all FATF Recommendations, with respect to both legislation and enforcement. The Netherlands also complies with the Second and Third EU Money Laundering Directives. The Dutch have implemented some obligations resulting from these directives, such as effective supervision of money transfer offices, trust and service provider companies, and the incorporation of reporting on terrorist financing.

The United States enjoys good cooperation with the Netherlands in fighting international crime, including money laundering. In September 2004, the United States and the Netherlands signed two agreements in the area of mutual legal assistance and extradition, stemming from the agreements that were concluded in 2003 between the EU and the United States. One of the amendments to the existing bilateral agreement is the exchange of information on bank accounts.

The MOT supervised the PHARE Project for the European Union (March 2002-December 2003). The PHARE Project was the European Commission's Anti-Money Laundering Project for Economic Reconstruction Assistance to Estonia, Latvia, Lithuania, Poland, the Czech Republic, Slovakia, Hungary, Slovenia, Romania, Bulgaria, Cyprus, and Malta. The purpose of the project was to provide support to Central and Eastern European countries in the development and/or improvement of anti-money laundering regulations. Although the PHARE project concluded in December 2003, the MOT has moved forward with the development of the FIU.NET Project, (an electronic exchange of current information between European FIUs by means of a secure intranet). In March 2006, the Dutch hosted a major international terrorist financing conference.

The Netherlands is a member of the Financial Action Task Force and the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The Netherlands participates in the Caribbean Financial Action Task Force as a Cooperating and Supporting Nation. As a member of the Egmont Group, MOT has established close links with the U.S Treasury's FinCEN as well as with other Egmont members, and is involved in efforts to expand international cooperation. The Netherlands is a party to the 1988 UN Drug Convention, and the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime.

The Netherlands should continue with its plans for a screening system for private and public-limited partnerships, and implement requirements for all charities to register with a state or state-sanctioned body that is set up to perform screening. The GON should also devote more resources toward getting better data and a better understanding of alternate remittance systems in the Netherlands, and channel more investigative resources toward underground banks. The Netherlands should also continue to its plans to implement improved procedures for tracing informal bank systems, including prosecution procedures where appropriate, and improve coordination vis-à-vis the responsibilities of the various involved agencies.

## Netherlands Antilles

The Netherlands Antilles is comprised of the islands of Curacao, Bonaire, Dutch Sint Maarten, Saba, and Sint Eustatius. Though a part of the Kingdom of the Netherlands, the Netherlands Antilles has autonomous control over its internal affairs. The Government of the Netherlands Antilles (GONA) is

located in Willemstad, the capital of Curacao, which is also the financial center for the five islands. A significant offshore sector and loosely regulated free trade zones, as well as narcotics trafficking and a lack of border control between Sint Maarten (the Dutch side of the island) and St. Martin (the French side), create opportunities for money launderers in the Netherlands Antilles.

The islands have seven local commercial banks, four foreign commercial banks, 12 credit unions, six specialized credit institutions, one savings bank, four savings and credit funds, 15 consolidated international banks and 19 nonconsolidated international banks. There are 54 institutional investors operating in the Netherlands Antilles, including ten life insurance companies, 20 non-life insurance companies and 24 pension funds. There are also two life captive-insurance businesses, 15 non-life captive-insurance business and four professional re-insurers.

The Netherlands Antilles has a significant offshore financial sector with 229 trust service companies providing financial and administrative services to an international clientele, which includes offshore companies, mutual funds and international finance companies. As of September 2006, there were a total of 15,009 offshore companies registered with the Chamber of Commerce in the Netherlands Antilles, as is required by law. International corporations may be registered using bearer shares. The practice of the financial sector in the Netherlands Antilles is for either the bank or the company service providers to maintain copies of bearer share certificates for international corporations, which include information on the beneficial owner(s). The Netherlands Antilles also permits internet gaming companies to be licensed on the islands. There are currently 32 licensed internet gaming companies.

On February 1, 2001, the GONA approved proposed amendments to the free zone law to allow e-commerce activities into these areas (National Ordinance Economic Zone no.18, 2001). It is no longer necessary for goods to be physically present within the zone as was required under the former free zone law. Furthermore, the name “Free Zone” was changed to “Economic Zone” (e-zone). Seven areas within the Netherlands Antilles qualify as e-zones, five of which are designated for e-commerce. The remaining two e-zones, located at the Curacao airport and harbor, are designated for goods. These zones are minimally regulated; however, administrators and businesses in the zones have indicated an interest in receiving guidance on detecting unusual transactions.

Money laundering is a criminal offence in the Netherlands Antilles. Legislation in 1993 and subsequent interpretations regarding the underlying crime establish that prosecutors do not need to prove that a suspected money launderer also committed an underlying crime in order to obtain a money laundering conviction. Thus, it is sufficient to establish that the money launderer knew, or should have known, of the money’s illegal origin. Suspicious transactions are required by law to be reported to the financial intelligence unit (FIU), the Meldpunt Ongebruikelijke Transacties (MOT NA).

In recent years, the GONA has taken steps to strengthen its anti-money laundering regime by expanding suspicious activity reporting requirements to nonfinancial sectors; introducing indicators for the reporting of unusual transactions for the gaming industry; issuing guidelines to the banking sector on detecting and deterring money laundering; and modifying existing money laundering legislation that penalizes currency and securities transactions by including the use of valuable goods. The 2002 National Ordinance on Supervision of Fiduciary Business institutes the Supervisory Board to oversee the international financial sector. At the same time, the GONA imposed know-your-customer rules upon the sector. A GONA interagency anti-money laundering working group cooperates with its Kingdom counterparts.

Both bank and nonbank financial institutions, such as company service providers and insurance companies, are under the obligation to report unusual transactions to the MOT NA. Each financial sector has its own reporting threshold amount. The GONA is currently amending its legislation to add new reporting entities, including lawyers, accountants, notaries, jewelers and real estate agents. It is expected that the legislation will be passed in 2007.

Through October 2006, 10,788 suspicious transaction reports totaling $1.3 billion were received by the MOT NA. Of these, 283 were reported to the relevant law enforcement authorities. The MOT NA currently has a staff of nine, and is engaged in increasing the effectiveness and efficiency of its reporting system. Significant progress has been reported in automating unusual activity reporting. Additionally, the MOT NA has issued a manual for casinos on how to file reports and has started to install software in casinos that will allow reports to be submitted electronically.

The Central Bank of the Netherlands Antilles supervises all banking and credit institutions, including banks for local and international business, specialized credit institutions, savings banks, credit unions, credit funds and pension funds. The laws and regulations on bank supervision provide that international banks must have a physical presence and maintain records on the island. The Central Bank also supervises insurance companies, insurance brokers, mutual funds and administrators of these funds, all of which must be licensed by the Central Bank. As of 2003, supervision of the company service providers in the Netherlands Antilles was transferred to the Central bank.

The Central Bank updated its anti-money laundering guidelines in 2003. These guidelines are more closely focused on banks, insurance companies, pension funds, money transfer services, financial administrators, and company service providers and specifically include terrorism financing indicators. Entities under supervision must submit an annual statement of compliance. The Central Bank has provided training to different sectors on the guidelines. The Central Bank also established the Financial Integrity Unit to monitor corporate governance and market behavior.

As of May 2002, all persons entering or leaving one of the island territories of the Netherlands Antilles shall report money of NAF 20,000 (approximately US$11,300) or more in cash or bearer instruments to Customs officials. This provision also applies to those entering or leaving who are demonstrably traveling together and who jointly carry with them money for a value of NAF 20,000 or more. Declaration of currency exceeding the threshold must include origin and destination. Violators may be fined up to NAF 250,000 (approximately $142,000) and/or face one year in prison.

In 2000, the National Ordinance on Freezing, Seizing and Forfeiture of Assets Derived from Crime was enacted. The law allows the prosecutor to seize the proceeds of any crime proven in court.

Terrorist financing is not a crime in the Netherlands Antilles. However, in January 2002, the GONA enacted legislation allowing a judge or prosecutor to freeze assets related to the Taliban and Usama Bin Laden, as well as all persons and companies connected with them. The legislation contains a list of individuals and organizations suspected of terrorism. The Central Bank instructed financial institutions to query their databases for information on the suspects and to immediately freeze any assets found. In October 2002, the Central Bank instructed the financial institutions under its supervision to continue these efforts and to consult the UN website for updates to the list.

Netherlands Antilles' law allows the exchange of information between the MOT NA and foreign FIUs by means of memoranda of understanding and by treaty. The MOT NA's policy is to answer requests within 48 hours of receipt. A tax information exchange agreement (TIEA) was signed between the Netherlands Antilles and the United States. As of the end of 2006, implementing legislation was pending the GONA parliament to allow this agreement to go into effect. The Mutual Legal Assistance Treaty between the Netherlands and the United States applies to the Netherlands Antilles. The U.S.-Netherlands Agreement Regarding Mutual Cooperation in the Tracing, Freezing, Seizure and Forfeiture of Proceeds and Instrumentalities of Crime and the Sharing of Forfeited Assets also applies to the Netherlands Antilles.

The MOT NA is a member of the Egmont Group. The Netherlands Antilles is also a member of the Caribbean Financial Action Task Force (CFATF), and as part of the Kingdom of the Netherlands, participates in the Financial Action Task Force (FATF). In 1999, the Netherlands extended application of the 1988 UN Drug Convention to the Netherlands Antilles. The Kingdom of the Netherlands

became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2002. In accordance with Netherlands Antilles' law, which stipulates that all the legislation must be in place prior to ratification, the GONA is preparing legislation to ratify the Convention.

The Government of the Netherlands Antilles has demonstrated a commitment to combating money laundering. The Netherlands Antilles should continue its focus on increasing regulation and supervision of the offshore sector and free trade zones, as well as pursuing money laundering investigations and prosecutions. The GONA should criminalize the financing of terrorism and enact the necessary legislation to implement the UN International Convention for the Suppression of the Financing of Terrorism.

## Nicaragua

Nicaragua is not a regional financial center. Nicaragua is not a major drug producing country, but continues to serve as a significant transshipment point for South American cocaine and heroin destined for the United States and—on a smaller scale—for Europe. There is evidence that the narcotics trade is increasingly linked to arms trafficking. This situation, combined with weak adherence to rule of law, judicial corruption, the politicization of the public prosecutor's office and insufficient funding for law enforcement institutions, makes Nicaragua's financial system an attractive target for narcotics-related money laundering. Nicaraguan officials have expressed concern that, as neighboring countries have tightened their anti-money laundering laws, established financial intelligence units (FIUs) and taken other enforcement actions, more illicit money has moved into the vulnerable Nicaraguan financial system. However, this concern has not translated into an appreciable strengthening of Nicaragua's legal and institutional frameworks to effectively combat money laundering and the financing of terrorism.

Nicaragua's geographical position, with access to both the Atlantic and the Pacific Oceans and porous border crossings to its north and south, makes it an area heavily used by transnational organized crime groups. These groups also benefit from Nicaragua's weak legal system and its ineffective fight against financial crimes, money laundering, trafficking of immigrants and the financing of terrorism.

While Nicaragua has pledged to fight the financing of terrorism, money laundering and other financial crimes, limited resources, corruption (especially in the judiciary), and the lack of political will in some sectors continue to complicate efforts to counteract these criminal activities. Nicaragua has recently made improvements to its oversight and regulatory control of its financial system. The current Prosecutor General and some Supreme Court justices advocate a narrow interpretation of money laundering law, claiming that, as written, Nicaraguan law only penalizes the laundering of proceeds of narcotics trafficking and not of other illegal activities. This position is believed to be politically motivated, as it would provide legal justification to overturn the conviction of former president Arnoldo Aleman for laundering the proceeds of corruption-related offenses. Regardless of this legally erroneous position, the Prosecutor General still refuses to prosecute narcotics offenders for money laundering despite ample evidence to support these types of cases. In the last 18 months, the National Prosecutor's Office has not prosecuted a single money laundering case, including those involving drug traffickers with large stashes of U.S. currency who have been arrested on Nicaraguan soil. This enforcement problem is exacerbated by the fact that the country does not have an operational FIU. All attempts to correct this deficiency have been stalled in the National Assembly, awaiting final resolution of Arnoldo Aleman's money laundering conviction.

A number of foreign institutions own significant shares of the Nicaraguan financial sector. In 2005, GE Consumer Finance, one of the largest financial service firms in the world, bought a 49.99 percent stake in Banco de America Central (BAC), which operates in several Central American countries, including Nicaragua. In October 2006, Citibank purchased a significant share of Grupo Financiero Uno's Central American operations, which include credit cards, commercial banking, insurance and

brokerage firms. The deal awaits regulatory approval. Banistmo, a Panamanian bank, operates in Nicaragua. Bancentro/Lafise, a financial institution covering all commercial banking and insurance services, maintains operations in El Salvador, Guatemala and Honduras. The entry into force on April 1, 2006, of the Central America/Dominican Republic Free Trade Agreement (CAFTA-DR) and increased pace of regional integration suggest growing involvement of Nicaraguan financial institutions with international partners and clients. Most large Nicaraguan banks already maintain correspondent relationships with Panamanian institutions.

Nicaragua does not permit direct offshore bank operations, but it does permit such operations through nationally chartered entities. Bank and company bearer shares are permitted. Nicaragua has a well-developed indigenous gaming industry, which remains largely unregulated. Two competing casino regulations bills are currently in the National Assembly; the main difference between the bills is whether regulatory authority will fall under the tax authority or if an independent institution will be established to supervise the industry. There are no known offshore or internet gaming sites in Nicaragua.

In 2005, the National Assembly reformed the law governing Nicaragua's general banks, nonbank financial institutions and financial groups, bringing it in line with Basel II international banking regulations. When enforced properly, the law will hold bank officials responsible for all of their institution's actions, including failure to report money laundering. Article 164 of the law calls for sanctions for financial institutions and professionals of the financial sector, including internal auditors who do not develop anti-money laundering programs or do not report to the appropriate authorities suspicious and unusual transactions that may be linked to money laundering, as required by the anti-money laundering law.

In 1999, Nicaragua passed Law 285, which requires all financial institutions under the supervision of the Superintendence of Banks and Other Financial Institutions (SIBOIF) to report cash deposits over $10,000 and suspicious transactions to the SIBOIF. The SIBIOF then forwards the reports to the Commission of Financial Analysis (CAF). All persons entering or leaving Nicaragua are also required to declare the transportation of currency in excess of $10,000 or its equivalent in foreign currency. Law 285 is not, however, being used as an effective tool against money laundering crimes committed by organized crime groups. The National Prosecutor's and the Attorney General's legal positions on Law 285 differ significantly. The National Prosecutor, who also heads the CAF, has sought to limit the application of the money laundering law to drug crimes. The Attorney General has led President Bolanos's charge against public corruption, and has argued in and out of court that the money laundering law as written applies to public corruption and other nondrug crimes.

On paper, the CAF is composed of representatives from various elements of law enforcement and banking regulators and is responsible for detecting money laundering trends, coordinating with other agencies and reporting its findings to Nicaragua's National Anti-Drug Council. The CAF does not analyze the information received, and is not considered to be a professional or independent unit. It is ineffective due to an insufficient budget, the politicization of its leadership, and a lack of trained personnel, equipment and strategic goals. The CAF is headed by the National Prosecutor, who receives the reports from banks and decides whether to refer them to the Nicaraguan National Police (NNP) for further investigation. The Economics Crimes Unit within the NNP is in charge of investigating financial crimes, including money laundering and terrorist financing. The Nicaraguan Deputy Attorney General is critical of the inactivity and ineffectiveness of the CAF. He has claimed that of the suspicious activity reports received by the CAF from financial institutions, not a single criminal money laundering investigation—including those related to drug trafficking—has been initiated by the National Prosecutor.

Legislation that would improve Nicaragua's anti-money laundering regime has been stalled in the National Assembly for years. There are at least two pending bills: an amended drug and anti-money

laundering law which would better define the crime of money laundering, and a special bill to create a central FIU that would replace and enhance the functions of the CAF and establish more stringent reporting requirements.

Draft legislation to criminalize terrorist financing is under consideration by the National Assembly, without any sign of imminent passage. In spite of the lack of terrorist financing legislation, many elements of terrorist financing can theoretically be prosecuted under existing laws. Through five SIBIOF administrative decrees, Nicaragua also has the authority to identify, freeze and seize terrorist-related assets, but has not as yet identified any such active cases. However, Nicaragua has not yet established the financing of terrorism as a criminal offense, placing it in a position of noncompliance with international standards.

Reportedly, there are no hawala or other similar alternative remittance systems operating in Nicaragua, and Nicaragua has not detected any use of gold, precious metals or charitable organizations to disguise transactions related to terrorist financing. However, there are informal "cash and carry" networks for delivering remittances from abroad. Over 300 micro-finance institutions exist in Nicaragua, serving over 300,000 clients, dominating the informal economy and managing a significant portion of the remittances. This sector has grown steadily at about 25 percent per year since 1999. While currently unregulated, a bill to bring this sector under the authority of the SIBOIF will be presented to the National Assembly in 2007.

Corruption within the judiciary is a serious problem: judges often let detained drug suspects go free after a short detention, a practice that puts drug traffickers back on the streets and thus increases the threat of money laundering. In a recent high profile case, judges released over $600,000 of funds from a suspected drug trafficker. From all indications, a number of judges may have been involved in the case and may have received payoffs. In another judicial scandal, two Mexican citizens believed to be involved in drug trafficking were acquitted, and over $300,000 in undeclared currency that Nicaraguan customs seized when they entered the country was returned to them. This case also involved a judge connected to the first drug-money scandal. Several judges have been exposed in the press for allegedly taking bribes to acquit drug traffickers at trials or to set aside their convictions on appeal. Other judges have been known to release drug defendants on bail for unsubstantiated medical reasons. Due to the rampant corruption in the Nicaraguan judiciary, the United States has cut off direct assistance to the Nicaraguan Supreme Court. U.S. anticorruption efforts have focused on creating a vetted Anti-Corruption Unit that would be housed within the NNP and include officials from the Attorney General's Office, with the aim of enhancing investigations and prosecutions of corruption, money laundering and related crimes.

In spite of corruption within the judicial branch, the SIBOIF is considered to be an independent and reputable financial institution regulator. The position of the Superintendent does not enjoy legal immunity, exposing the Superintendent to lawsuits from regulated institutions. Given the corrupt nature of the judicial system, this exposure can limit the willingness of SIBIOF to make "unpopular" decisions; however, the institution's financial experts have reached out to the NNP to work with them. For example, in December 2005, the SIBOIF closed down a business named Agave Azul that was allegedly operating an illegal Ponzi scheme. Agave Azul opened for business in May 2005, and by December 2005, approximately $8 million in U.S. currency had been deposited in its accounts in at least two U.S. banks. The SIBOIF notified the National Prosecutor about the scheme in early August 2005; however, the National Prosecutor has hampered the investigation through failure to act. Efforts to freeze the business' bank accounts in the United States were unsuccessful due to the failure of the NNP to provide complete financial information, and the unwillingness of the National Prosecutor to seek U.S. Government cooperation. Despite these failures, the case demonstrates the willingness of the SIBIOF and NNP to investigate financial crimes, and a substantial level of cooperation between the Attorney General's Office and the NNP on financial crimes and money laundering issues.

Nicaragua is a party to the 1988 United Nations Drug Convention, the UN International Convention on the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. On February 15, 2006, Nicaragua ratified the UN Convention against Corruption. Nicaragua has also ratified the Inter-American Convention on Mutual Legal Assistance in Criminal Matters and the Inter-American Convention against Terrorism. Nicaragua is a member of the Money Laundering Experts Working Group of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) and the Caribbean Financial Action Task Force (CFATF). CFATF, which monitors its members' compliance with the international anti-money laundering and counterterrorist financing standards established by the Financial Action Task Force (FATF), has criticized Nicaragua for its failure to prosecute money laundering beyond drug-related offenses, criminalize terrorist financing or create an effective FIU. Due to Nicaragua's failure to establish a functional FIU, it is the only country in Central America and one of the only countries in the Western Hemisphere that is not a member of the Egmont Group.

The Government of Nicaragua needs to enhance its limited efforts to combat financial crime by expanding the predicate crimes for money laundering beyond narcotics trafficking, criminalizing terrorist financing, allocating the necessary resources to develop an effective financial intelligence unit, and combating corruption. Nicaragua should develop a more effective method of obtaining information and cooperation from foreign law enforcement agencies and banks, take steps to immobilize its bearer shares and adequately regulate its gambling industry. These actions, coupled with increased enforcement, would significantly strengthen the country's financial system against money laundering and terrorist financing, and would bring Nicaragua closer to compliance with relevant international anti-money laundering and counterterrorist financing standards and controls.

## Nigeria

The Federal Republic of Nigeria is the most populous country in Africa and is West Africa's largest democracy. Although Nigeria is not an offshore financial center; its large economy is a hub for the trafficking of persons and narcotics. Nigeria is a major drug-transit country and is a center of criminal financial activity for the entire continent. Individuals and criminal organizations have taken advantage of the country's location, weak laws, systemic corruption, lack of enforcement, and poor economic conditions to strengthen their ability to perpetrate all manner of financial crimes at home and abroad. Nigerian criminal organizations are adept at devising new ways of subverting international and domestic law enforcement efforts and evading detection. Their success in avoiding detection and prosecution has led to an increase in many types of financial crimes, including bank fraud, real estate fraud, identity theft, and advance fee fraud. Despite years of government effort to counter rampant crime and corruption, Nigeria continues to be plagued by crime. The establishment of the Economic and Financial Crimes Commission (EFCC) along with the Independent Corrupt Practices Commission (ICPC) and the improvements in training qualified prosecutors for Nigerian courts yielded some successes in 2005 and 2006.

In addition to narcotics-related money laundering, advance fee fraud is a lucrative financial crime that generates hundreds of millions of illicit dollars annually for criminals. Nigerian criminals initially made the advance fee fraud scheme infamous. Today, nationals of many African countries and from a variety of countries around the world also perpetrate advance fee fraud. This type of fraud is referred to internationally as "Four-One-Nine" (419), a reference to the fraud section in Nigeria's criminal code. While there are many variations, the main goal of 419 frauds is to deceive victims into the payment of a fee by persuading them that they will receive a very large benefit in return, or by persuading them to pay fees to "rescue" or help a newly-made "friend" in some sort of alleged distress. . A majority of these schemes end after the victims have suffered monetary losses, but some have also involved kidnapping, and/or murder. Through the internet, businesses and individuals around the world have been, and continue to be, targeted by perpetrators of 419 scams. The EFCC has

tried to combat 419-related cyber crimes, but there have only been a few recorded successes as a result of their cyber crime initiatives.

In June 2001, the Financial Action Task Force (FATF) placed Nigeria on its list of noncooperative countries and territories (NCCT) in combating money laundering and in April 2002, the United States issued an advisory to inform banks and other financial institutions operating in the United States of serious deficiencies in the anti-money laundering regime of Nigeria and to warn U.S. banks to give "enhanced scrutiny" to all financial transactions emanating from Nigeria or going to, or through it. In December 2002, Nigeria enacted three pieces of legislation: an amendment to the 1995 Money Laundering Act that extends the scope of the law to cover the proceeds of all crimes; an amendment to the 1991 Banking and Other Financial Institutions (BOFI) Act that expands coverage of the law to stock brokerage firms and foreign currency exchange facilities, gives the Central Bank of Nigeria (CBN) greater power to deny bank licenses, and allows the CBN to freeze suspicious accounts; and the Economic and Financial Crimes Commission (Establishment) Act that establishes the Economic and Financial Crimes Commission (EFCC), that coordinates anti-money laundering investigations and information sharing. The Economic and Financial Crimes Commission Act also criminalizes the financing of terrorism and participation in terrorism. Violation of the Act carries a penalty of up to life imprisonment.

In May 2006, the FATF visited Nigeria to conduct an evaluation of the revisions made to the government's anti-money laundering regime. FATF recognized the progress Nigeria made in implementing AML policies, the establishment of a financial intelligence unit (FIU) and the progress on money laundering investigations, prosecution and convictions. As a result, Nigeria was removed from the NCCT but the FATF enhanced monitoring its efforts for compliance with international standards.

In April 2003, the EFCC was formally constituted, with the primary mandate to investigate and prosecute financial crimes. It has recovered or seized assets from various people guilty of fraud inside and outside of Nigeria, including a syndicate that included highly placed government officials who were defrauding the Federal Inland Revenue Service (FIRS). Several influential individuals have been arrested and are currently awaiting trial. In an effort to expedite the trial process, the Commission has been assigned two high court judges in Lagos and two in Abuja to hear all cases involving financial crimes.

In 2004, the National Assembly passed the Money Laundering (Prohibition) Act (2004), which applies to the proceeds of all financial crimes. It also covers stock brokerage firms and foreign currency exchange facilities, in addition to banks and financial institutions. The legislation gives the CBN greater power to deny bank licenses and freeze suspicious accounts. This legislation also strengthens financial institutions by requiring more stringent identification of accounts, removing a threshold for suspicious transactions, and lengthening the period for retention of records. In November 2004, the EFCC reported that the great majority of Nigeria's banks were not in compliance with the new law, typically by not adhering to the due diligence provisions of the law and by neglecting to file suspicious transactions reports (STRs). The EFCC promised a new initiative to educate bank personnel and the general public about the provisions of the law before imposing sanctions for noncompliance. Nigeria has not yet detected a case of terrorist financing laundered through the banking system. The UNSCR 1267 Sanctions Committee's consolidated list is periodically distributed to Nigerian financial institutions.

Under the 2004 Money Laundering (Prohibition) Act and 1995 Foreign Exchange (Monitoring and Miscellaneous Provisions) Act, money laundering controls apply to nonbanking financial institutions. These institutions include: dealers in jewelry, cars and luxury goods, chartered accountants, audit firms, tax consultants, clearing and settlement companies, legal practitioners, hotels, casinos,

supermarkets and other such businesses as the Federal Ministry of Commerce may designate. To date, the oversight of compliance by the Ministry of Commerce has not been very rigorous or effective.

In 2004, the Economic and Financial Crimes Commission (Establishment) Act of 2002 was amended. The 2004 EFCC act enlarged the number of EFCC board members, enabled the EFCC police members to bear arms, and banned interim court appeals that hinder the trial court process. The commission's primary mandate is to investigate and prosecute financial crimes, and in particular to coordinate anti-money laundering investigations and information sharing in Nigeria and internationally.

In 2005, the EFCC established the Nigerian Financial Intelligence Unit (NFIU). The NFIU draws its powers from the Money Laundering (Prohibition) Act of 2004 and the Economic and Financial Crimes Commission Act of 2004. It is the central agency for the collection, analysis and dissemination of information on money laundering and terrorism financing. All financial institutions and designated nonfinancial institutions are required by law to furnish the NFIU with details of their financial transactions. Provisions have been included to give the NFIU power to receive suspicious transaction reports made by financial institutions and nondesignated financial institutions, as well as to receive reports involving the transfer to or from a foreign country of funds or securities exceeding $10,000 in value.

The NFIU is a significant component of the EFCC. It complements the EFCC's directorate of investigations but does not carry out its own investigations. The NFIU fulfills a crucial role in receiving and analyzing STRs. As a result, banks have improved both their timeliness and quality in filing STRs reported to the NFIU. Under the EFCC Act, safe-harbor provisions are provided. Nigeria has no secrecy laws that prevent the disclosure of client and ownership information by domestic financial services companies to bank regulatory and law enforcement authorities. The NFIU has access to records and databanks of all government and financial institutions, and it has entered into memorandums of understandings (MOUs) on information sharing with several other financial intelligence centers. The establishment of the NFIU was part of Nigeria's efforts towards the removal of Nigeria from the NCCT list.

Nigeria criminalized the financing of terrorism under the Economic and Financial Crimes Commission (Establishment) Act of 2004. The EFCC has authority under the act to identify, freeze, seize, and forfeit terrorist finance-related assets. Due to the recent creation of the EFCC, the enactment of new laws, and a successful public enlightenment campaign, crimes such as bank fraud and counterfeiting are being reported and prosecuted for the first time. In addition to the EFCC, the National Drug Law Enforcement Agency (NDLEA), the Independent Corrupt Practices Commission (ICPC), and the Criminal Investigation Department of the Nigeria Police Force (NPF/CID) are empowered to investigate financial crimes. The Nigerian Police Force is incapable of handling financial crimes because of corruption and poor institutional capacity. Currently, the EFCC is the agency most capable of effectively investigating and prosecuting financial crimes, including money laundering and terrorist financing. The EFCC coordinates all other agencies in financial crimes investigations.

In 2005, the EFCC marked significant successes in combating financial crime. Two fraudsters in a Brazilian bank scam involving a total of $242 million in assets were successfully prosecuted and convicted for terms of 25 and 12 years in prison, respectively. Their assets were seized, and they were ordered to give $110 million in restitution to the bank. The EFCC also returned $4.481 million to an elderly woman swindled by a Nigerian 419 kingpin in 1995. The kingpin was arrested, prosecuted, convicted, and is serving his prison sentence. A former inspector general of police was arrested and prosecuted for financial crimes valued at over $13 million. His assets were seized and bank accounts frozen. He is currently serving a prison sentence and still faces 92 charges of money laundering and official corruption. Currently, two sitting state governors are the subject of money laundering investigations. The EFCC, working with the FBI, also has an active case involving a group of money brokers using banks in the United States to launder money. The money laundering legislation of 2004

has given the EFCC the authority to investigate and prosecute such cases. The EFCC also has the authority to prevent the use of charitable and nonprofit entities as laundering vehicles, though no such case has yet been reported. There were 23 money laundering convictions in 2005 and 96 convictions through October 2006. The trial court process has improved after several experienced judges were assigned specifically to handle EFCC cases; this has motivated EFCC officials to bring more cases to court. Since its establishment the EFCC has reportedly seized assets worth $5 billion.

Depending on the nature of the case, the tracing, seizing, and freezing of assets may be done by the NDLEA, NPF, or the ICPC, in addition to the EFCC. The proceeds from seizures and forfeitures are remitted to the federal government, and a portion of the recovered sums is used to provide restitution to the victims of the criminal acts. While the NDLEA has the authority to handle narcotics-related cases, it does not have adequate resources to trace, seize, and freeze assets. Cases of this nature are usually referred to the EFCC. There were no significant narcotics related assets seizures in 2006.

For cases that are investigated by the EFCC, the seizure of property is governed by the EFCC (Establishment) Act of 2004. Section 20 of the act provides for the forfeiture of assets and properties to the federal government after the accused has been convicted of money laundering, including foreign assets acquired as a result of such crime. The properties subject to forfeiture are set forth in Section 24. They include any real or personal property that represents the gross receipts a person obtains directly as a result of the violation of the act or which is traceable to such gross receipts. They also include any property that represents the proceeds of an offense under the laws of a foreign country within whose jurisdiction such offense or activity would be punishable for a term exceeding one year. Section 25 states that all means of conveyance, including aircraft, vehicles, or vessels that are used or intended to be used to transport or in any manner to facilitate the transportation, sale, receipt, possession or concealment of economic or financial crimes would be punishable. Section 26 provides for circumstances under which property subject to forfeiture may be seized. Under the NDLEA act, farms on which illicit crops are cultivated can be destroyed. The banking community is cooperating with law enforcement to trace funds and seize or freeze bank accounts. It should be noted, however, that forfeiture is currently possible only under the criminal law. There is no comparable law governing civil forfeiture, but a committee has been set up by the EFCC to draft such legislation.

Nigeria is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. Nigeria ranks 146 out of 163 countries in Transparency International's 2006 Corruption Perception Index. The United States and Nigeria have a Mutual Legal Assistance Treaty, which entered into force in January 2003. Nigeria has signed memoranda of understanding with Russia, Iran, India, Pakistan and Uganda to facilitate cooperation in the fight against narcotics trafficking and money laundering. Nigeria has also signed bilateral agreements for exchange of information on money laundering with South Africa, the United Kingdom, and all Commonwealth and Economic Community of West African States countries. Nigeria has been instrumental in the establishment of a permanent secretariat for the Intergovernmental Task Force against Money Laundering in West Africa (GIABA). Nigeria has also ratified the African Union Convention on Preventing and Combating Corruption, which was adopted in Mozambique in July 2003.

The Government of Nigeria has done a better job in preventing and pursuing money laundering both within and outside the country in 2006. It should continue to engage with the FATF and other relevant international organizations to identify and eliminate remaining anti-money laundering deficiencies. Nigeria should continue to pursue their anticorruption program and support both the ICPC and EFCC in their mandates to investigate and prosecute corrupt government officials and individuals, while at the same time maintaining the independence of those entities, and prevent political encroachment. The supervision of banking and nonbanking financial institutions should be further strengthened and moved from the Ministry of Commerce. Nigeria should continue towards implementation of a

comprehensive anti-money laundering regime that promotes respect the rule of law, willingly shares information with foreign regulatory and law enforcement agencies, is capable of thwarting money laundering and terrorist financing, and maintains compliance with all relevant international standards.

## Pakistan

Pakistan is not considered a regional or offshore financial center; however, financial crimes related to narcotics trafficking, terrorism, smuggling, tax evasion and corruption are significant problems. Pakistan is a major drug-transit country. As a result of tighter controls in the financial sector, smuggling, trade-based money laundering, hawala, and physical cross-border cash transfers are the common methods used to launder money and finance terrorism in Pakistan. Pakistani criminal networks play a central role in the transshipment of narcotics and smuggled goods from Afghanistan to international markets. Pakistan has very little control of the border area, which allows the flow of smuggled goods to the Federally Administered Tribal Areas (FATA) and Balochistan. Goods such as foodstuffs, electronics, building materials, and other products that are primarily exported from Dubai to Karachi are falsely documented as destined for Afghanistan under the "Afghan Transit Trade Agreement," which allows goods to pass through Pakistan to Afghanistan exempt from Pakistani duties or tariffs. Through smuggling, corruption, avoidance of taxes, as well as barter deals for narcotics, many of the goods destined for Afghanistan find their way to the Pakistani black market. The proliferation of counterfeit goods and intellectual property rights violations generate substantial illicit proceeds that are laundered. A group of private, unregulated charities has also emerged as a major source of illicit funds for international terrorist networks. Another issue is the use of madrassas as training grounds for terrorists. The lack of control of madrassas, similar to the lack of control of Islamic charities, allows terrorist organizations to receive financial support under the guise of support of Islamic education.

Money laundering and terrorist financing are often accomplished in Pakistan via the alternative remittance system called hundi or hawala. This system is also widely used by the Pakistani people for informal banking and legitimate remittance purposes. Free trade zones do operate in Pakistan. The government established its first Export Processing Zone (EPZ) in Karachi in 1989 and has subsequently created additional EPZs in the Sindh and Balochistan provinces. Although no evidence has emerged of EPZs being used in money laundering, over-or under-invoicing is common in the region and could be used by entities operating out of these zones. Fraudulent invoicing is typical in hundi/hawala countervaluation schemes.

Pakistan has adopted measures to strengthen its financial regulations and enhance the reporting requirements for the banking sector, in order to reduce its susceptibility to money laundering and terrorism financing. For example, financial institutions must report within three days any funds or transactions they believe are proceeds of criminal activity. However, this is largely not observed by financial institutions because. Pakistan has not yet formally established a Financial Intelligence Unit (FIU) to which such reports of suspicious transactions can be filed. Additionally, there is no safe harbor provision for financial institutions to protect them from civil and criminal liability for filing such reports.

Pakistan has had a comprehensive anti-money laundering law under consideration by its parliament since 2005 although such legislation has not yet been enacted. As a result, the offense of money laundering cannot be prosecuted in Pakistan. Several law enforcement agencies have responsibility to enforce laws against financial crimes. The National Accountability Bureau (NAB), the Anti-Narcotics Force (ANF), the Federal Investigative Agency (FIA), and the Customs authorities all oversee Pakistan's law enforcement efforts. The major laws in these areas include: The Anti-Terrorism Act of 1997, which defines the crime of terrorist finance and establishes jurisdiction and punishments; the National Accountability Ordinance of 1999, which requires financial institutions to report corruption

related suspicious transactions to the NAB and establishes accountability courts; and The Control of Narcotics Substances Act of 1997, which also requires the reporting of narcotics related suspicious transactions to the ANF, contains provisions for the freezing and seizing of assets associated with narcotics trafficking, and establishes special courts for the offenses (including financing) involving illegal narcotics. Because Pakistan lacks a central repository for the reporting of suspicious transactions, due to confusion over which law enforcement agency should receive reports and the lack of protection from liability for reporting, suspicious transactions go largely unreported. The implementing laws for the law enforcement agencies such as NA, ANF, and FIA include provisions to allow investigators to access financial records and conduct financial investigations. However, none of these laws provides for the establishment and funding of a FIU.

Since 2002, the Ministry of Finance has been coordinating an inter-ministerial effort to draft AML and counterterrorism financing legislation, with the goal of bringing Pakistan into compliance with international standards. As of November 2006, draft AML legislation has been approved by the Cabinet and is currently being reviewed by the Standing Committee on Finance in the National Assembly. The draft law provides for the establishment of an FIU; however, the bill as it currently stands, does not meet international standards in several key respects. One problem is with the asset forfeiture scheme, particularly where its application is dependent upon a prosecution for the predicate offense. Another issue is with the filing of suspicious transactions reports, where the imposition of a threshold requirement—the minimum transaction amount to trigger a report—has yet to be determined. A provision for the exchange of information with the U.S. on all-source money laundering is contained in the draft AML bill.

The State Bank of Pakistan (SBP) and the Securities and Exchange Commission of Pakistan (SECP) are Pakistan's primary financial regulators. Notwithstanding the absence of stand-alone AML legislation, the SBP and SECP have independently established AML units to enhance their oversight of the financial sector. The SBP has introduced regulations intended to be consistent with FATF recommendations in the areas of "know your customer" policy, record retention, due diligence of correspondent banks, and the reporting of suspicious transactions. The SECP, which has regulatory oversight for nonbank financial institutions, has applied "know your customer" regulations to stock exchanges, trusts, and other nonbank financial institutions.

Pakistan's cooperation in the global war on terrorism has brought renewed focus on the role of informal financial networks in financing terrorist activity. In June 2004, the SBP required all hawaladars to register as authorized foreign exchange dealers and to meet minimum capital requirements. Failure to comply was punished by forced closures. However, despite increased enforcement efforts, unregistered hawaladars continue to operate illegally. A large percentage of hawala transfers to Pakistan are for the repatriation of wages from the roughly five million Pakistani expatriates residing abroad. The U.S. Government has observed an increasing migration of transactions from the informal to the formal financial institutions sector, due to countries' increased awareness and regulation of hawala, post-September 11 changes in the behavior patterns of overseas Pakistanis, and a substantial increase in credit available in the formal financial sector.

Pakistan has criminalized the financing of terrorism under its Anti-Terrorism Act of 1997. It includes the provision that it is a crime to enter into or become part of an arrangement that facilitates retention or control of terrorist property by or on behalf of another person, by concealment, removal from the jurisdiction, transfer to nominees, or in any other way. Pakistan, through the SBP, circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list as being linked with Usama Bin Laden, members of the al-Qaida organization or the Taliban. SBP has the ability to freeze bank accounts and property held by these individuals and entities. However, there have been some deficiencies concerning the timeliness and thoroughness of the asset freezing.

The Ministry of Social Welfare is drafting a Charities Registration Act bill. Under this bill, charities would have to prove the identity of their directors and open their financial statements to government scrutiny. Currently, charities can register under one of a dozen different acts, some dating back to the middle of the nineteenth century. The Ministry hopes that when the new legislation is enacted, it will be better able to monitor suspicious charities and ensure that they have no links to designated terrorists or terrorist organizations. The Act is not expected to be passed during the next year

Reportedly, bulk cash couriers are the major source of funding for terrorist activities. According to the Pakistan Central Board of Revenue, cash smuggling is an offense punishable by up to five years in prison. It is illegal for passengers to carry more than $10,000 per person. It is illegal to bring money into Pakistan except through legal banking channels; however, there are no reporting requirements upon entering the country. There are joint counters at international airports staffed by the SBP and Customs to monitor the transportation of foreign currency. However, enforcement is spotty and corruption rampant.

Pakistan enforces existing drug related asset seizure and forfeiture laws. Pakistan's Anti Narcotics Force shares information about seized narcotics assets and the number of arrests with the USG. Section 12 of the Control of Narcotic Substances Act of 1997 criminalizes the acquisition and possession of assets derived from drug money. The Act also makes it an offense to conceal or disguise the true nature, source, location, disposition, movement or ownership of such assets through false declaration. The suspected assets and properties shall also be liable to forfeiture. The SBP has the ability to freeze assets while the NAB, FIA, and ANF have the ability to seize assets.

Pakistan is an active member of the Asia/Pacific Group on Money Laundering (APG), although its failure to enact an AML law has called into question its commitment to membership, since the terms of reference of APG membership require a country to develop, pass and implement anti-money laundering and antiterrorist financing legislation and other measures based on accepted international standards. In 2005, the APG member states conducted a peer review of Pakistan's AML/CTF laws, rules and procedures. APG representatives identified a number of deficiencies and highlighted the need for a comprehensive AML law.

Pakistan is party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Crime and the UN Convention against Corruption. Pakistan is 142 out of 163 countries monitored in Transparency International's 2006 Corruption Perception Index. Pakistan has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

Five years after draft anti-money laundering (AML) legislation was first drafted, the Government of Pakistan should now move quickly to enact an AML law that comports with international standards. It also should issue financial regulations to consolidate and de-conflict the reporting of all suspicious transactions, and establish an FIU consistent with international standards. In addition, in light of the role that private charities have played in terrorist financing, Pakistan should work quickly to develop a system to regulate the finances of charitable organizations and to close those that finance terrorism. Pakistan also needs to exert greater efforts to track and suppress cash couriers. Per FATF Recommendation Nine, Pakistan should implement and enforce cross-border currency reporting requirements at a reporting threshold level that makes sense given the low-per capita income of the Pakistani people. Customs and financial police should be trained in recognizing trade-based money laundering and value transfer. Pakistan should explore establishing a Trade Transparency Unit (TTU) that will work with its major trading partners to examine trade anomalies that may be indicative of customs fraud and/or trade-based-money laundering. The establishment of a TTU could bring needed revenue streams to the government. Pakistan should become a party to the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of Terrorist

Financing, and the UN Convention against Corruption. Pakistan should take additional steps to address pervasive corruption at all levels of government and commerce.

## Palau

Palau is an archipelago of more than 300 islands in the Western Pacific with a population of 20,900 and per capita GDP of about $7,267. Upon its independence in 1994, the Republic of Palau entered the Compact of Free Association with the United States. The U.S. dollar is legal tender. Palau is not a major financial center. Nor does it offer offshore financial services. There are no offshore banks, securities brokers/dealers or casinos in Palau. The Authorities report that within the last year at least one trust company has been registered, though the scope and size of its business is unknown. Palauan authorities believe that drug trafficking and prostitution are the primary sources of illegal proceeds that are laundered.

In January 2005, Palau prosecuted its first ever case under the Money Laundering and Proceeds of Crimes Act (MLPCA) of 2001 (MLPCA) against a foreign national engaged in a large prostitution operation. The defendant was convicted on all three counts as well as a variety of other counts. Subsequently, Palau has prosecuted three more money laundering cases obtaining convictions in two of the cases. Two of the cases involved domestic proceeds of crime, while one of the cases involved criminal conduct both within and outside of Palau.

Amid reports in late 1999 and early 2000 that offshore banks in Palau had carried out large-scale money laundering activities, a few international banks banned financial transactions with Palau. In response, Palau established a Banking Law Review Task Force that recommended financial control legislation to the Olbill Era Kelulau (OEK), the national bicameral legislature, in 2001. Following that, Palau took several steps toward addressing financial security through banking regulation and supervision and putting in place a legal framework for an anti-money laundering regime. Several pieces of legislation were enacted in June 2001.

The Money Laundering and Proceeds of Crimes Act (MLPCA) of 2001 criminalized money laundering and created a financial intelligence unit. This legislation imposes suspicious transactions reporting (for suspicious transactions over $10,000) and record keeping requirements for five years from the date of the transaction. Credit and financial institutions are required to keep regular reports of all transactions made in cash or bearer securities in excess of $10,000 or its equivalent in foreign cash or bearer securities. This threshold reporting also covers domestic or international transfers of funds of currency or securities involving a sum greater than $10,000. All such transactions (domestic and/or international) are required to go through a credit or financial institution licensed under the laws of the Republic of Palau.

The Financial Institutions Act of 2001 established the Financial Institutions Commission, an independent regulatory agency, which is responsible for licensing, supervising and regulating financial institutions, defined as banks and security brokers and dealers in Palau. The insurance industry is not currently regulated by the FIC and insurance companies in Palau are primarily agents for companies registered in the U.S. or out of the U.S. Territory of Guam. Currently, there are seven licensed banks in Palau and all are majority foreign owned. On November 7, 2006, the FIC closed the second largest and the only locally owned bank, Pacific Savings Bank, for illiquidity and insolvency. The Receiver has filed several civil actions against former bank insiders and the litigation is ongoing. An amendment intended to strengthen the supervisory powers of the FIC and promote greater financial stability within Palau's bank market passed its first reading in the Senate in January 2005 but the Senate Committee on Ways and Means and Financial Matters did not report out the bill until December 2006 when the bill was referred back to the Committee for further study.

Other entities subject to the provisions of the MLPCA, such as the three money services businesses, four finance companies and five insurance companies, are essentially unsupervised. Once the amendments to the MLPCA are passed, all alternative money remittance systems will be licensed and regulated by the FIC. The amendments to the MLPCA were introduced in the Senate in 2004 and passed in March 2006. The amendments passed their first reading in the House of Delegates in March 2006 and were referred to the House Committee on Ways and Means and Financial Matters where they remain. Credit and financial institutions are required to verify customers' identity and address. In addition, these institutions are required to check for information by "any legal and reasonable means" to obtain the true identity of the principal/party upon whose behalf the customer is acting. If identification cannot, in fact, be obtained, all transactions must cease immediately.

The lack of both and human and fiscal resources has hampered the development of a viable anti-money laundering regime in Palau. The Republic has only recently established a functioning Financial Intelligence Unit (FIU), though its operations are severely restricted by a lack of dedicated human and no dedicated budget. The implementing regulations to ensure compliance with the MLPCA have yet to be written but the authorities have stated that they will be drafted once the revisions to the MLPCA have been passed. The will of the Executive branch to comply with international standards, however, was clearly demonstrated by President Remengesau in 2003, when he vetoed a bill that would have extended the deadline for bank compliance and would have reduced the minimum capital for a bank from $500,000 to $250,000. Additionally, the President established the Anti-Money Laundering Working Group that is comprised of the Office of the President, the FIC, the Office of the Attorney General, Customs, the FIU, Immigration and the Bureau of Public Safety.

Palau has enacted several legislative mechanisms to foster international cooperation. The Mutual Assistance in Criminal Matters Act (MACA), passed in June 2001, enables authorities to cooperate with other jurisdictions in criminal enforcement actions related to money laundering and to share in seized assets. The Foreign Evidence Act of 2001 provides for the admissibility in civil and criminal proceedings of certain types of evidence obtained from a foreign State pursuant to a request by the Attorney General under the MACA. Under the Compact of Free Association with the United States, a full range of law enforcement cooperation is authorized and in 2004 Palau was able to assist the Department of Justice in a money laundering investigation by securing evidence critical to the case and freezing the suspected funds. Palau has also entered into an MOU with the Taiwan, R.O.C. and the Philippines for mutual sharing of information and inter-agency cooperation in relation to financial crimes and money laundering.

Pursuant to the adoption of the Asia/Pacific Group's (APG) mutual evaluation of Palau at its September 2003 Plenary, the Government of Palau (GOP) has proposed amendments to the MLPCA that, if enacted, would strengthen Palau's anti-money laundering regime. Among the more significant proposals are the following: the promulgation of reporting regulations for all covered financial institutions as well as alternative remittance providers; the requirement to obtain the identification of the beneficial owner of any type of account; mandatory reporting of suspicious transaction reports to the FIU regardless of the amount of the transaction; the requirement that any currency transaction over $5000 be done by wire transfer; the requirement that alternative remittance systems providers report any cash remittance over $500; and, a burden shifting regime for the seizure and forfeiture of assets upon a conviction for money laundering.

The President has also recently proposed the Cash Courier Act of 2004 that was drafted by the Palau Anti-Money Laundering Working Group. The bill passed the Senate in March 2006 and went to the House of Delegates where it passed its first reading in the same month and was referred to the House Committee on Ways and Means and Financial Matters where, once again, it remains.

The Counter-Terrorism bill, which also has anti-money laundering provisions, was originally introduced in September 2002, but was not acted on by the Senate. An amended version of the Bill

was reintroduced in January 2005 and the Senate passed it in January 2006. The bill is in the House of Delegates. If enacted with changes proposed by the President of the Republic, the Act would comport with current international standards, including provisions for the freezing of assets of entities and persons designated by the United Nations as terrorists or terrorist organizations, provisions for the regulation of nonprofit entities to prevent abuses by criminal organizations and terrorists and provisions for criminalizing the financing of terrorism. The OEK has issued resolutions ratifying Palau's accession to all the United Nation's Conventions and Protocols relating to terrorism.

The Government of Palau has taken several steps toward enacting a legal framework by which to combat money laundering. It has signed Pacific Island Forum anti-money laundering initiatives and as a member of the Asia/Pacific Group on Money Laundering, Palau is committed to implement the Financial Action Task Force Revised Forty Recommendations and its Nine Special Recommendations on Terrorist Financing. As a party to the UN Convention for the Suppression of the Financing of Terrorism, Palau should criminalize the financing of terrorism. In continuing it efforts to comport with international standards, Palau should enact legislation and promulgate implementing regulations to the MLPCA, as recommended by the APG, including but not limited to establishing funding for the FIU, eliminating the threshold for reporting suspicious transactions and beginning a broad-based implementation of the legal reforms already put in place.

## Panama

Panama is a major drug-transit country, and is particularly vulnerable to money laundering because of its proximity to Colombia and other drug-producing countries. Colombian nationals are able to enter Panama without visas, facilitating the investment of drug money into Panama's economy. The economy of Panama is 80 percent service-based, 14 percent industry and 6 percent agriculture. The service sector is comprised mainly of maritime transportation, commerce, tourism, banking and financial services.

Panama's sophisticated international banking sector, Colon Free Zone (CFZ), U.S. dollar-based economy, and legalized gambling sector are utilized to facilitate potential money laundering. The CFZ serves as an originating or transshipment point for some goods purchased with narcotics proceeds (mainly dollars obtained in the United States) through the Colombian Black Market Peso Exchange. There are approximately 1,400 businesses operating in the CFZ, facilitating opportunities for trade-based money laundering. Reports indicate that the amount of money passing through casinos increased by over 200 percent in 2006. The present construction boom also presents opportunities for money laundering. As many as 150 new high-rise buildings are currently being constructed. Some of the new construction is due to construction tax breaks which ended December 31, 2006.

Panama has the second highest number of offshore-registered companies in the world. Panama's large offshore financial sector includes international business companies, offshore banks, captive insurance companies and fiduciary companies. Law No. 42 of October 2000 requires Panamanian trust companies to identify to the Superintendence of Banks the real and ultimate beneficial owners of trusts. Executive Decree 213 of October 2000, amending Executive Order 16 of 1984 (trust operations), provides for the dissemination of information related to trusts to appropriate administrative and judicial authorities.

Law No. 41 (Article 389) of October 2000 amended the Penal Code by expanding the predicate offenses for money laundering beyond narcotics trafficking, to include criminal fraud, arms trafficking, trafficking in humans, kidnapping, extortion, embezzlement, corruption of public officials, terrorism, and international theft or trafficking of motor vehicles. Law No. 41 establishes a punishment of 5 to 12 years' imprisonment and a fine. In June 2003, the Panamanian Legislative Assembly approved the Financial Crimes Bill (Law No. 45), which established criminal penalties of up to ten years in prison and fines of up to one million dollars for financial crimes that undermine

public trust in the banking system, the financial services sector, or the stock market. The penalties criminalized a wide range of activities related to financial intermediation, including illicit transfers of monies, accounting fraud, insider training, and the submission of fraudulent data to supervisory authorities. Law No. 1 of January 2004 added crimes against intellectual property as a predicate offense for money laundering.

Law No. 42 requires financial institutions to report to Panama's financial intelligence unit (FIU), the Financial Analysis Unit of the Treasury Ministry (Unidad de Análisis Financiero, or UAF), suspicious financial transactions and currency transactions in excess of $10,000. Casinos, CFZ businesses, the national lottery, real estate agencies and developers, and insurance and reinsurance companies are also required report to the UAF currency or quasi-currency transactions that exceed $10,000. Under Law No. 48 of June 2003 and Law No. 16 of May 2005, money remitters and pawnshops are also subject to anti-money laundering regulations. Resolutions Nos. 327 and 328 of August 2004 of the Ministry of Commerce and Industries similarly require promotional companies and real estate agents to identify their clients, declare cash transactions over $10,000, and report suspicious transactions to the UAF.

In October 2000, Panama's Superintendent of Banks issued Agreement No. 9 that defines requirements that banks must follow for identification of customers, exercise of due diligence, and retention of transaction records. It also increased the number of inspections of finance companies it conducted. In 2005, the Superintendence of Banks modified that Agreement, in order to include fiduciary (offshore) companies within the measures of prevention of illegal use and to bring the Banking Center into line with the highest international standards, thus increasing compliance with the Financial Action Task Force (FATF) Recommendations.

The Autonomous Panamanian Cooperative Institute established a specialized unit for the supervision of loans and credit cooperatives regarding compliance with the requirements of Law No. 42. The National Securities Commission carried out numerous training sessions and workshops for its personnel and regulated entities. The CFZ possesses and issues a procedures manual for the users of the CFZ, outlining their responsibilities regarding prevention of money laundering and requirements under Law No. 42. In 2006, the UAF continued efforts to raise the level of compliance for reporting suspicious financial transactions, particularly by nonbank financial institutions and trading companies within the CFZ.

With support from the Inter-American Development Bank (IDB), the Government of Panama (GOP) is implementing a "Program for the Improvement of the Transparency and Integrity of the Financial System." This Transparency Program is targeted, through enhanced communication and information flow, training programs and technology, at strengthening the capabilities of those government institutions responsible for preventing and combating financial crimes and terrorist financed activities. Employees from 14 different institutions have received training, including bank compliance officials, and representatives of the private sector, stock markets and credit unions. In addition, Panama has launched an educational campaign to prevent money laundering and terrorist financing. The program began in 2002 and is intended to raise consciousness of citizens regarding these crimes. This program has included hosting a hemispheric congress on the prevention of money laundering in 2004 and 2006.

In 2005, a pilot program was developed for money laundering prevention training, which was financed by the IDB and executed by the Caribbean Financial Action Task Force (CFATF). The training has reached over 5,000 public and private sector employees. Participants have been from various financial institutions, insurance companies, the CFZ and money order companies.

To increase GOP interagency coordination, the UAF and the Panamanian Customs are developing an office at the Tocumen International Airport to expedite the entry of customs currency declaration information into the UAF's database. This has enabled the UAF to begin more timely investigations. The creation of a joint airport interdiction task force at Tocumen, made up of members from the Panamanian National Police (PNP), Technical Judicial Police (PTJ), National Air Service (SAN),

Customs and Immigration has produced significant seizures of undeclared currency. In 2006, a total of $4.7 million in undeclared currency was seized. The most significant seizures were in two separate incidents where gold bars painted silver were seized from Mexican nationals traveling from Mexico through Panama en route to Colombia. The Task Force also participated in a continuous operation designed to interdict bulk cash smuggling ("Operation Firewall") in coordination with U.S. Embassy Narcotics Affairs Section and U.S. Immigration and Customs Enforcement (ICE).

Executive Order No. 163 of October 2000, which amended the June 1995 decree that created the UAF, allows the UAF to provide information related to possible money laundering directly to the Office of the Attorney General for investigation. Panama has initiated cases for domestic prosecution, and the UAF routinely transfers cases to the PTJ's Financial Investigations Unit for investigation. During 2006, Panama worked with the United States on two large cases. The first involved a gold and jewelry company in the CFZ that was used to launder money. Assets estimated at over $30 million were seized in connection with this case. The second case was connected to an international narcotics trafficking case in which an entire trafficking organization was taken down. In Panama alone an estimated $25 million in assets were seized. Both cases have ongoing investigations as a result of information obtained. Panama assists other Central American countries with investigations. For example, Panama assisted Nicaragua with the corruption case against former Nicaraguan President Arnoldo Aleman. Panama also assisted Costa Rica and Peru in investigating allegations against high ranking political figures in each country.

Panama identified the combating of money laundering as one of five goals in its five-year National Drug Control Strategy issued in 2002. The Strategy commits the GOP to devote $2.3 million to anti-money laundering projects, the largest being institutional development of the UAF. The UAF currently maintains inter-institutional cooperation agreements with the Attorney General's Office and the Superintendence of Banks, and has signed a cooperation agreement with the Public Registry of Panama.

Terrorist financing is a criminal offense in Panama. Decree No. 22 of June 2003 gave the Presidential High Level Commission against Narcotics Related Money Laundering responsibility for combating terrorist financing. Law No. 50 of July 2003 criminalizes terrorist financing and gives the UAF responsibility for prevention of this crime. There are no legal impediments to the GOP's ability to prosecute or extradite suspected terrorists. Public security sources and the judicial system have limited resources to deter terrorists; however, there are several special investigations units capable of carrying out investigations.

In January 2003 the GOP entered into a border security cooperation agreement with Colombia and also increased funds to the Frontier Division of the National Police to assist in border security. The GOP and the Government of Colombia hold quarterly meetings to discuss border security initiatives of mutual interest to the two countries. The GOP has also created the Department of Analysis and Study of Terrorist Activities. This department is tasked with working with the United Nations and the Organization of American States (OAS) to investigate transnational issues, including money laundering. Panama has an implementation plan for compliance with the FATF 40 Recommendations on Money Laundering and Nine Special Recommendations on Terrorist Financing.

In May 2005, the International Monetary Fund (IMF) conducted an assessment of Panama's Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) under the new FATF methodology. The assessment has also been accepted by the CFATF as its mutual evaluation of Panama. Since its assessment, Panama has taken many steps to implement evaluator's recommendations, including providing adequate training to government officials and issuing new regulations to financial institutions to ensure that they continue filing suspicious transaction reports to the UAF.

The GOP remains active in international anti-money laundering efforts, including the multilateral Black Market Peso Exchange Group Directive. In March 2002, the GOP signed the cooperation agreement issued by the working group as part of a regional effort against the black market system. Panama is a member of the OAS Inter-American Drug Abuse Control Commission (CICAD), and served as the Chair of CFATF and the Central American Council of Superintendents of Banks, Insurance Companies and Other Financial Institutions during 2004 and 2005. Panama is currently the vice-president of the Association of Supervisors of Banks in the Americas (ASBA), with the term running through 2007. The GOP is also a member of the Offshore Group of Banking Supervisors. The UAF is a member of the Egmont Group.

Panama is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the Inter-American Convention against Terrorism. Panama is also a signatory to 11 of the UN terrorism conventions and protocols. Panama and the United States have a Mutual Legal Assistance Treaty that entered into force in 1995. The GOP has also assisted numerous countries needing help in strengthening their anti-money laundering programs, including Guatemala, Costa Rica, Russia, Honduras, and Nicaragua. Executive Decree No. 163 authorizes the UAF to share information with FIUs of other countries, subject to entering into a memorandum of understanding (MOU) or other information exchange agreement. Panama currently has 37 such MOUs with other countries, including the United States.

During 2006, the Government of Panama has continued to make progress in strengthening its anti-money laundering regime. The GOP has been a cooperating partner to the United States and other countries throughout the world in investigating money laundering crimes that have a nexus in Panama. Panama should continue its regional assistance efforts. It should emphasize effective law enforcement actions that address Panama's continuing vulnerabilities such as smuggling, abuse of the real estate sector, trade-based money laundering, and the proliferation of nontransparent offshore companies.

## Paraguay

Paraguay is a principal money laundering center, involving both the banking and nonbanking financial sectors. The multi-billion dollar contraband re-export trade that occurs on the borders shared with Argentina and Brazil, the Triborder Area, facilitates much of the money laundering in Paraguay. Paraguay is a major drug-transit country. The Government of Paraguay (GOP) suspects that proceeds from narcotics trafficking are often laundered, but it is difficult to determine the percentage of the total amount of laundered funds generated from narcotics sales. Weak controls in the financial sector, an open border, and minimal enforcement activity for financial crimes allow money launderers and terrorist financiers to take advantage of Paraguay's financial system. The GOP successfully prosecuted a major money laundering case in 2006 and has demonstrated an increased willingness to press money laundering charges against defendants notwithstanding the limitations of current laws.

Paraguay is particularly vulnerable to money laundering, as little personal background information is required to open a bank account or to conduct financial transactions in Paraguay. Paraguay is an attractive financial center for neighboring countries, particularly Brazil. Foreign banks are registered in Paraguay and nonresidents are allowed to hold bank accounts, but current regulations forbid banks from advertising or seeking deposits from outside the country. Paraguay is not considered to be an offshore financial center, but the GOP does allow representative offices of offshore banks to maintain a presence in the country. Shell companies are not permitted; trusts, however, are permitted and are regulated by the Central Bank. The Superintendence of Banks audits financial institutions and supervises all banks under the same rules and regulations. However, there are few effective controls over businesses, and a large informal economy exists outside the regulatory scope of the GOP. A number of cooperatives function effectively as financial institutions and may have as much as 30

percent of financial system assets. These co-ops, as they are known, are not regulated by the Superintendent of Banks but are instead self-regulated. The industry organization charged with oversight—INCOOP—issues guidelines, but does not have regulatory authority to compel compliance with anti-money laundering or prudential measures.

The multi-billion dollar contraband re-export trade that occurs largely in the Triborder Area shared by Paraguay, Argentina, and Brazil facilitates money laundering in Paraguay. Ciudad del Este (CDE), on the border between Brazil and Paraguay, represents the heart of Paraguay's informal economy. The area is well known for arms and narcotics trafficking, as well as crimes against intellectual property rights. The illicit proceeds from these crimes are an additional source of laundered funds. A wide variety of counterfeit goods, including cigarettes, CDs, DVDs, and computer software, are imported from Asia and transported primarily across the border into Brazil, with a significantly smaller amount remaining in Paraguay for sale in the local economy. Some senior government officials, including members of Congress, have been accused of involvement in the smuggling of contraband or pirated goods. To date, there have been few criminal investigations, much less prosecutions of senior GOP officials' involvement in smuggling contraband or pirated goods. Paraguay has taken some measures to tackle the "gray" economy and to develop strategies to implement a formal, diversified economy. The Ministry of Industry and Commerce's Specialized Technical Unit (UTE), working in close coordination with the Attorney General's Trademarks and Intellectual Property Unit, has effectively opened a number of significant investigations against groups involved in piracy.

On December 6, 2006, the U.S. Department of Treasury designated nine individuals and two entities in the Triborder Area that have provided financial or logistical support to Hizballah. The nine individuals operate in the Triborder Area and all have provided financial support and other services for Specially Designated Global Terrorist Assad Ahmad Barakat, who was previously designated by the U.S. Treasury in June 2004 for his support to Hizballah leadership. The two entities, Galeria Page and Casa Hamze, are located in Ciudad del Este and have been used to generate or move terrorist funds. The GOP has publicly disagreed with the designations, stating that the U.S. has not provided any new information that would prove terrorist financing activity is occurring in the Triborder Area.

Money laundering is a criminal offense under Paraguay's two anti-money laundering statutes, Law 1015 of 1996 and Article 196 of Paraguay's Criminal Code, adopted in 1997. The existence of the two laws has led to substantial confusion due to overlapping provisions. Under Article 196, the scope of predicate offenses includes only offenses that carry a maximum penalty of five years or more; Law 1015 includes additional offenses. Article 196 also establishes a maximum penalty of five years for money laundering offenses, while Law 1015 carries a prison term of two to ten years. This is particularly significant because, under the Criminal Code and Criminal Procedure Code, defendants who accept charges that carry a maximum penalty of five years or less are automatically entitled to a suspended sentence and a fine instead of jail time, at least for the first offense. Since a defendant cannot be charged with money laundering unless he or she has first been convicted of the predicate offense, many judges are apparently reluctant to prosecute defendants on money laundering charges because a sentence has already been issued for a predicate offense.

Law 1015 of 1996 also contains "due diligence" and "banker negligence" provisions and applies money laundering controls to nonbanking financial institutions, such as exchange houses. Bank secrecy laws do not prevent banks and financial institutions from disclosing information to bank supervisors and law enforcement entities. Under Paraguay's Commercial Law 1023 and Law 1015, banks are required to maintain account records for five years, but there is little government enforcement of this regulation. Bankers and others are protected under the anti-money laundering law with respect to their cooperation with law enforcement agencies. Additional provisions of Law 1015 require banks, finance companies, insurance companies, exchange houses, stock exchanges and securities dealers, investment companies, trust companies, mutual and pension funds administrators, credit and consumer cooperatives, gaming entities, real estate brokers, nongovernmental organizations,

pawn shops, and dealers in precious stones, metals, art and antiques to know and record the identity of customers engaging in significant currency transactions and to report those, as well as suspicious activities, to Paraguay's financial intelligence unit (FIU), the Unidad de Análisis Financiera (UAF). The UAF received over 3,000 suspicious activity reports from these entities in 2006, a significant improvement over previous years.

The UAF began operating in 1997 within the Secretariat to Combat Money Laundering (SEPRELAD), under the auspices of the Ministry of Industry and Commerce (MIC). In recent years, the GOP has made significant efforts to strengthen SEPRELAD, and as a result, cooperation between SEPRELAD and other government agencies on anti-money laundering issues has improved. Initially reluctant to seek SEPRELAD's assistance due to past weaknesses, most government entities are increasingly prepared to work with SEPRELAD. SEPRELAD has signed several agreements with other government entities to strengthen interagency cooperation, including memoranda of understanding with the Public Ministry and the Superintendence of Banks. In 2005 the UAF and the Superintendence of Banks' Risk Control Division, which has the primary responsibility of reviewing the records of national financial institutions for suspected terrorist activity and is empowered to coordinate information exchange with the Central Banks of other MERCOSUR countries, signed a memorandum of understanding (MOU) laying out the provisions for increased cooperation. The MOU includes provisions for SEPRELAD to issue regulations for the banking industry, including the designations of a compliance officer and utilizing due diligence and "know your customer" policies, which are included in Resolution 233 of 2005.

The UAF is seeking to strengthen its relationship with other financial intelligence units and has signed agreements for information exchange with regional FIUs. The UAF also increased its role in regional and international anti-money laundering groups, including the Egmont Group and the Financial Action Task Force for South America (GAFISUD). The UAF's director participates in the GAFISUD FIU Working Group and a committee within the Egmont Group, further expanding Paraguay's role in these organizations. GAFISUD conducted its second mutual evaluation of Paraguay in 2005, finding Paraguay to be noncompliant with counterterrorist financing standards and its legal framework for investigating cases deficient.

A new law to improve the effectiveness of Paraguay's anti-money laundering regime was drafted in late 2003 and was formally introduced to Congress in 2004. This legislation has since been broken down and incorporated into three bills emerging through a multi-institutional legal reform commission. Proposed amendments to Paraguay's Penal Code, including enhanced legislation on money laundering, were introduced to Congress in October 2006. The other two bills addressing procedural reform and administrative structures should be introduced in early 2007. The proposed amendments also include legislation criminalizing the financing of terrorism. A bill on terrorist financing had been drafted in 2004, yet was not introduced until the amendments to the Penal Code were proposed.

In addition to confirming the UAF's role as the sole FIU, the new legislation establishes SEPRELAD as an independent secretariat or agency reporting directly to the Office of the President. The amendments to the Penal Code submitted to Congress in October establish money laundering as an autonomous crime punishable by a prison term up to 8 years, terrorism financing up to 15 years and terrorism punishable up to 30 years. It establishes predicate offenses as any crimes that are punishable by a prison term exceeding six months, and specifically criminalizes money laundering tied to the financing of terrorist groups or acts. The full range of covered institutions will be required to maintain registries of large currency transactions that equal or exceed $10,000, in addition to complying with existing suspicious transaction reporting requirements.

Other provisions of the draft bills include penalties for failure to file, falsification of reports, enhanced "know-your-client" provisions, and standardized record keeping for a minimum of five -years. The

UAF will continue to refer cases as appropriate for further investigation by Paraguay's Anti-Drug Secretariat (SENAD) and to the Attorney General's Office for prosecution. It will also serve as the central entity for related information exchanges with other concerned foreign entities. The bills further specify that the financial crimes investigative unit of SENAD is the principal authority for carrying out all counternarcotics and other financial investigations, including money laundering, and will also have the authority to initiate investigations on its own.

There are other challenges, however, that the new money laundering legislation, when passed, will not address. With only eight positions available for prosecutors dedicated to financial crimes, of which only six are filled, Paraguay currently has limited resources to investigate and prosecute money laundering and financial crimes. New criteria were issued in 2005 for the selection of judges, prosecutors and public defenders; however, the process remains one that is largely based on politics, nepotism and influence peddling, affording the ruling party an opportunity to manipulate the justice system to its advantage.

Moreover, unless the new legislation is enacted, most judges have little incentive to receive money laundering cases because many believe that sentencing on predicate offenses is sufficient punishment. As it is, those individuals implicated in money laundering are typically prosecuted on tax evasion charges. For example, in May 2004, Assad Barakat—widely alleged to be involved in money laundering and designated by the United States as a financier of terrorism—was convicted of tax evasion and sentenced to six and one-half years in prison. In late 2004, prosecutors began investigating several tax evasion cases involving suspected money laundering by both authorized and unauthorized money exchange offices in Ciudad del Este. A case against Lebanese businessman Kassem Hijazi, suspected of having laundered proceeds from illicit activities in the Triborder Area and sending a portion of those funds to support Lebanese Hizbollah activities, is ongoing on the basis on tax evasion charges, not money laundering.

In spite of limitations in prosecuting Barakat and Hijazi, the GOP is making improvements in its ability to successfully investigate and prosecute some money laundering cases. Daniel Fretes Ventre, a former Inspector General under President Wasmosy in the 1990s, was sentenced by an Appeals Court to 12 years in prison and fined $68,000 for money laundering and other crimes on October 24, 2006. Several members of his family were convicted on the same charges. Fretes and his accomplices laundered money through a family-established college and three family-owned businesses. In addition to the above-noted penalties, authorities confiscated 11 family-owned properties in Asuncion and Ciudad del Este. This case represents the most significant money laundering conviction—from less than a handful to date—and reinforces the fact that convictions are possible, although difficult under the current legal framework. Fretes Ventre has appealed this decision to the Supreme Court.

In cooperation with the U.S. Department of Homeland Security's Office of Immigration and Customs Enforcement (ICE), Paraguay is in the process of developing a Trade Transparency Unit (TTU) that will examine discrepancies in trade data that could be indicative of customs fraud, trade-based money laundering, or the financing of terrorism. The development of such a unit constitutes a positive step with respect to Special Recommendation VI of the Financial Action Task Force (FATF) on the use of alternative remittance systems. Trade-based systems such as hawala and black market exchanges often use fraudulent trade documents and over and under-invoicing schemes to provide counter valuation in transferring value and settling accounts.

Despite its low rating on corruption and other indices that prevented Paraguay from qualifying to participate fully in the Millennium Challenge Account (MCA) Compact Program, Paraguay was invited to participate in the MCA's Threshold Program. In May, Paraguay signed a Threshold Program agreement to receive $34.9 million in assistance to address the problems of impunity and informality, both of which hamper law enforcement efforts and contribute to money laundering. Paraguay's Millennium Challenge Account Threshold Program also supports the continued development of the

"maquila" sector, which comprises businesses operating for export (of either goods or services) that enjoy special tax advantages. Since the GOP stepped up promotion beginning in 2004, the sector has experienced rapid growth. The new customs code implemented in early 2004 provides for the creation of formal free trade zones. One zone currently exists in Ciudad del Este and another is planned for the town of Villeta, near Asuncion. Paraguay's customs agency is responsible for monitoring these zones; however, there is little oversight. As a result, the addition of free trade zones may provide additional venues for money laundering.

There are no effective controls or laws that regulate the amount of currency that can be brought into or out of Paraguay. Cross-border reporting requirements are limited to those issued by airlines at the time of entry into Paraguay. Persons transporting $10,000 into or out of Paraguay are required to file a customs report, but these reports are often not actually collected or checked. Customs operations at the airports or land ports of entry provide no control of the cross-border movement of cash. The nonbank financial sector, particularly exchange houses, is used to move illegal proceeds both from within and outside of Paraguay into the formal banking system of the United States. Paraguay exercises a dual monetary system in which most high-priced goods are paid for in U.S. dollars. Large sums of dollars generated from normal commercial activity and suspected illicit commercial activity are transported physically from Paraguay through Uruguay to banking centers in the United States. The GOP is only just beginning to recognize and address the problem of the international transportation of currency and monetary instruments derived from illegal sources. Recently, though, the commercial banks operating in Paraguay have dropped exchange houses as clients based on pressure from either their home offices or correspondent banks in the United States, which have told them that they would sever the relationship if the banks maintained accounts of exchange houses. The principal state-owned bank was also forced to drop the accounts of the exchange houses rather than lose its correspondent relationship with a U.S. bank.

Bank fraud, which has led to several bank failures, and other financial crimes related to corruption, are serious problems in Paraguay. Following bank failures in 2002 and 2003, Paraguay continues to experience problems in the banking industry. The GOP has worked with the U.S. Treasury and Justice Departments to trace, account for, and seek the return of the $16 million diverted in 2002 to private accounts linked to the family of former President Luis Gonzalez Macchi. However, corruption charges against Macchi were dropped in November after the court failed to meet the deadline for hearing full testimony on the accusations. Under the current interpretation of laws, the GOP has limited authority to seize, or forfeit assets of suspected money launderers. In most cases, assets that the GOP is permitted to, seize, or forfeit are limited to transport vehicles, such as planes and cars, and normally do not include bank accounts. However, authorities may not auction off these assets until a conviction is announced by the judicial system. At best, the GOP can establish a "preventative seizure" (which has the same effect as freezing) against assets of persons under investigation for a crime in which the state risks loss of revenue from furtherance of a criminal act, such as tax evasion. However, in those cases the limit of the seizure is set as the amount of liability of the suspect to the government. More recently, SENAD has been permitted to use on a temporary basis assets seized on cases not yet decided provided it pays no maintenance or repair costs. The new anti-money laundering legislation will, when passed, allow prosecutors to recommend that judges seize or confiscate assets connected to money laundering and its predicate offenses. The draft law also provides for the creation of a special asset forfeiture fund to be administered by a consortium of national governmental agencies, which will support programs for crime prevention and suppression, including combating money laundering, and related training.

The GOP currently has no authority to freeze, seize, or forfeit assets related to the financing of terrorism, which is not yet criminalized under current Paraguayan law. However, the Ministry of Foreign Affairs often provides the Central Bank and other government entities with the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee consolidated

list. To date, the GOP has not identified, seized, or forfeited any such assets linked to these groups or individuals. The current law also does not provide any measures for thwarting the misuse of charitable or nonprofit entities that can be used as conduits for the financing of terrorism. Following the submission of the draft anti-money laundering law to Congress in May 2004, a working group began drafting legislation to address terrorism, terrorist association and terrorist financing. This draft legislation, also incorporated into the legal reforms to Paraguay's penal, procedural and administrative codes, will allow the GOP to conform to international standards on the suppression of terrorist financing. The anti-money laundering provisions of the proposed legal reforms also specifically criminalize money laundering tied to the financing of terrorist groups or acts.

The GOP is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the Inter-American Convention on Terrorism, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. Paraguay participates in the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) money laundering experts working group, and is a member of GAFISUD and the "3 Plus 1" Security Group between the United States and the Triborder Area countries. The UAF has been a member of the Egmont Group since 1998.

While the Government of Paraguay took a number of positive steps in 2006, there are other initiatives that should be pursued to increase the effectiveness of Paraguay's efforts to combat money laundering and terrorist financing. Most important is enactment of legislation that meets international standards and enables law enforcement authorities to more effectively investigate and prosecute money laundering and terrorist financing cases. Paraguay also should continue its efforts to combat corruption and increase information sharing regarding corruption among concerned agencies when and if the corruption issues arises. Paraguay does not have a counterterrorism law or a law criminalizing terrorist financing, and the GOP should take steps as quickly as possible to ensure that comprehensive counterterrorism legislation, including the terrorist financing legislation introduced in October 2006, is passed in the context of the penal and procedural code reform process. Further reforms in the selection of judges, prosecutors and public defenders are needed, as well as reforms to the customs agency in order to allow for increased inspections and interdictions at ports of entry and to develop strategies targeting the physical movement of bulk cash. It is essential that the Unidad de Análisis Financiera (UAF) continue to receive the financial and human resources necessary to operate as an effective, fully functioning financial intelligence unit capable of effectively combating money laundering, terrorist financing, and other financial crimes. The GOP should also enter into a mutual legal assistance treaty with the United States.

## Peru

Peru is not a major regional financial center, nor is it an offshore money laundering haven. Peru is a major drug producing and drug-transit country. Narcotics-related and other money laundering does occur, and the Government of Peru (GOP) has taken several steps to improve its money laundering legislation and enforcement abilities in recent years. Nevertheless, more reliable and adequate mechanisms are necessary to better assess the scale and methodology of money laundering in Peru. Peru is the world's second largest producer of cocaine, and, although no reliable figures exist regarding the exact size of the narcotics market in Peru, estimates indicate that the cocaine trade generates in a range of one to two billion dollars per year, or up to 2.5 percent of Peru's GDP. As a result, money laundering is believed to occur on a significant scale in order to integrate these illegal proceeds into the Peruvian economy.

Money laundering has historically been facilitated by a number of factors, primarily Peru's cash-based economy. Peru's economy is heavily dependent upon the U.S. dollar, and approximately 65 percent of the economy is dollarized, allowing traffickers to handle large bulk shipments of U.S. currency with

minimal complications. Currently no restrictions exist on the amount of foreign currency an individual can exchange or hold in a personal account, and until recently, there were no controls on bulk cash shipments coming into Peru.

Corruption remains an issue of serious concern in Peru. It is estimated that 15 percent of the public budget is lost due to corruption. A number of former government officials, most from the Fujimori administration, are under investigation for corruption-related crimes, including money laundering. These officials have been accused of transferring tens of millions of dollars in proceeds from illicit activities (e.g., bribes, kickbacks, or protection money) into offshore accounts in the Cayman Islands, the United States, and/or Switzerland. The Peruvian Attorney General, a Special Prosecutor, the office of the Superintendent of Banks (SBS), and the Peruvian Congress have conducted numerous investigations, some of which are ongoing, involving dozens of former GOP officials.

Since June 2002, Peru has adopted substantial changes to its existing anti-money laundering regime, significantly broadening the definition of money laundering beyond a crime associated with narcotics trafficking. Prior to the changes, money laundering was only a crime when directly linked to narcotics trafficking and "narcoterrorism," It also included nine predicate offenses that did not include corruption, bribery or fraud. Under Law 27.765 of 2002, predicate offenses for money laundering were expanded to include the laundering of assets related to all serious crimes, such as narcotics trafficking, terrorism, corruption, trafficking of persons, and kidnapping. However, there remains confusion on the part of some GOP officials and attorneys as to whether money laundering must still be linked to the earlier list of predicate offenses. The law's brevity and lack of implementing regulations are also likely to limit its effectiveness in obtaining convictions. However, reportedly, money laundering is an autonomous offense. There does not have to be a conviction relating to the predicate offense. Rather it must only be established that the predicate offense occurred and that the proceeds of crime from that offense were laundered.

The penalties for money laundering were also revised in 2002. Instead of a life sentence for the crime of laundering money, Law 27.765 sets prison terms of up to 15 years for convicted launderers, with a minimum sentence of 25 years for cases linked to narcotics trafficking, terrorism, and laundering through banks or financial institutions. In addition, revisions to the Penal Code criminalize "willful blindness," the failure to report money laundering conducted through one's financial institution when one has knowledge of the money's illegal source, and imposes a three to six year sentence for failure to file suspicious transaction reports.

Peru's financial intelligence unit, the Unidad de Inteligencia Financiera (UIF) began operations in June 2003 and today has 48 personnel. As Peru's financial intelligence unit, the UIF is the government entity responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs) filed by obligated entities. The entities obligated to report suspicious transactions to the UIF within 30 days include banks, financial institutions, insurance companies, stock funds and brokers, the stock and commodities exchanges, credit and debit card companies, money exchange houses, mail and courier services, travel and tourism agencies, hotels and restaurants, notaries, the customs agency, casinos, auto dealers, construction or real estate firms, notary publics, and dealers in precious stones and metals. The UIF cannot receive STRs electronically; obligated entities must hand-deliver STRs to the UIF. The UIF received 209 STRs in 2004, 796 in 2005 ($442.3 million), and 948 from January through October 2006. The UIF is able to sanction persons and entities for failure to report suspicious transactions, large cash transactions, or the transportation of currency or monetary instruments.

Obligated entities are also required to maintain reports on large cash transactions. Individual cash transactions exceeding $10,000 or transactions totaling $50,000 in one month must be maintained in internal databases for a minimum of five years and made available to the UIF upon request. Non financial institutions, such as exchange houses, casinos, lotteries or others, must report individual transactions over $2,500 or monthly transactions over $10,000. Individuals or entities transporting

more than $10,000 in currency or monetary instruments into or out of Peru must file reports with the customs agency, and the UIF may have access to those reports upon request. These reporting requirements are not being strictly enforced by the responsible GOP entities.

The UIF currently does not receive cash transactions reports (CTRs) or reports on the international transportation of currency or monetary instruments. CTRs are maintained in internal registries within the obligated entities, and reports on the international transportation of currency or monetary instruments are maintained by the customs agency. If the UIF receives an STR and determines that the STR warrants further analysis, it contacts the covered entity that filed the report for additional background information-including any CTRs that may have been filed-and/or the customs agency to determine if the subject of the STR had reported the transportation of currency or monetary instruments. Some requests for reports of transactions over $10,000-such as those that are deposits into savings accounts-are protected under the constitution by bank secrecy provisions and require an order from the Public Ministry or SUNAT, the tax authority. A period of 15-30 days is required to lift the bank secrecy restrictions. All other types of cash transaction reports, however, may be requested directly from the reporting institution. There are two bills under consideration in Congress that would make bank secrecy provisions less stringent and strengthen disclosure requirements.

Law 28.306 mandates that obligated entities also report suspicious transactions related to terrorist financing, and expanded the UIF's functions to include the ability to analyze reports related to terrorist financing. Terrorist financing is criminalized under Executive Order 25.475. On July 25, 2006, the Government issued Supreme Decree 018-2006-JUS to better implement Law 28.306. The decree introduces the specific legal framework for the supervision of terrorism financing.

Supreme Decree 018-2006-JUS further strengthened the UIF by allowing it to participate in the on-site inspections performed by the supervisors of obligated entities. The UIF may also conduct the on-site inspections of the obligated entities that do not fall under the supervision of another regulatory body, such as notaries, money exchange houses, etc. The new regulations also detail the procedures by which compliance officials can obtain a secret code from UIF in order to maintain the secrecy of their identities. Supreme Decree 018-2006-JUS contains instructions for supervisors with prior UIF approval to establish which obligated entities must have a full-time compliance official (depending on each entity's size, patrimony, etc.), and allows supervisors to exclude entities with certain characteristics from maintaining currency transaction reports. If an obligated entity does not have a supervisor, the aforementioned faculties fall to the UIF. The UIF can also request that a supervisor review an obligated entity that is not under its supervision. The supervisors of the obligated entities must update their internal regulations with the provisions enacted by Supreme Decree 018-2006-JUS.

To assist with its analytical functions, the UIF may request information from such government entities as the National Superintendence for Tax Administration, Customs, the Securities and Exchange Commission, the Public Records Office, the Public or Private Risk Information Centers, and the National Identification Registry and Vital Statistics Office, among others. However, the UIF can only share information with other agencies-including foreign entities-if there is a joint investigation underway. Once the UIF has completed the analysis process and determined that a case warrants further investigation or prosecution, the case is sent to the Public Ministry.

As of October 31, 2006, the UIF had sent 47 suspected cases (totaling over $565.5 million) of money laundering stemming from STRs to the Public Ministry for investigation (9 in 2006, totaling $13.9 million).Twenty-one of the 47 cases were linked to drug trafficking, seven involved official corruption, six involved tax fraud, and the remaining 13 had fraud, arms trafficking, contraband, kidnapping, or intellectual property violations as the predicate offenses. The UIF has also participated in 18 joint investigations with the Public Ministry. The Public Ministry has so far presented seven money laundering cases to the judiciary (five stemming from STRs and two from the joint investigations), but there have not yet been any convictions.

Within the counternarcotics section of the Public Ministry, two specialized prosecutors are responsible for dealing with money laundering cases. In addition to being able to request any additional information from the UIF in their investigations, the Public Ministry may also request the assistance of the Directorate of Counter-Narcotics (DINANDRO) of the Peruvian National Police. Under Law 28.306, DINANDRO and the UIF may collaborate on investigations, although each agency must go through the Public Ministry in order to do so. DINANDRO may provide the UIF with intelligence for the cases the UIF is analyzing, while it provides the Public Ministry with assistance on cases that have been sent to the Public Ministry by the UIF.

The UIF was given regulatory responsibilities in July 2004 under Law 28.306. Most covered entities fall under the supervision of the Superintendence of Banks and Insurance (banks, the insurance sector, financial institutions), the Peruvian Securities and Exchange Commission (securities, bonds), and the Ministry of Tourism (casinos). All entities that are not supervised by these three regulatory bodies, such as auto dealers, construction and real estate firms, etc., fall under the supervision of the UIF. However, some covered entities remain unsupervised. For instance, the Superintendence of Banks only regulates money remittances that are done through special fund-transfer businesses (ETFs) that do more than 680,000 soles (about $200,000) in transfers per year, and remittances conducted through postal or courier services are supervised by the Ministry of Transportation and Communications. Informal remittance businesses are not supervised. There is also difficulty in regulating casinos, as roughly 60 percent of that sector is informal. An assessment of the gaming industry conducted by GOP and U.S. officials in 2004 identified alarming deficiencies in oversight and described an industry that is vulnerable to being used to launder large volumes of cash. Approximately 580 slot houses operate in Peru, with less than 65 percent or so paying taxes. Estimates indicate that less than 42 percent of the actual income earned is being reported. This billion-dollar cash industry continues to operate with little supervision.

Peru currently lacks comprehensive and effective asset forfeiture legislation. The Financial Investigative Office of DINANDRO has seized numerous properties over the last several years, but few were turned over to the police to support counternarcotics efforts. While Peruvian law does provide for asset forfeiture in money laundering cases, and these funds can be used in part to finance the UIF, no clear mechanism exists to distribute seized assets among government agencies. A bill to amend the asset forfeiture regime is being considered by Congress.

Terrorism is considered a problem in Peru, which is home to the terrorist organization Shining Path. Although the Shining Path has been designated by the United States as a foreign terrorist organization pursuant to Section 219 of the Immigration and Nationality Act and under Executive Order (E.O.) 13224, and the United States and 100 other countries have issued freezing orders against its assets, the GOP has no legal authority to quickly and administratively seize or freeze terrorist assets. In the event that such assets are identified, the Superintendent for Banks must petition a judge to seize or freeze them and a final judicial decision is then needed to dispose of or use such assets. Peru also has not yet taken any actions to thwart the misuse of charitable or nonprofit entities that can be used as conduits for the financing of terrorism.

Foreign Ministry Officials are working with other GOP agencies to complete the necessary legal revisions that will permit asset-freezing actions. The Office of the Superintendent of Banks routinely circulates to all financial institutions in Peru updated lists of individuals and entities that have been included on the UNSCR 1267 Sanctions Committee's consolidated list as being linked to Usama Bin Laden, the Taliban, and al-Qaida, as well as those on the list of Specially Designated Global Terrorist Entities designated by the United States pursuant to E.O. 13224 on terrorist financing. To date, no assets connected to designated individuals or entities have been identified, frozen, or seized.

Peru is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the Inter-American Convention on Terrorism. However, terrorism has not yet been specifically

and correctly established as a crime under Peruvian legislation as mandated by the UN Convention. The only reference to terrorism as a crime is in Executive Order 25.475, which establishes the punishment of any form of collaboration with terrorism, including economic collaboration. There are several bills pending in the Peruvian Congress concerning the correct definition of the crime of terrorist financing. Peru is also a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. The GOP participates in the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Money Laundering Experts Working Group. Peru is also a member of the South American Financial Action Task Force (GAFISUD) and the Egmont Group of financial intelligence units. Although an extradition treaty between the U.S. Government and the GOP entered into force in 2003, there is no mutual legal assistance treaty or agreement between the two countries.

The Government of Peru has made advances in strengthening its anti-money laundering regime in recent years. However, some progress is still required. There are still a number of weaknesses in Peru's anti-money laundering system: bank secrecy must be lifted in order for the Unidad de Inteligencia Financiera to have access to certain cash transaction reports, smaller financial institutions are not regulated, and the UIF is not able to work directly with law enforcement agencies; rather, the Public Ministry must coordinate any collaboration between the UIF and the other agency. There are a number of bills under review in the Peruvian Congress that would lift bank secrecy provisions for the UIF in matters pertaining to money laundering and terrorist financing. Although there is an Executive Order criminalizing terrorist financing, Peru should also pass legislation establishing this particular crime. The Congress is also considering bills regarding the obligation of nongovernmental organizations to report the origins of their funds. Anticorruption efforts in Peru should be a priority, and Peru should also enact legislation that allows for administrative as well as judicial blocking of terrorist assets. These issues should be addressed in order to strengthen Peru's ability to combat money laundering and terrorist financing.

## Philippines

The Philippines is a regional financial center. In the past few years, the illegal drug trade in the Philippines reportedly has evolved into a billion-dollar industry. The Philippines continues to experience an increase in foreign organized criminal activity from China, Hong Kong, and Taiwan. Reportedly, insurgency groups operating in the Philippines fund their activities, in part, through the trafficking of narcotics and arms, as well as engaging in money laundering through alleged ties to organized crime. The proceeds of corrupt activities by government officials are also a source of laundered funds. Most of the chemicals used in narcotics production in the Philippines are purchased using letters of credit. U.S. dollars are the preferred currency for international narcotics transactions. Drugs circulated within the Philippines are usually exchanged for local currency. Remittances and cash smuggling are also sources of money laundering.

In June 2000, the Financial Action Task Force (FATF) placed the Philippines on its list of Non-Cooperative Countries and Territories (NCCT) for lacking basic anti-money laundering regulations, including customer identification and record keeping requirements, and excessive bank secrecy provisions.

The Government of the Republic of the Philippines (GORP) initially established an anti-money laundering regime by passing the Anti-Money Laundering Act of 2001 (AMLA). The GORP enacted Implementing Rules and Regulations (IRR) for the AMLA in April 2002. The AMLA criminalized money laundering, an offense defined to include the conduct of activity involving the proceeds from unlawful activity in any one of 14 major categories of crimes, and imposes penalties that include a term of imprisonment of up to 14 years and a fine no less than 3,000,000 pesos (approximately $60,000); but no more than twice the value or property involved in the offense. The Act also imposed

identification, record keeping, and reporting requirements on banks, trusts, and other institutions regulated by the Central Bank, insurance companies, securities dealers, foreign exchange dealers, and money remitters, as well as any other entity dealing in valuable objects or cash substitutes regulated by the Securities and Exchange Commission (SEC).

However, the FATF deemed the original legislation inadequate and pressured the Philippines to amend the legislation to be more in line with international standards. The GORP enacted amendments to the Anti-Money Laundering Act of 2001 in March 2003. The amendments to the AMLA lowered the threshold amount for covered transactions (cash or other equivalent monetary instrument) from 4,000,000 pesos to 500,000 pesos ($80,000 to $10,000) within one banking day; expanded financial institution reporting requirements to include the reporting of suspicious transactions, regardless of amount; authorized the Central Bank (Bangko Sentral ng Pilipinas or BSP) to examine any particular deposit or investment with any bank or nonbank institution in the course of a periodic or special examination (in accordance with the rules of examination of the BSP); ensured institutional compliance with the Anti-Money Laundering Act; and deleted the prohibitions against the Anti-Money Laundering Council's examining particular deposits or investments opened or created before the Act.

The FATF deemed those amendments to have sufficiently addressed the main legal deficiencies in the original Philippines anti-money laundering regime, and decided not to recommend the application of countermeasures. The FATF removed the Philippines from its Non-Cooperating Countries and Territories (NCCT) List in February 2005.

The AMLA established the Anti-Money Laundering Council (AMLC) as the country's financial intelligence unit (FIU). The Council is composed of the Governor of the Central Bank, the Commissioner of the Insurance Commission, and the Chairman of the Securities and Exchange Commission. By law, the AMLC Secretariat is an independent agency responsible for receiving, maintaining, analyzing, evaluating covered and suspicious transactions and investigating reports for possible criminal activity. It provides advice and assistance to relevant authorities and issues relevant publications. The AMLC completed the first phase of its information technology upgrades in 2004. This allowed AMLC to electronically receive, store, and search CTRs filed by regulated institutions. Through 2006, the AMLC had received more than 6200 suspicious transaction reports (STRs) involving 13,474 suspicious transactions, and had received over 72 million covered transaction reports (CTRs). AMLC recently acquired software to implement link analysis and visualization to enhance its ability to produce information in graphic form from the CTRs and STRs filed electronically by regulated institutions.

AMLC's role goes well beyond traditional FIU responsibilities and includes the investigation and prosecution of money laundering cases. AMLC has the ability to seize terrorist assets involved in money laundering on behalf of the Republic of the Philippines after a money laundering offense has been proven beyond a reasonable doubt. In order to freeze assets allegedly connected to money laundering, the AMLC must establish probable cause that the funds relate to an offense enumerated in the Act, such as terrorism. The Court of Appeals then may freeze the bank account for 20 days. The AMLC may apply to extend a freeze order prior to its expiration. The AMLC is required to obtain a court order to examine bank records for activities not listed in the Act, except for certain serious offenses such as kidnapping for ransom, drugs, and terrorism-related crimes. The AMLC and the courts are working to shorten the time needed so funds are not withdrawn before the freeze order is obtained.

The Philippines has no comprehensive legislation pertaining to civil and criminal forfeiture. Various government authorities, including the Bureau of Customs and the Philippine National Police, have the ability to temporarily seize property obtained in connection with criminal activity. Money and property must be included in the indictment, however, to permit forfeiture. Because ownership is

difficult to determine in these cases, assets are rarely included in the indictment and are rarely forfeited. The AMLA gives the AMLC the authority to seize assets involved in money laundering operations that may end up as forfeited property after conviction, even if it is a legitimate business. In December 2005, the Supreme Court issued a new criminal procedure rule covering civil forfeiture, asset preservation, and freeze orders. The new rule provides a way to preserve assets prior to any forfeiture action and lists the procedures to follow during the action. The rule also contains clear direction to the AMLC and the court of appeals on the issuance of freeze orders for assets under investigation that had been confused by changes in the amendment to the AMLA in 2003. There are currently 90 prosecutions underway in the Philippine court system that involved AMLC investigations or prosecutions, including 33 for money laundering, 22 for civil forfeiture, and the rest pertaining to freeze orders and bank inquiries. Although some of these cases may conclude shortly, the Philippines had its first conviction for a money laundering offense in early 2006.

Under the AMLA and the bank secrecy act, officers, employees, representatives, agents, consultants, and associates of financial institutions are exempt from civil or criminal prosecution for reporting covered transactions. These institutions must maintain and store records of transactions for a period of five years, extending beyond the date of account or bank closure. The AMLC has frozen funds at the request of the UN Security Council, the United States and other foreign governments. Through November 2006, the AMLC has frozen funds in excess of 500 million Philippine pesos (approximately $10,000,000).

Questions remain regarding the covered institutions fully complying with the Philippine anti-money laundering regime. For example, the BSP does not have a mechanism in place to ensure that the financial community is adhering to the reporting requirements. Banks in more distant parts of the country, especially Mindinao where terrorist groups operate more freely, may feel threatened and inhibited from providing information about financial transactions requested by AMLC. While bank secrecy provisions to the BSP's supervisory functions were lifted in Section 11 of the AMLA, implementation still appears to be incomplete. Due to the Philippines' "privacy issues," examiners of the BSP are not allowed to review documents held by covered institutions in order to determine if the covered institutions are complying with the reporting requirement. BSP examiners are only allowed to ask AMLC, as a result of their examination, if a STR has been filed. If AMLC determines one was not filed, then the AMLC has the responsibility to make inquiries of the covered institution. This process is slow and cumbersome; AMLC is working with the BSP to find ways of streamlining the process.

The AMLC continues to work to bring the numerous foreign exchange offices in the country under its purview. The Monetary Board issued a decision in February 2005 defining the 15,000 exchange houses as financial institutions and instituting a new licensing system to bring them under the provisions of the AMLA. This requirement reduced the number of foreign exchange dealers dramatically as many offices chose to close down rather than seek licensing. The remaining exchange dealers around the country have participated in more than 1500 training programs sponsored by the AMLC. There are still several sectors operating outside of AMLC control, under the revised AMLA. Although the revised AMLA specifically covers exchange houses, insurance companies, and casinos, it does not cover stockbrokers or accountants. Although covered transactions for which AMLC solicits reports include asset transfers, the law does not require direct oversight of car dealers and sales of construction equipment, which are emerging as creative ways to launder money and avoid the reporting requirement.

In 2006, the AMLC requested the chain of casinos operated by the state-owned Philippine Amusement and Gaming Corporation (PAGCOR) to submit covered and suspicious transaction reports, but it has not yet done so. There is increasing recognition that the 15 casinos nationwide offer abundant opportunity for money laundering, especially with many of these casinos catering to international clientele arriving on charter flights from around Asia. Several of these gambling facilities are located near small provincial international airports that may have less rigid enforcement procedures and

standards for cash smuggling. PAGCOR is the sole franchisee in the country for all games of chance, including lotteries conducted through cell phones. At present, there are no offshore casinos in the Philippines, though the country is a growing location for internet gaming sites that target overseas audiences in the region.

The Philippines has over 5,000 nongovernmental organizations (NGOs) that do not fall under the requirements of the AMLA. Charitable and nonprofit entities are not required to make covered or suspicious transaction reports. The SEC provides limited regulatory control over the registration and operation of NGOs. These entities are rarely held accountable for failure to provide year-end reports of their activities, and there is no consistent accounting and verification of their financial records. Because of their ability to circumvent the usual documentation and reporting requirements imposed on banks for financial transfers, NGOs could be used as conduits for terrorist financing without detection. The AMLC is aware of the problem and is working to bring charitable and not-for-profit entities under the interpretation of the amended implementing regulations for covered institutions.

There are seven offshore banking units (OBUs) established since 1976. At present, OBUs account for less than two percent of total banking system assets in the country. The Bangko Sentral ng Pilipinas (BSP) regulates onshore banking, exercises regulatory supervision over OBUs, and requires them to meet reporting provisions and other banking rules and regulations. In addition to registering with the SEC, financial institutions must obtain a secondary license from the BSP subject to relatively stringent standards that would make it difficult to establish shell companies in financial services of this nature. For example, a financial institution operating an OBU must be physically present in the Philippines. Anonymous directors and trustees are not allowed. The SEC does not permit the issuance of bearer shares for banks and other companies.

Despite the efforts of the GORP authorities to publicize regulations and enforce penalties, cash smuggling remains a major concern for the Philippines. Although there is no limit on the amount of foreign currency an individual or entity can bring into or take out of the country, any amount in excess of $10,000 equivalent must be declared upon arrival or departure. Based on the amount of foreign currency exchanged and expended, there is systematic abuse of the currency declaration requirements and a large amount of unreported cash entering the Philippines.

The problem of cash smuggling is exacerbated by the large volume of foreign currency remitted to the Philippines by Overseas Filipino Workers (OFWs). The amount of remitted funds grew by 15 percent during the first ten months of 2006, and should exceed $12 billion for the year, equal to 10 percent of GDP. The BSP estimates that an additional $2-3 billion is remitted outside the formal banking system. Most of these funds are brought in person by OFWs or by designated individuals on their return home and not through any alternative remittance system. Since most of these funds enter the country in smaller quantities than $10,000, there is no declaration requirement and the amounts are difficult to calculate. The GORP encourages local banks to set up offices in remitting countries and facilitate fund remittances, especially in the United States, to help reduce the expense of remitting funds.

The Philippines is a member of the Asia/Pacific Group on Money Laundering (APG) and hosted the 9th annual APG plenary in July, 2006. The Philippines FIU became the 101st member of the Egmont Group of FIUs in July 2005. The GORP is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime and to all 12 international conventions and protocols related to terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism). The Anti-Money Laundering Council must obtain a court order to freeze assets of terrorists and terrorist organizations placed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, and other foreign governments.

For several years, the GORP has realized the need to enact and implement an antiterrorism law that among other things would define and criminalize terrorism and terrorist financing, and give military

and law enforcement entities greater tools to detect and interdict terrorist activity. President Arroyo declared in her State of the Nation address in June 2005 that the passage of such a law was one of her priorities for the remainder of the year. Although the Philippine House passed its version of the Anti-Terrorism Law in April 2006, the Senate version remains stalled due to political infighting and fear the government could use certain provisions against political opponents.

In lieu of specific counterterrorist legislation, the government has broadly criminalized terrorist financing through Republic Law legislation, which defines "hijacking and other violations under Republic Act No. 6235; destructive arson and murder, as defined under the Revised Penal Code, as amended, included those perpetrated by terrorists against noncombatant persons and similar targets" as one of the violations under the definition of unlawful acts. The Revised Implementing Rules and Regulations R.A. No. 9160, as amended by R.A. No.9194, further state that any proceeds derived or realized from an unlawful activity includes all material and monetary effects will be deemed a violation against the law.

The Government of the Republic of the Philippines has made significant progress enhancing and implementing its amended anti-money laundering regime. To fully comport with international standards and become a more effective partner in the global effort to staunch money laundering and thwart terrorism and its financing, it should enact and implement new legislation that criminalizes terrorism and terrorist financing . Additionally, the Central Bank should be empowered to levy administrative penalties against covered entities in the financial community that do not comply with reporting requirements. Stockbrokers and accountants should be required to report CTRS and STRs and AMLC should use its authority to require all casinos to file CTRs and STRs. The GORP should enact comprehensive legislation regarding freezing and forfeiture of assets that would empower AMLC to issue administrative freezing orders to avoid funds being withdrawn before a court order is issued. The creation of an asset forfeiture fund would enable law enforcement agencies to draw on the fund to augment their budgets for investigative purposes. Such a fund would benefit the AMLC and enable it to purchase needed equipment. Finally, AMLC should separate its analytical and investigative responsibilities and establish a separate investigative division that would focus its attention on dismantling money laundering and terrorist financing operations.

## Poland

Poland's geographic location places it directly along one of the main routes between the former Soviet Union republics and Western Europe that is used by narcotics traffickers and organized crime groups. According to Polish Government estimates, narcotics trafficking, organized crime activity, auto theft, smuggling, extortion, counterfeiting, burglary, and other crimes generate criminal proceeds in the range of $2-3 billion each year. The Government of Poland (GOP) estimates that the unregistered or gray economy, used primarily for tax evasion, may be as high as 13 percent of Poland's $330 billion GDP; it believes the black economy is only one percent of GDP. Poland's entry into the European Union (EU) in May 2004 increased its ability to control its eastern borders, thereby allowing Poland to become more effective in its efforts to combat all types of crime, including narcotics trafficking and organized crime.

Poland's banks serve as transit points for the transfer of criminal proceeds. As of March 2006, 54 commercial banks were licensed for operation in Poland, as were 585 "cooperative banks" that primarily serve the rural and agricultural community. The GOP considers the nation's banks, insurance companies, brokerage houses, and casinos to be important venues of money laundering. According to the GOP, fuel smuggling, by which local companies and organized crime groups seek to avoid excise taxes by forging gasoline delivery documents, is a major source of proceeds to be laundered. Money laundering through trade in scrap metal and recyclable material is also a newly

emerging trend. It is also believed that some money laundering in Poland originates in Russia or other countries of the former Soviet Union.

The genesis of Poland's anti-money laundering (AML) regime was November 1, 1992, when the President of the National Bank of Poland issued an order instructing banks how to deal with money entering the financial system through illegal sources. The August 29, 1997 Banking Act was followed by a 1998 Resolution of the Banking Supervisory Commission, adding customer identification requirements and instructions on registering transactions exceeding a certain threshold.

On November 16, 2000, a law went into effect that improves Poland's ability to combat money laundering (entitled the Act of 16 November, or the Act on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources and on Counteracting the Financing of Terrorism, as amended). The GOP has updated this law several times to bring it into conformity with EU standards and to improve its operational effectiveness. This law increases penalties for money laundering and contains safe harbor provisions that exempt financial institution employees from normal restrictions on the disclosure of confidential banking information. The law also provides for the creation of a financial intelligence unit (FIU), the General Inspectorate of Financial Information (GIIF), housed within the Ministry of Finance, to collect and analyze large cash and suspicious transactions. Poland has adopted a National Security Strategy that treats the anti-money laundering effort as a top priority. The GOP has worked diligently to bring its laws into full conformity with EU obligations.

The Criminal Code criminalizes money laundering. Article 299 of the Criminal Code addresses self-laundering and criminalizes tipping off. In June 2001, the Parliament passed amendments to the Act of 16 November that broadened the definition of money laundering to encompass all serious crimes. In March 2003, Parliament further amended the law to broaden the definition of money laundering to include assets originating from illegal or undisclosed sources.

A major weakness of Poland's initial money laundering regime was that it did not cover many nonbank financial institutions that had traditionally been used for money laundering. To remedy this situation, between 2002 and 2004, the Parliament passed several amendments to the 2000 money laundering law. The amendments expand the scope of institutions subject to identity verification, record keeping, and suspicious transaction reporting requirements. Financial institutions subject to the reporting requirements prior to March 2004 amendments included banks, the National Depository for Securities, post offices, auction houses, antique shops, brokerages, casinos, insurance companies, investment and pension funds, leasing firms, private currency exchange offices, real estate agencies, and notaries public. The March 2004 amendments to the money laundering law widen the scope of covered institutions to include lawyers, legal counselors, auditors, and charities, as well as the National Bank of Poland in its functions of selling numismatic items, purchasing gold, and exchanging damaged banknotes. The law also requires casinos to report the purchase of chips worth 1,000 euros (approximately $1,200) or more. The law's extension to the legal profession was not without controversy. Lawyers strongly opposed the new amendments, claiming that the law violates attorney-client confidentiality privileges, and the Polish Bar has mounted a challenge to some provisions, and submitted a motion to the Constitutional Tribunal to determine the consistency of certain regulations with ten articles in the Polish Constitution.

In 2002, Parliament adopted measures to bring the nation's anti-money laundering legislation into compliance with EU standards. Poland's customs law was amended in order to require the reporting of any cross-border movement of more than 10,000 euros (approximately $12,000) in currency or financial instruments. Also, in addition to requiring that the GIIF be notified of all financial deals exceeding 15,000 euros (approximately $19,000), covered institutions are also required to file reports of suspicious transactions, regardless of the size of the transaction. Polish law also requires financial

institutions to put internal anti-money laundering procedures into effect, a process that is overseen by the GIIF.

The GIIF began operations on January 1, 2001. During its first three years of operation, the GIIF received 3,326 suspicious transaction reports (STRs) which resulted in the development of 370 cases by the Prosecutor's Office. In 2005 and 2006, the number of STRs received by the FIU continued to increase with a total of 1,558 reports forwarded to the FIU, resulting in the development of 175 cases by the Prosecutor's Office. Between January and October 2006, the GIIF received more than 1,200 STRs, resulting in the creation of 182 cases with violations exceeding $210 million. Banks filed ninety percent of the STRs submitted in 2005. At a minimum, all reports submitted by the GIIF to the Prosecutor's Office have resulted in the instigation of initial investigative proceedings. In 2005, the number of convictions for money laundering exceeded 30, a number of which were connected with fuel smuggling. There were four convictions under the money laundering law in 2004. Many of the investigations begun by the GIIF have resulted in convictions for other nonfinancial offenses. The GIIF receives approximately 1.8 million reports per month on transactions exceeding the threshold level.

The vast majority of required notifications to the GIIF are sent through a newly developed electronic reporting system. The system is very well developed and is considered to be one of Europe's finest electronic reporting systems, collecting more information than the paper version of the report. Only a small percentage of notifications are now submitted by paper, mainly from small institutions that lack the equipment to use the electronic system. Although the new system is an important advance for Poland's anti-money laundering program, the efficient processing and analyzing of the large number of reports that are sent to the GIIF continues to be a challenge for the understaffed FIU. To help improve the FIU's efficiency in handling the large volume of reports filed by obliged institutions, the GIIF has initiated work on a specialized IT program that will support complex data analysis and improve the FIU's efficiency in handling the increasing number of reports which it receives.

The GIIF also conducts on-site training and compliance monitoring investigations. In 2005, the GIIF carried out 25 compliance investigations, an increase over the 15 completed in 2004, and received several hundred follow-up reports from institutions responsible for routinely supervising covered institutions. The GIIF has also introduced a new electronic learning course designed to familiarize obliged institutions with Poland's anti-money laundering regulations. In March 2005, an updated version of the course was installed on the Ministry of Finance Website. In 2005, 3,443 individuals (mainly from obligated institutions) participated in the GIIF's new electronic learning course, with a total of 3,032 individuals passing the final test. The Polish Code of Criminal Procedure, Article 237, allows for certain Special Investigative Measures. However, money laundering investigations are not specifically covered, although the organized crime provisions might apply in some cases. Two main police units deal with the detection and prevention of money laundering: the General Investigative Bureau and the Unit for Combating Financial Crime. Overall, both police units cooperate well with the GIIF. The Internal Security Agency (ABW) may also investigate the most serious money laundering cases.

A recognized need exists for an improved level of coordination and information exchange between the GIIF and law enforcement entities, especially with regard to the suspicious transaction information that the GIIF forwards to the National Prosecutor's Office. To alleviate this problem the GIIF and the National Prosecutor's Office signed a cooperation agreement in 2004. The agreement calls for the creation of a computer-based system that would facilitate information exchange between the two institutions. Work on the development of this new system is currently underway. With regard to information exchange with its foreign counterparts, the GIIF remains active. In 2005, it sent official requests to foreign financial intelligence units on 155 cases concerning 284 national and foreign entities suspected of money laundering, while foreign FIUs sent 59 requests to the GIIF, concerning 164 national and foreign entities suspected of attempting to launder proceeds from crime. The most

intensive exchange of information was conducted with the United States: In 2005 GIIF submitted 31 requests to the financial intelligence of the United States. The GIIF also actively exchanges with the German, Russian, British, and Ukrainian financial intelligence units.

The total number of suspected transactions sent by obliged institutions in 2005 was approximately 70,000. The GIIF is authorized to put a suspicious transaction on hold for 48 hours. The Public Prosecutor then has the right to suspend the transaction for an additional three months, pending a court decision. In 2004, Article 45 of the criminal code was amended to further improve the government's ability to seize assets. On the basis of the amended article, an alleged perpetrator must prove that his assets have a legal source; otherwise, the assets are presumed to be related to the crime and as such can be seized. Both the Ministry of Justice and the GIIF desire to see more aggressive asset forfeiture regulations. However, because the former communist regime employed harsh asset forfeiture techniques against political opponents, lingering political sensitivities make it difficult to approve stringent asset seizure laws. In 2005, the GIIF suspended five transactions worth $500,000 and blocked 34 accounts worth $ 11 million. In 2006, the GIIF suspended four transactions worth $2.3 million and blocked 85 accounts worth $12.36 million.

The GOP has created an office of counterterrorist operations within the National Police, which coordinates and supervises regional counterterrorism units and trains local police in counterterrorism measures. Poland also has created a terrorist watch list of entities suspected of involvement in terrorist financing. The list contains the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the names of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224, and the names designated by the EU under its relevant authorities. All covered institutions are required to verify that their customers are not included on the watch list. In the event that a covered institution discovers a possible terrorist link, the GIIF has the right to suspend suspicious transactions and accounts. Despite these efforts, Poland has not yet criminalized terrorist financing as is required by UNSCR 1373, arguing that all possible terrorist activities are already illegal and serve as predicate offenses for money laundering and terrorist financing investigations. The Ministry of Justice continues to work on draft amendments to the criminal code that would criminalize terrorist financing as well as elements of all terrorism-related activity.

As a member of the Council of Europe, Poland participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). In 2006, MONEYVAL conducted its third round mutual evaluation of Poland. The GIIF is an active participant in the Egmont Group and in FIU.NET, the EU-sponsored information exchange network for FIUs. All information exchanged between the GIIF and its counterparts in other EU states takes place via FIU.NET. In 2005, Poland twice hosted law enforcement, FIU and financial sector supervisors from the Former Yugoslav Republic of Macedonia on study visits designed to increase the operational capacities of the agencies and the people staffing them.

A Mutual Legal Assistance Treaty between the United States and Poland came into force in 1999. In addition, Poland has signed bilateral mutual legal assistance treaties with Sweden, Finland, Ukraine, Lithuania, Latvia, Estonia, Germany, Greece, and Hungary. Polish law requires the GIIF to have memoranda of understanding (MOUs) with other international competent authorities before it can participate in information exchanges. The GIIF has been diligent in executing MOUs with its counterparts in other countries, signing a total of 33 MOUs between 2002 and 2005. The MOU between the Polish FIU and the U.S. FIU was signed in fall 2003. The FIU is also currently in the process of negotiating MOUs with FIUs in Canada, Argentina, Turkey, Serbia and Montenegro, Belarus, China and Taiwan. Because Poland is an EU member state, the exchange of information between the GIIF and the FIUs of other member states is regulated by the EU Council Decision of October 17, 2000.

Poland is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the European Convention on Extradition and its Protocols, the European Convention on Mutual Assistance in Criminal Matters, and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Poland is also a party to the UN Convention against Transnational Organized Crime, which was, in part, a Polish initiative.

Over the past several years, the Government of Poland has worked to implement a comprehensive anti-money laundering regime that meets international standards. Further improvements should be made by promoting additional training at the private sector level and by working to improve communication and coordination between the General Inspectorate of Financial Information and relevant law enforcement agencies. The Code of Criminal Procedure should also be amended to allow the use of Special Investigative Measures in money laundering investigations, which would help law enforcement attain a better record of prosecutions and convictions. Poland should also act on the draft amendments to the criminal code and specifically criminalize terrorist financing, as it is obligated to do as a party to the UN International Convention for the Suppression of the Financing of Terrorism.

## Portugal

Portugal is an entry point for narcotics transiting into Europe, and officials of the Government of Portugal (GOP) indicate that most of the money laundered in Portugal is narcotics-related. The GOP also reports that currency exchanges, wire transfers, and real estate purchases are used for laundering criminal proceeds.

Portugal has a comprehensive anti-money laundering regime that criminalizes the laundering of proceeds of serious offenses, including terrorism, arms trafficking, kidnapping, and corruption. Financial and nonfinancial institutions have a mandatory requirement to report all suspicious transactions to the Public Prosecutor regardless of threshold amount. The October 2006 Financial Action Task Force (FATF) Mutual Evaluation of Portugal stated, “the Portuguese legal framework for combating money laundering and terrorist financing is generally comprehensive.” The report notes that the Portuguese confiscation and seizure system is also “generally comprehensive.”

Act 11/2004, which implements the European Union’s Second Money Laundering Directive, broadened the GOP’s anti-money laundering regime. Act 11/2004 mandates suspicious transaction reporting by credit institutions, investment companies, life insurance companies, traders in high-value goods (e.g., precious stones, aircraft), and numerous other entities. Portugal employs an all-crimes approach to the predicate offense. “Tipping off” is prohibited and liability protection is provided for regulated entities making disclosures in good faith. Despite Law 5/2002, Article 2, which waives banking secrecy in cases related to organized crime and financial crime, in practice banking secrecy laws made it extremely difficult for investigators to obtain information about bank accounts and financial transactions of individuals or companies without their permission until 2004.

If a regulated entity has knowledge of a transaction likely to be related to a money laundering offense, it must inform the GOP, which may order the entity not to complete the transaction. If stopping the transaction is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, the government also may allow the entity to proceed with the transaction but require the entity to provide it with complete details.

All financial institutions must identify their customers, maintain records for a minimum of ten years, and demand written proof from customers regarding the origins and beneficiaries of transactions that exceed 12,500 euros (approximately $16,533). Nonfinancial institutions, such as casinos, property dealers, lotteries and dealers in high-value assets, must also identify customers engaging in large transactions, maintain records, and report suspicious activities to the Office of the Public Prosecutor.

However, the 2006 FATF mutual evaluation team reported that the mechanism for determining the beneficial owner does not fully comply with FATF requirements. The National Registry of Legal Persons does not include all information to reveal the beneficial owners of legal persons. Requirements for obliged entities to identify beneficial owners are located in instructions and regulatory standards set forth by the Bank of Portugal (BdP) and the Portuguese Insurance Institute (ISP), and not stipulated by law as required by the Methodology; this raises the question of whether these regulations could be considered secondary legislation or other enforceable means. For some entities in the securities sector subject to the Securities Market Commission (CMVM) regulations rather than those from the BdP, the CMVM regulations do not explicitly comply with requirements regarding the identification of the beneficial owners of legal persons.

Decree-Law 295/2003 of November 2003 sets out reporting requirements for the transportation across borders of cash, nonmanufactured gold, and certain negotiable financial instruments, such as travelers' checks. When a person travels across the Portuguese border with more than 12,500 euros worth of such assets, a declaration must be made to Portuguese customs officials. The GOP expects to approve by year's end national legislation per EC Regulation 1899/2005 to more tightly control the movement of cash across borders.

The November 2003 law also revised and tightened the legal framework for foreign currency exchange transactions, including gold, subjecting them to the reporting requirement for transactions exceeding 12,500 euros. Beyond the requirements to report large transactions, foreign exchange bureaus are not subject to any special requirements to report suspicious transactions. The law does, however, give the GOP the authority to investigate suspicious transactions without notifying targets of the investigation.

New rules that took effect in January 2005 permit tax authorities to lift secrecy rules without authorization from the target of an investigation. The rules require companies to have at least one bank account and, for companies with more than 20 employees, to conduct their business through bank transfers, checks, and direct debits rather than cash. These rules are mainly designed to help the GOP investigate possible cases of tax evasion but may facilitate enforcement of other financial crimes as well.

With regard to nonbanking financial institutions, namely financial intermediaries, the Portuguese Securities Market Commission issued Regulation 7/2005 (amending Regulation 12/2000 on Financial Intermediation), requiring financial intermediaries to submit detailed annual Control and Supervision Reports to the Commission by June 30 of the following year. The regulation entered into force on January 1, 2006. Regulation 2/2006 entered into force on May 26, 2006, further amending Regulation 12/2000, Articles 36 and 36-A (concerning internal auditing and supervision), to require additional information.

The three principal regulatory agencies for supervision of the financial sector in Portugal are the Central Bank of Portugal, the Portuguese Insurance Institute, and the Portuguese Securities Market Commission. The Gambling Inspectorate General, the Economic Activities Inspectorate General, the Registries and Notaries General Directorate, the National Association for Certified Public Accountants and the Association for Assistant Accountants, the Bar Association, and the Chamber of Solicitors also monitor and enforce the reporting requirements of regulated entities, which include casinos, realtors, dealers in precious metals and stones, accountants, notaries, statutory auditors and registry officials. Attorneys and solicitadores became obliged entities in 2004.

Portugal's financial intelligence unit (FIU), known as the Financial Information Unit, or Unidade de Informação Financeira (UIF), was established through Decree-Law 304/2002 of December 13, 2002, and operates independently as a department of the Portuguese Judicial Police (Polícia Judiciária). The UIF is comprised of 28 persons and is responsible for gathering, centralizing, processing, and publishing information pertaining to investigations of money laundering and tax crimes. It also

facilitates cooperation and coordination with other judicial and supervising authorities. All suspicious transaction reports (STR's) received by the UIF come from the Attorney General's office, as that office is the designated competent authority to receive STRs. At the international level, UIF coordinates with other FIUs. The UIF has policing duties but no regulatory authority.

In 2002, obligated entities filed 166 STRs. In 2005, they had filed 330 STRs and 44,165 currency transaction reports (CTRs). From January to September 2006, UIF received 391 STRs and 13,806 CTRs. Credit institutions and the Central Bank were the source of the vast majority of STRs, with the former submitting 346 and the latter 25. Portugal's Gambling Inspectorate General was the source of 12,599 CTRs, as it reports all transactions at casinos above a certain threshold. In this same time period, UIF sent 203 cases for further investigation to the Judicial Police and other police departments. Most of the case information originated from financial institutions and the Central Bank. Twelve cases resulted in proposals to freeze assets involving over 17 million euro (approximately $22.5 million).

The FATF mutual evaluation report noted that sixteen persons were found guilty and convicted of money laundering from 2002 to 2005, receiving penalties ranging from one year to eight and one-half years' imprisonment. The GOP has not yet released statistics on arrests or prosecutions for money laundering or terrorist financing in 2006. However, the media reported in November that the Judicial Police detained seven individuals suspected of belonging to a money laundering network in 2006. Portuguese authorities believe these individuals were involved in the transfer of funds generated by illegal activities in Mozambique, Angola, and Dubai.

Portuguese laws provide for the confiscation of property and assets connected to money laundering and authorize the Judicial Police to trace illicitly obtained assets (including those passing through casinos and lotteries), even if the predicate offense occurs outside of Portugal. Police may request files of individuals under investigation and, with a court order, can obtain and use audio and videotape as evidence in court. The law allows the Public Prosecutor to request that a lien be placed on the assets of individuals being prosecuted in order to facilitate asset seizures related to narcotics and weapons trafficking, terrorism, and money laundering.

Act 5/2002 shifted the burden of proof in cases of criminal asset forfeiture from the government to the defendant; an individual must prove that his assets were not obtained as a result of his illegal activities. The law defines criminal assets as those owned by an individual at the time of indictment and thereafter. The law also presumes that assets transferred by an individual to a third party within the previous five years still belong to the individual in question, unless proven otherwise. Portugal has comprehensive legal procedures that enable it to cooperate with foreign jurisdictions and share seized assets.

In August 2003, Portugal passed Act 52/2003, which specifically defines terrorist acts and organizations and criminalizes the transfer of funds related to the commission of terrorist acts. It also addresses the criminal liability of legal persons regarding terrorism financing. However, the legislation does not extend the customer due diligence practices to risk association with terrorism financing. While the broadly-worded law covers both illicit and licit funds that support a terrorist act or organization, it does not extend coverage to the provision of funds to an individual terrorist. Portugal has created a Terrorist Financing Task Force that includes the Ministries of Finance and Justice, the Judicial Police, the Security and Intelligence Service, the Bank of Portugal, and the Portuguese Insurance Institution. Names of individuals and entities included on the United Nations Security Council Resolution 1267 Committee's consolidated list, or that the United States and EU have linked to terrorism, are passed to private sector entities through the Bank of Portugal, the Stock Exchange Commission, and the Portuguese Insurance Institution. In practice, the actual seizure of assets would only occur once the EU's clearinghouse process agrees to the EU-wide seizure of assets of terrorists and terrorist-linked groups. While Portugal does not have an administrative procedure to freeze assets independently of the relevant EU directive, judicial procedure exists for the Public Prosecutor to open

a special inquiry and to freeze assets at the request of a foreign country. To date, no significant assets have been identified or seized. In its 2006 report on the mutual evaluation of Portugal, the FATF noted that it found "deficiencies in scope and time" as related to the freezing of terrorism-related funds.

The Portuguese Madeira Islands International Business Center (MIBC) has a free trade zone, an international shipping register, offshore banking, trusts, holding companies, stock corporations, and private limited companies. The latter two business groups, similar to international business corporations, account for approximately 6,500 companies registered in Madeira. All entities established in the MIBC will remain tax exempt until 2011. Twenty-seven offshore banks are currently licensed to operate within the MIBC. The Madeira Development Company supervises offshore banks. There is no indication that MIBC has been used for money laundering or terrorist financing.

Companies can also take advantage of Portugal's double taxation agreements. Decree-Law 10/94 permits existing banks and insurance companies to establish offshore branches. Applications are submitted to the Central Bank of Portugal for notification, in the case of EU institutions, or authorization, in the case of non-EU or new entities. The law allows establishment of "external branches" that conduct operations exclusively with nonresidents or other Madeiran offshore entities, and "international branches" that conduct both offshore and domestic business. Although Madeira has some local autonomy, Portuguese and EU legislative rules regulate its offshore sector, and the competent oversight authorities supervise it. Exchange of information agreements contained in double taxation treaties allow for the disclosure of information relating to narcotics or weapons trafficking. Bearer shares are not permitted.

According to the FATF mutual evaluation report, Portugal has undertaken many mutual legal assistance obligations, especially with regard to identification, seizure and confiscation of assets. Portugal is a member of the Council of Europe, the European Union, and the FATF. The GOP is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism, and has signed, but not yet ratified, the UN Convention against Corruption. Portugal is also a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Portugal's FIU is a member of the Egmont Group.

The Government of Portugal has put into place a comprehensive and effective regime to combat money laundering. Laws passed in 2002 strengthen its ability to investigate and prosecute, and steps taken in 2003 extended the regime's reach to terrorist financing. Legislative measures adopted in 2004 have consolidated the anti-money laundering legal framework, imposing on financial and nonfinancial institutions obligations to prevent the use of the financial system for the purpose of money laundering. The GOP continued to implement these measures in 2006 to effectively combat money laundering and terrorist financing. However, Portugal should collect and maintain more information and data regarding the number of money laundering and terrorism financing investigations, prosecutions and convictions as well as the amount of property and assets frozen, seized and confiscated as it relates to money laundering and terrorism financing. The GOP should work to correct any identified deficiencies regarding its asset freezing and forfeiture regime, improve its mechanisms to determine the beneficial owners, and ensure that the terrorism financing law covers financing to individuals. Lastly, the FIU should be the competent authority to receive and analyze all STRs.

## Qatar

Qatar has a small population (approximately 850,000 residents) with a low rate of general and financial crime. The financial sector, though modern, is limited in size and subject to strict regulation by the Qatar Central Bank (QCB). There are 16 licensed financial banks, including three Islamic banks and a specialized bank, the Qatar Industrial Development Bank. Qatar Financial Centre (QFC) allows

major international financial institutions and corporations to set up offices and operate in a "free zone" environment. The QFC allows full repatriation of profits and 100 percent foreign ownership. Qatar has 19 exchange houses, three investment companies and one commercial finance company. Although Qatar still has a cash-intensive economy, authorities believe that cash placement by money launderers is a negligible risk due to the close-knit nature of the society and the rigorous "know your customer" procedures required by Qatari law.

On September 11, 2002, the Emir of the State of Qatar signed the Anti-Money Laundering Law. According to Article 28, money laundering offenses involve the acquisition, holding, disposing of, managing, keeping, exchanging, depositing, investing, transferring, or converting of funds from illegal proceeds. The law imposes fines and penalties of imprisonment of five to seven years. The law expanded the powers of confiscation to include the identification and freezing of assets as well as the ultimate confiscation of the illegal proceeds upon conviction of the defendant for money laundering. Article Two includes any activities related to terrorist financing. Article 12 authorizes the Central Bank Governor to freeze suspicious accounts for up to ten days and to inform the Attorney General within three days of any action taken. The Attorney General may renew or nullify the freeze order for a period of up to three months.

The law requires all financial institutions to report suspicious transactions and retain records for up to 15 years. The law also gives the QCB greater powers to inspect suspicious bank accounts and grants the authorities the right to confiscate money in illegal transactions. Article 17 permits the State of Qatar to extradite convicted criminals in accordance with international or bilateral treaties.

The Anti-Money Laundering Law established the National Anti-Money Laundering Committee (NAMLC) to oversee and coordinate money laundering combating efforts. It is chaired by the Deputy Governor of the QCB and includes members from the Ministries of Interior, Civil Service Affairs and Housing, Economy and Commerce, Finance, Justice, Customs and Ports Authority and the State Security Bureau.

In February 2004, the Government of Qatar (GOQ) passed the Combating Terrorism Law. According to Article Four of the law, any individual or entity that provides financial or logistical support, or raises money for activities considered terrorist crimes, is subject to punishment. The punishments are listed in Article Two of the law, which include the death penalty, life imprisonment, and 10 or 15 year jail sentences depending on the crime. Qatar has a national committee to review the consolidated UN 1267 terrorist designation lists and to recommend any necessary actions against individuals or entities found in Qatar.

The QCB updates regulations regarding money laundering and financing of terrorism on a regular basis, in accordance with international requirements. The Central Bank aims to increase the awareness of all banks operating in Qatar with respect to anti-money laundering efforts by explaining money laundering schemes and monitoring suspicious activities.

In October, 2004, the GOQ established a Financial Intelligence Unit (FIU) known as the Qatar Financial Information Unit (QFIU). The FIU is responsible for receiving and reviewing all suspicious and financial transaction reports, identifying transactions and financial activities of concern, ensuring that all government ministries and agencies have procedures and standards to ensure proper oversight of financial transactions, and recommending actions to be taken if suspicious transactions or financial activities of concern are identified. The FIU also obtains additional information from the banks and other government ministries. The QCB, Public Prosecutor and the Criminal Investigation Division (CID) of the Ministry of the Interior work together with the FIU to investigate and prosecute money laundering and terrorism finance cases. The FIU also coordinates closely with the Doha Securities Market (DSM) to establish procedures and standards to monitor all financial activities that occur in Qatar's stock market. The FIU coordinates the different regulatory agencies in Qatar. The Qatari FIU became a member of the Egmont Group in 2005.

In December 2004, QCB installed a central reporting system to assist the FIU in monitoring all financial transactions made by banks. All accounts must be opened in person. Banks are required to know their customers; the banking system is considered open in that in addition to Qatari citizens and legal foreign residents, nonresidents can open an account based on a reliable recommendation from his or her primary bank. Hawala transactions are prohibited by law in Qatar.

The Qatar Authority for Charitable Works monitors all charitable activity in and outside of Qatar. The Secretary General of the Authority approves all international fund transfers by the charities. The Authority has primary responsibility for monitoring overseas charitable, development, and humanitarian projects that were previously under the oversight of several government agencies such as the Ministry of Foreign Affairs, the Ministry of Finance and the Ministry of Economy and Commerce. Overseas activities must be undertaken in collaboration with a nongovernmental organization (NGO) that is legally registered in the receiving country. The Authority prepares an annual report on the status of all projects and submits the report to relevant ministries. The Authority also regulates domestic charity collection.

Qatar does not have cross-border reporting requirements for financial transactions. Immigration and customs authorities are reviewing their policies in expanding their ability to enforce money declarations and detect trade-based money laundering.

Qatar is a party to the 1988 UN Drug Convention but not the UN Convention for the Suppression of the Financing of Terrorism or the UN Convention against Transnational Organized Crime. Qatar is one of the original signatories of the memorandum of understanding governing the establishment of the Middle East and North Africa Financial Action Task Force (MENA-FATF), a FATF-style regional body that promotes best practices to combat money laundering and terrorist financing in the region.

The Government of Qatar has demonstrated a willingness to fight financial crimes, including terrorist financing, and to work cooperatively with other countries in doing so. Per FATF Special Recommendation Nine, Qatar should initiate and enforce in-bound and out-bound cross-border currency reporting requirements. The data should be shared with the FIU. The government should continue to work to ensure that law enforcement, prosecutors, and customs authorities receive the necessary training and technical assistance to improve their capabilities in recognizing and pursuing various forms of terrorist financing, money laundering and other financial crimes. Qatar should publish the number of annual money laundering investigations, prosecutions, and convictions. Qatar should become a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

## Romania

Romania's geographic location makes it a natural transit country for trafficking in narcotics, arms, stolen vehicles, and persons. As such, the nation is vulnerable to financial crimes. Romania's central bank, the National Bank of Romania, estimates the dollar amount of financial crimes to range from $1 billion to $1.5 billion per year. Value-added tax (VAT) fraud has fallen to below 10 percent (down from 45 percent in previous years) of this total. Trans-border smuggling of counterfeit goods, fraudulent bankruptcy claims, tax fraud, and fraudulent claims in relation to consumer lending are additional types of financial crimes prevalent in Romania. Romania also has one of the highest occurrences of online credit card fraud in the world.

Laundered money comes primarily from international crime syndicates who conduct their criminal activity in Romania and subsequently launder their illicit proceeds through false limited liability companies. Another source of laundered money is the proceeds of illegally smuggled goods such as cigarettes, alcohol, coffee, and other dutiable commodities. Widespread corruption in Romania's

customs and border control and as well in several neighboring Eastern European countries also facilitates money laundering.

Romania first criminalized money laundering with the adoption in January 1999 of Law No. 21/99, On the Prevention and Punishment of Money Laundering. The law became effective in April 1999 and required customer identification, record keeping, suspicious transaction reporting, and currency transaction reporting for transactions (including wire transfers) over 10,000 euros. The list of entities covered by Law No. 21/99 includes banks, nonbank financial institutions, attorneys, accountants, and notaries. Tipping off has been prohibited. Romanian law permits the disclosure of client and ownership information to bank supervisors and law enforcement authorities, and protects banking officials with respect to their cooperation with law enforcement.

In December 2002, Romania issued modifications to its anti-money laundering law with the passage of the Law on the Prevention and Sanctioning of Money Laundering (Law 656/2002). This law changed the list of predicate offenses to an all crimes approach. The 2002 law also expanded the number and types of entities subject to anti-money laundering (AML) regulations. Some of these new entities include art dealers, travel agents, privatization agents, postal officials, money service businesses, and real estate agents. Even though nonbank financial institutions are covered under Romania's money laundering law, regulatory supervision of this sector is weak and not nearly as rigorous as that imposed on banks.

In July 2005, Romania's money laundering law was further modified by the passage of Law 230/2005. The new law provides for a uniform approach to combating and preventing money laundering and terrorist financing. The purpose of the law is to meet the requirements of EU Directive 2001/97/EC and EU Directive 91/308/EEC on Preventing Use of the Financial System for Money Laundering, as well as the requirements of the European Council's Framework Decision of June 2001 on Identification, Search, Seizure, and Confiscation of the Means and Goods Obtained from Such Offenses. The modified law also responds to Financial Action Task Force (FATF) Recommendations and establishes an STR reporting requirement for transactions linked to terrorist financing.

During 2006, several changes were made in Romania's laws in order to bring the country into harmony with FATF recommendations and EU Directives. Specifically, laws were changed to allow an increase in the level of fines in correspondence with the inflation rate; use of undercover investigators; reports to be sent from the FIU to the General Prosecutor's Office in an unclassified manner so that they may be used in operational investigations; confiscation of goods used in or resulting from money laundering activities; an increase in the length of time that bank accounts may be frozen from ten days up to one month.

In keeping with new international standards, Romania has taken steps to strengthen its know-your-customer (KYC) identification requirements. Romania has implemented KYC regulations that mandate identification of the client upon account opening and when single or multiple transactions meet or approach 10,000 euros (approximately $13,000). In December 2003, Romania's central bank, the National Bank of Romania (BNR), introduced Norm No. 3, "Know Your Customer." This regulation strengthens information disclosure for outgoing wire transfers and correspondent banking by requiring banks to include information about the originator's name, address, and account. The same information is required for incoming wires as well. Banks are further required to undertake proper due diligence before entering into international correspondent relations, and are prohibited from opening correspondent accounts with shell banks. In 2006, the BNR widened the scope of its KYC norms by extending their application to all other nonbanking financial institutions falling under its supervision. In 2005, the Insurance Supervision Commission instituted similar regulations for the insurance industry.

Romania's financial intelligence unit (FIU), the National Office for the Prevention and Control of Money Laundering (NOPCML), was established in 1999. All currency transaction reports and

suspicious transaction reports must be forwarded to the FIU. The FIU oversees the implementation of anti-money laundering guidelines for the financial sector and works to ensure that adequate training is provided for all domestic financial institutions covered by the law. The FIU is also authorized to participate in inspections and controls in conjunction with supervisory authorities, having carried out 118 on-site inspections during the first ten months of 2006. In July 2006, the FIU Board issued regulations implementing KYC standards for nonfinancial reporting agencies that are not the subject of supervision by other national authorities. These norms are consistent with EU Directives and allow the FIU to increase supervision of entities (casinos, notaries, real estate brokers) previously unsupervised for compliance with AML regulations.

In 2006, the FIU received 46,725 currency transaction reports detailing 8,377,762 transactions exceeding the reporting threshold of 10,000 Euros. Of these transactions, 3.9 percent were carried out by individuals; the remainder was carried out by corporate entities. During the same period, the FIU also received 6,054 reports of foreign banking transfers detailing 753,674 transactions that exceed the reporting threshold. Of these transactions, 5.1 percent were carried out by individuals and the rest by corporations. The total number of suspicious transactions reported to the FIU dropped slightly from 2,826 in the first ten months of 2005 to 2,296 in the first ten months of 2006. Of this figure, reporting by banks and other credit institutions dropped from 1,993 in the first ten months of 2005 to 1,756 in the first ten months of 2006. During the first ten months of 2006, the FIU suspended two suspicious transactions totaling $9.65 million and levied fines totaling $81,273.

Upon completion of its analysis, the FIU forwards its findings to the appropriate government agency for follow-up investigation. During the first ten months of 2006, the number of files sent to the General Prosecutor's Office on suspicion of money laundering was 124, compared to 411 in 2005 and 501 in 2004. During the first ten months of 2006, the number of files sent to the National Anti-Corruption Department on suspicion of money laundering was seven, compared to 41 notifications in the first ten months of 2005, and 22 in 2004. With regard to terrorism financing, the FIU did not send any files to the Romanian Intelligence Service (SRI) during the first ten months of 2006. The FIU also sent six notifications to the Police General Inspectorate, three to the Financial Guard and three to the National Agency for Fiscal Administration in the first ten months of 2006.

Efforts to prosecute these cases have been hampered by a lack of specialization and technical knowledge of financial crimes within the judiciary. Moreover, coordination between law enforcement and the justice system remains limited. Between January 1, 2006 and December 31, 2006, 102 defendants were indicted by the Directorate for the Investigation of Organized Crime and Terrorism Offences (DIICOT) in 22 cases involving money laundering. Between January 1, 2006 and September 30, 2006, four persons received final convictions and one person was acquitted on charges originating in previous years. A conviction is not final in Romania until all appeals remedies have been exhausted.

Since its establishment, the NOPCML has had to deal with numerous operational and political challenges. However, in June 2004, the standing of Romania's FIU began to improve when the Government of Romania (GOR) appointed a new director to head the FIU. The new director significantly improved the office's operational efficiency and brought greater visibility to the importance of AML and counterterrorism financing CTF efforts in Romania. Some significant improvements made include the approval of a new organizational structure for the FIU (as mandated by Governmental Decision No. 1078/2004), as well as the passage of legislation that was designed to improve the procedures for analyzing STR information and the suspension of suspicious accounts and transactions.

In February 2006, the GOR again appointed a new director to head the FIU. The new director and the FIU's supervisory board have worked to improve the quality of cases forwarded to prosecutors for judicial action. While the number of cases forwarded to the General Prosecutor's Office in 2006 has declined, the FIU believes that the number of indictments, and eventually convictions, will increase as

the FIU has started to place a greater emphasis on the quality of reports produced as opposed to the quantity of reports forwarded to the Prosecutor's Office. In April 2006, the GOR approved a new organizational charter for the FIU that established a new division (Legal, Methodology, and Control Department) within the FIU and also allowed an increase in the FIU's staff from 84 to 120 people. In July 2006, the FIU moved to new facilities that will better accommodate staff growth and provide improved infrastructure for resource enhancements and security.

In response to the events of September 11, 2001, Romania passed a number of legislative measures designed to sanction acts contributing to terrorism. Emergency Ordinance 141, passed in October 2001, provides that the production or acquisition of means or instruments, with intent to commit terrorist acts, are offenses of exactly the same level as terrorist acts themselves. These offenses are punishable with imprisonment ranging from five to 20 years.

In April 2002, the Supreme Defense Council of the Country (CSAT) adopted a National Security Strategy, which includes a General Protocol on the Organization and Functioning of the National System on Preventing and Combating of Terrorist Acts. This system, effective July 2002 and coordinated through the Intelligence Service, brings together and coordinates a multitude of agencies, including 14 ministries, the General Prosecutor's Office, the central bank, and the FIU. The GOR has also set up an inter-ministerial committee to investigate the potential use of the Romanian financial system by terrorist organizations.

The GOR announced a national anticorruption plan in early 2003 and passed a law criminalizing organized crime in April 2003. A new Criminal Procedure Code was passed and entered into force on July 1, 2003. The new Code contains provisions for authorizing wiretaps and intercepting and recording telephone calls in money laundering and terrorist financing cases.

Romanian law has some limited provisions for asset forfeiture in the Law on Combating Corruption, No. 78/2000, and the Law on Prevention and Combat of Tax Evasion, No. 241, introduced in July 2005. The GOR, and particularly the central bank, has been cooperative in seeking to identify and freeze terrorist assets. Emergency Ordinance 159, passed in late 2001, includes provisions for preventing the use of the financial and banking system to finance terrorist attacks, and sets forth the parameters for the government to combat such use. Emergency Ordinance 153 was passed to strengthen the government's ability to carry out the obligations under UNSCR 1373, including the identification, freezing, and seizure of terrorist funds or assets. Legislative changes in 2005 extended the length of time a suspect account may be frozen. The FIU is now allowed to suspend accounts suspected of money laundering activity for three working days, as opposed to the previous two day limit. In addition, once the case is sent to the General Prosecutor's Office, it may further extend the period by four working days instead of the previously allowed three days.

In November 2004, the Parliament adopted law 535/2004 on preventing and combating terrorism, which abrogates some of the previous government ordinances and incorporates many of their provisions. The law includes a chapter on combating the financing of terrorism by prohibiting financial and banking transactions with persons included on international terrorist lists, and requiring authorization for transactions conducted with entities suspected of terrorist activities in Romania.

The central bank receives lists of individuals and terrorist organizations provided by the United States, the UNSCR 1267 Sanctions Committee, and the EU, and it circulates these to banks and financial institutions. The new law on terrorism provides for the forfeiture of assets used or provided to terrorist entities, together with finances resulting from terrorist activity. To date, no terrorist financing arrests, seizures, or prosecutions have been carried out.

The GOR recognizes the link between organized crime and terrorism. Romania is a member of and host country for the headquarters of the Southeast European Cooperative Initiative's (SECI) Center for Combating Transborder Crime, a regional center that focuses on intelligence sharing related to

criminal activities, including terrorism. Romania also participates in a number of regional initiatives to combat terrorism. Romania has worked within SEEGROUP (a working body of the NATO initiative for Southeast Europe) to coordinate counterterrorist measures undertaken by the states of Southeastern Europe. The Romanian and Bulgarian Interior Ministers signed an inter-governmental agreement in July 2002 to cooperate in the fight against organized crime, drug smuggling, and terrorism.

The FIU is a member of the Egmont Group and participates as a member in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). A Mutual Legal Assistance Treaty signed in 2001 between the United States and Romania entered into force in October 2001. The GOR has demonstrated its commitment to international anticrime initiatives by participating in regional and global anticrime efforts. Romania is a party to the 1988 UN Drug Convention, the Agreement on Cooperation to Prevent and Combat Transborder Crime, and the UN Convention against Transnational Organized Crime. Romania also is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the Council of Europe's Criminal Law Convention on Corruption; and the UN International Convention for the Suppression of the Financing of Terrorism. On November 2, 2004, Romania became a party to the UN Convention against Corruption. The FIU has signed bilateral memoranda with Spain, Belgium, Poland, Czech Republic, Austria, Croatia, Slovenia, Italy, Serbia, Greece, Bulgaria, Ukraine, Turkey, South Korea, and Thailand. The NOPCML is currently working on finalizing an MOU with the United States. In an EU project completed in July 2005, the FIU worked closely with Italy to improve its efficiency and effectiveness.

Although Romania's AML legislation and regulations are comprehensive in scope, implementation lags. The FIU has improved in its ability to report and investigate cases in a timely fashion, and has improved the quality of its reporting. However, these investigations have resulted in only a handful of successful prosecutions to date. With the conclusion of the Romanian capital account liberalization in 2006, the risk of money laundering through nonbanking entities will increase. Romania should continue its efforts to ensure that nonbank financial institutions are adequately supervised and that the sector is trained on identification of suspicious transaction and reporting and record-keeping responsibilities. Romania should continue to improve communications between reporting and monitoring entities, as well as between prosecutors and the FIU. There is an over-reliance on financial reporting to initiate investigations. More effort should be made by Romanian law enforcement and customs authorities to recognize money laundering. Increased border enforcement and antismuggling measures are necessary. The General Prosecutor's Office should place a higher priority on money laundering cases. Romania should further implement existing procedures for the timely freezing, seizure, and forfeiture of criminal or terrorist-related assets. Romania should take specific steps to combat corruption in commerce and government.

## Russia

Russia's financial system does not attract a significant portion of legal or illegal depositors, and therefore Russia is not considered an important regional financial center. Criminal elements from Russia and neighboring countries continue to use Russia's financial system to launder money because of familiarity with the language, culture, and economic system. The majority of laundered funds do not appear to be from activities related to narcotics production or trafficking, although these activities occur. Experts believe that most of the illicit funds flowing through Russia derive from domestic criminal or quasi-criminal activity, including evasion of tax and customs duties and smuggling operations. Despite making progress in combating financial crime, Russia remains vulnerable to such activity because of its vast natural resource wealth, the pervasiveness of organized crime, and a high level of corruption. Other factors include porous borders, Russia's role as a geographic gateway to Europe and Asia, a weak banking system with low public confidence in it, and under-funding of

regulatory and law enforcement agencies. However, due to rapid economic growth in various sectors, the number of depositors has steadily been increasing.

Russia has recently changed its laws to allow direct foreign ownership and investment in Russian financial institutions. Net private capital inflows for 2006 amounted to $41.6 billion according to the Russian Central Bank, an increase from $1.1 billion in 2005. In contrast to the capital flight that occurred during the 1990s, the majority of more recent outflows involved the legitimate movement of money to more secure and profitable investments abroad, which reflects the maturing of the Russian business sector. However, a portion of this money undoubtedly involved the proceeds of criminal activity. According to official statistics, the trend toward net capital inflows involves the transfer of assets from tax havens, such as Cyprus and the Virgin Islands, previously known to be popular destinations for Russian capital outflows in the 1990s.

Russia has the legislative and regulatory framework in place to pursue and prosecute financial crimes, including money laundering and terrorism finance. The Russian Federation's Federal Law No. 115-FZ "On Combating Legalization (Laundering) of Criminally Gained Income and Financing of Terrorism" became effective on February 1, 2002, with subsequent amendments to the laws on banking, the securities markets, and the criminal code taking effect in October 2002, January 2003, December 2003, and July 2004, respectively. Law RF 115-FZ obligates banking and nonbanking financial institutions to monitor and report certain types of transactions, keep records, and identify their customers.

According to the original language of RF 115-FZ, institutions legally required to report include: banks, credit organizations, securities market professionals, insurance and leasing companies, the federal postal service, jewelry and precious metals merchants, betting shops, and companies managing investment and nonstate pension funds. Amendments to the law that came into force on August 31, 2004 extend the reporting obligation to real estate agents, lawyers and notaries, and to persons rendering legal or accounting services that involve certain transactions (e.g., managing money, securities, or other property; managing bank accounts or securities accounts; attracting or managing money for organizations; or incorporating, managing, and buying or selling organizations).

Various regulatory bodies ensure compliance with Russia's anti-money laundering and counterterrorism finance laws. The Central Bank of Russia (CBR) supervises credit institutions; the Federal Insurance Supervision Service oversees insurance companies; the Federal Service for Financial Markets regulates entities managing nongovernmental pension and investment funds, as well as professional participants in the securities sector; and the Assay Chamber (under the Ministry of Finance) supervises entities buying and selling precious metals or stones.

The CBR has issued guidelines regarding anti-money laundering (AML) practices within credit institutions, including "know your customer" (KYC) and bank due diligence programs. Banks are required to obtain and retain for five years information regarding individuals and legal entities and beneficial owners of corporate entities. Banks must also adopt internal compliance rules and procedures and appoint compliance officers. The amendment to Law 115-FZ has required banks to identify the original source of funds and to report to the financial intelligence unit (FIU) all suspicious transactions since July 2004. Institutions that fail to meet mandatory reporting requirements face revocation of their licenses to carry out relevant activity, limits on certain banking operations, and possible criminal or administrative penalties. An administrative fine of up to $16,700 can be levied against an institution, with a fine of up to $700 on an officer of an institution. The maximum criminal penalty is 10 years in prison with applicable fines.

All obligated financial institutions must monitor and report to the government: any transaction that equals or exceeds 600,000 rubles (approximately $22,700) and involves or relates to cash payments, individuals or legal entities domiciled in states that do not participate in the international fight against money laundering, bank deposits, precious stones and metals, payments under life insurance policies,

or gambling; all transactions of "extremist organizations" or individuals included on Russia's domestic list of such entities and individuals; and suspicious transactions.

Since the CBR issued Order 1317-U in August 2003, Russian financial institutions must now report all transactions with their counterparts in offshore zones. In some cases, offshore banks are also subject to enhanced due diligence and maintenance of additional mandatory reserves to offset potential risks undertaken when conducting specific transactions. The CBR has also raised the standards for offshore financial institutions, resulting in a reduction in the number of such institutions. Overall wire transfers from Russian banks to offshore financial centers have dropped significantly as a result of such regulatory measures.

Foreign financial entities, including those from known offshore havens, are not permitted to operate directly in Russia; they must do so solely through subsidiaries incorporated in Russia, which are subject to domestic supervisory authorities. During the process of incorporating and licensing these subsidiaries, Russian authorities must identify and investigate each director of the Russian unit, as nominee or anonymous directors are prohibited under Russian law. In September 2005, the CBR completed its review of all banks that sought admission to the recently established Deposit Insurance System (DIS). To gain admission to the DIS, a bank had to verifiably demonstrate to the CBR that it complies with Russian identification and transparency requirements. Currently, 927 of Russia's estimated 1200 banks have been admitted to the DIS, effectively removing over 200 banks from Russia's banking system.

By law, Russian businesses must obtain government permission before opening operations abroad, including in offshore zones. A department within the Ministry of Economic Development and Trade (MEDT) reviews such requests from Russian firms, and once the MEDT approves, the CBR must then approve the overseas currency transfer. In either case, the regulatory body responsible for the offshore activity is the same as for domestic activity, i.e., the Federal Service for Financial Markets regulates brokerage and securities firms, while the CBR regulates banking activity.

Article 8 of Law 115-FZ provides for the establishment of Russia's FIU, called the Federal Service for Financial Monitoring (FSFM). FSFM is an independent executive agency administratively subordinated to the Ministry of Finance. All financial institutions with an obligation to report certain transactions must report the required information to the FSFM. The FSFM is also the regulator for the real estate and leasing, pawnshops, and gaming services sectors. An administrative unit, it has no law enforcement investigative powers. Depending on the nature of the activity, the FSFM provides information to the appropriate law enforcement authorities for further investigation, i.e., the Economic Crimes Unit of the Ministry of Interior (MVD) for criminal matters, the Federal Drug Control Service (FSKN) for narcotics-related activity, or the Federal Security Service (FSB) for terrorism-related cases.

In June 2005, President Putin approved a national strategy for combating money laundering and terrorism finance, part of which called for the creation of a new Interagency Commission on Money Laundering, comprised of twelve ministries and government departments. In addition to receiving, analyzing and disseminating information from the reporting entities, the FSFM has the responsibility of implementing the state policy to combat money laundering and terrorism financing. The Interagency Commission is chaired by the head of the FSFM and is responsible for monitoring and coordinating the government's activity on money laundering and terrorism financing. FSFM authorities credit cooperation among Commission members for the conviction of 257 individuals on money laundering charges between January and June 2006.

Nearly all financial institutions submit reports to the FSFM via encrypted software provided by the FSFM. According to press reports, Russia's national database contains over four million reports involving operations and deals worth over $877 billion. The FSFM estimates that Russian citizens may have laundered as much as $8 billion in the first three quarters of 2006. The FSFM receives

approximately 30,000 transaction reports daily. Of these daily reports, 25 percent result from mandatory (currency) transaction reports, and 75 percent relate to suspicious transactions.

Each of the FSFM's seven territorial offices corresponds with one of the federal districts that comprise the Russian Federation. The Central Federal District office is headquartered in Moscow; the remaining six are located in the major financial and industrial centers throughout Russia (St. Petersburg, Ekaterinburg, Nizhny Novgorod, Khabarovsk, Novosibirsk and Rostov-on-Don). The territorial offices coordinate with regional law enforcement and other authorities to enhance the information flow into the FSFM, and to supervise compliance with anti-money laundering and counterterrorism financing legislation by institutions under FSFM supervision. Additionally, the satellite offices must identify and register at the regional level all pawnshops, leasing and real estate firms, and gaming entities under their jurisdiction. The regional offices also are charged with coordinating the efforts of the CBR and other supervisory agencies to implement anti-money laundering and counterterrorist financing regulations. Russia's anti-money laundering law, as amended, provides the FSFM with the appropriate authority to gather information regarding the activities of investment foundations, nonstate pension funds, gambling businesses, real estate agents, lawyers and notaries, persons rendering legal/accountancy services, and sellers of precious metals and jewelry.

During the first eight months of 2006, the FSFM carried out 2,700 financial investigations, referring 1,050 of them to law enforcement agencies for possible criminal investigations. According to the MVD, in the first half of 2006 Russian law enforcement investigated 6,300 cases of money laundering, sent 3,500 of the cases to court, and convicted 257 individuals on money laundering charges. Both the FSFM and MVD report that the number of suspicious transaction reports in 2006 has grown nearly ten-fold over the previous year, an increase which both agencies attribute to a greater focus government-wide on financial crimes and terrorism financing.

As part of administrative reforms enacted in 2004, the FSKN now has a full division committed to money laundering, staffed by agents with experience in counter narcotics and economic crimes. This division cooperates closely with the FSFM in pursuing narcotics-related money laundering cases. From January through August 2006, the FSKN reportedly initiated 1,332 money laundering cases and referred over 340 of these cases to the General Procuracy for prosecution. Consistent with Financial Action Task Force (FATF) recommendations, the criminal code was amended in December 2003 to remove a specific monetary threshold for crimes connected with money laundering, thus paving the way for prosecution of criminal offenses regardless of the sum involved.

With its legislative and enforcement mechanisms in place, Russia has begun to prosecute high-level money laundering cases. Through September 2006, the CBR revoked the licenses of 48 banks for failing to observe banking regulations. Of these, 25 banks lost their licenses for violating Russia's anti-money laundering laws. First Deputy Chairman Andrey Kozlov led the CBR's efforts to implement stronger anti-money laundering guidelines until his assassination in September 2006. He worked to implement the managerial and reporting requirements that made license revocation politically feasible, and had taken steps to prohibit individuals convicted of money laundering from serving in leadership positions in the banking community. This latter issue remains pending with the CBR. President Putin publicly committed to continuing Kozlov's work to preclude shadow economy groups from finding haven in the country's financial sector.

In October 2006, the Interior Ministry's Department for Economic Security reported that it had shut down a Georgian crime ring that had laundered as much as $9 billion from April 2004 to January 2005 through as many as five Russian banks. The announcement stated that the FSFM's analysis and cooperation with law enforcement authorities in Germany, Austria, Latvia, Lithuania, and Israel provided sufficient information to freeze the crime ring's bank assets. According to Interior Ministry representatives, two of the suspected banks' licenses had been revoked more than a year before the Department of Economic Security action.

Russian legislation provides for the tracking, seizure and forfeiture of criminal proceeds. None of this legislation is specifically tied to narcotics proceeds. Legislation provides for investigative techniques such as search, seizure, and the identification, freezing, seizing, and confiscation of funds or other assets. Authorities can also compel targets to produce documents. Where sufficient grounds exist to suppose that property was obtained as the result of a crime, investigators and prosecutors can apply to the court to have the property frozen or seized. Law enforcement agencies have the power to identify and trace property that is, or may become, subject to confiscation or is suspected of being the proceeds of crime or terrorist financing. The law allows the FSFM, in concert with banks, to freeze possible terrorist-related financial transactions for one week: banks may freeze transactions for two days, and the FSFM may follow up with freezing for an additional five days.

In accordance with its international agreements, Russia recognizes rulings of foreign courts relating to the confiscation of proceeds from crime within its territory and can transfer confiscated proceeds of crime to the foreign state whose court issued the confiscation order. However, Russian law still does not provide for the seizure of instruments of crime. Businesses can be seized only if it can be shown that they were acquired with criminal proceeds. Legitimate businesses cannot be seized solely on the basis that they were used to facilitate the commission of a crime.

The Presidential Administration as well as Russian law enforcement agencies have expressed concern about ineffective implementation of Russia's confiscation laws. The government has proposed amendments that are currently under review by the Duma (Parliament) which would make it easier to identify and seize criminal instrumentalities and proceeds. While Russian law enforcement has adequate police powers to trace assets, and the law permits confiscation of assets, most Russian law enforcement personnel lack experience and expertise in these areas.

The Russian Federation has enacted several pieces of legislation and issued executive orders to strengthen its ability to fight terrorism. On January 11, 2002, President Putin signed a decree entitled "On Measures to Implement the UN Security Council Resolution (UNSCR) No. 1373 of September 28, 2001." Noteworthy among this decree's provisions are the introduction of criminal liability for intentionally providing or collecting assets for terrorist use, and the instructions to relevant agencies to seize assets of terrorist groups. When this latter clause conflicted with existing domestic legislation, the Duma within the year approved an amendment to the anti-money laundering law, resolving the conflict and allowing banks to freeze assets immediately pursuant to UNSCR 1373. Article 205.1 of the criminal code, enacted in October 2002, criminalizes terrorist financing. On October 31, 2002, the Federation Council, Russia's upper house, approved a supplemental article to the 2003 federal budget, allocating from surplus government revenues an additional 3 billion rubles ($1.1 million) in support of federal counterterrorism programs and improvement of national security.

The FSFM reports that in regard to terrorism financing, it has compiled a list of 1,300 organizations and individuals suspected of financing terrorism, 400 of which were foreign. There are five sources of information that may designate entities for inclusion on the FSFM's list of proscribed organizations. International organizations' designations, such as the UN 1267 Sanctions Committee, constitute the first source. Second, Russian court decisions provide a basis for inclusion. Third, resolutions from the Prosecutor General can identify individuals and organizations for inclusion. Fourth, Ministry of Interior investigations serve as a basis for inclusion if subsequent court decisions do not dismiss the investigation's findings. Finally, bilateral agreements, which include information sharing regarding entities on the counterpart's entities list, may provide a basis for inclusion on the FSFM list. As of a year ago, the FSFM has uncovered 113 bank accounts related to organizations and individuals included on Russia's terrorist list.

In February 2003, at the request of the General Procuracy, the Russian Supreme Court issued an official list of 15 terrorist organizations. According to press reports, the financial assets of these organizations were immediately frozen. In addition, Russia has assisted the United States in

investigating high profile cases involving terrorist financing. In 2003, Russia provided vital financial documentation and other evidence that helped establish the criminal activities of the Benevolence International Foundation (BIF). In April 2005, a U.S. Federal Court convicted a British national for attempting to smuggle shoulder-held missiles into the U.S. with the intent to sell the weapons to a presumed terrorist group. The subject was arrested in a sting operation that involved 18 months of collaboration among U.S., Russian, and British authorities. He was found guilty on five counts, including material support to terrorists, unlawful arms sale, smuggling, and two counts of money laundering. However, Russia and the U.S. continue to differ about the purpose of the UN 1267 Sanctions Committee's designation process, and such political differences have hampered bilateral cooperation in this forum.

The United States and Russia signed a Mutual Legal Assistance Treaty in 1999, which entered into force on January 31, 2002. The FSFM has signed cooperation agreements with the Financial Intelligence Units (FIUs) of 24 countries, including the United States. The FSFM has been an active member of the Egmont Group since June 2002, having sponsored candidate FIUs from the former Soviet republics, including current FIU members in Ukraine and Georgia. U.S. law enforcement agencies exchange operational information with their Russian counterparts on a regular basis. In 2005, Russian law enforcement agencies cooperated with the U.S. in a high-profile case that led to the conviction of a Russian national in a U.S. District Court on charges that he laundered over $130 million through a Moscow bank. The individual was sentenced to 51 months imprisonment and ordered to pay $17.4 million in restitution to the Russian government. This close cooperation between Russian and U.S. agencies has continued and strengthened in 2006.

Russia became a full member of the Financial Action Task Force in June 2003 and participates as an active member in two FATF-style regional bodies. It is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and was instrumental in the creation of the Eurasian Group on Combating Legalization of Proceeds from Crime and Terrorist Financing (EAG). The EAG Secretariat is located in Moscow. In December 2005, under the auspices of the EAG, the FSFM established the International Training and Methodological Center of Financial Monitoring (ITMCFM). The main function of the Center is to provide technical assistance to EAG member-states, primarily in the form of staff training for FIUs and other interested ministries and agencies involved in AML/CFT efforts. The ITMCFM also conducts research on AML/CFT issues. As Chairman of the EAG, Russia's FIU continues to play a strong leadership role in bringing the region up to international standards in its capacity to fight money laundering and terrorism financing.

Russia ratified the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime in January 2001. Russia is a party to the 1988 UN Drug Convention and on May 26, 2004, became a party to the UN Convention against Transnational Organized Crime. In November 2002, Russia ratified the UN International Convention for the Suppression of the Financing of Terrorism. Russia also became a signatory to, and ratified on May 9, 2006, the UN Convention against Corruption.

Through aggressive enactment and implementation of comprehensive money laundering and counterterrorism financing legislation, Russia now has well-established legal and enforcement frameworks to deal with money laundering and terrorism financing. Given its role in the creation and maintenance of the EAG, Russia has also demonstrated the will and capability to improve the region's capacity for countering money laundering and terrorism financing.

Nevertheless, serious vulnerabilities remain. Russia is among the world's most sophisticated perpetrators of fraud and money laundering through electronic and internet-related means. To meet its goal of combating money laundering and corruption, Russia needs to follow through on its commitment to improve CBR oversight of shell companies and scrutinize more closely those banks

that do not carry out traditional banking activities, including making all offshore operations subject to the identical due diligence and reporting requirements as other sectors. To prevent endemic corruption and deficiencies in the business environment from undermining Russia's efforts to establish a well-functioning anti-money laundering and counterterrorism finance regime, Russia should strive to stamp out official corruption, particularly at high levels, and to increase transparency in the financial sector and the corporate environment. Russia should also commit adequate resources to its regulatory and law enforcement entities in order to help them fulfill their responsibilities. Additionally, Russia should work to increase the effectiveness of its confiscation laws and their implementation including enacting legislation providing for the seizure of instruments, in addition to the proceeds, of criminal activity. Finally, Russia should continue to play a leadership role in the region with regard to anti-money laundering and counterterrorist finance regime implementation.

## Samoa

Samoa does not have major organized crime, fraud, or drug problems. The most common crimes that generate revenue within the jurisdiction are primarily the result of low-level fraud and theft. The domestic banking system is very small, and there is relatively little risk of significant money laundering derived from domestic sources. Samoa's offshore banking sector is relatively small. The Government of Samoa (GOS) enacted the Money Laundering Prevention Act (the Act) in 2000. This law criminalizes money laundering associated with numerous crimes, sets measures for the prevention of money laundering and related financial supervision. Newly adopted regulations and guidelines fully implementing this legislation came into force in 2002. Under the Act, a conviction for a money laundering offense is punishable by a fine not to exceed Western Samoa Tala (WST) one million (approximately $354,000), a term of imprisonment not to exceed seven years, or both.

The Act requires financial institutions to report transactions considered suspicious to the Money Laundering Prevention Authority (MLPA), the Samoa Financial Intelligence Unit (FIU) currently working under the auspices of the Governor of the Central Bank. The MLPA receives and analyzes Samoa disclosures, and if it establishes reasonable grounds to suspect that a transaction involves the proceeds of crime, it refers the information to the Attorney General and the Commissioner of Police. The MLPA has received 69 suspicious transaction reports as of September 2006. In 2003, Samoa established an independent and permanent Transnational Crime Unit (TCU) under the authority of the Ministry of the Prime Minister. The TCU is staffed by personnel from the Samoa Police Service, Immigration Division of the Ministry of the Prime Minister, and Division of Customs. The TCU is responsible for intelligence gathering and analysis and investigating transnational crimes, including money laundering, terrorist financing and the smuggling of narcotics and people.

The Act requires financial institutions to record new business transactions exceeding WST 30,000 (approximately $10,000), to retain records for a minimum of seven years, and to identify all parties to the transactions. This threshold reporting system could expose the financial institutions to potential abuse. Nevertheless, Section 43(a) of the Money Laundering Prevention Regulations 2002 requires financial institutions to identify their customers when "there are reasonable grounds for believing that the one-off transaction is linked to one or more other one-off transactions and the total amount to be paid by or to the applicant for business in respect to all of the linked transactions is WST 30,000, or the equivalent in another currency." Proposed amendments to the Act would delete the threshold reporting system, leaving it open for all financial institutions to report any amount or transaction that purports to involve money laundering.

Section 12 of the Act establishes that all financial institutions have an obligation under this law to "develop and establish internal policies, procedures and controls to combat money laundering, and develop audit functions in order to evaluate such policies, procedures and controls." Reportedly, the Regulations and Guidelines that have been developed remedy the lack of specificity in the Act about

the obligation of financial institutions to establish the identity of the beneficial owner of an account managed by an intermediary. Specifically, Section 12.06 of the Money Laundering Prevention Guidelines for the Financial Sector provides that "[i]f funds to be deposited or invested are being supplied by or on behalf of a third party, the identity of the third party (the underlying beneficiary) should also be established and verified." The law requires individuals to report to the MLPA if they are carrying with them WST 10,000 (approximately $3,300) or more, in cash or negotiable instruments, upon entering or leaving Samoa.

The Act removes secrecy protections and prohibitions on the disclosure of relevant information. Moreover, it provides protection from both civil and criminal liability for disclosures related to potential money laundering offenses to the competent authority.

The Central Bank of Samoa, the Samoa International Finance Authority, and the MLPA regulate the financial system. There are four locally incorporated commercial banks, supervised by the Central Bank. The Samoa International Finance Authority has responsibility for regulation and administration of the offshore sector. There are no casinos, but two local lotteries are in operation.

Samoa is an international offshore financial center, with six licensed international banks which have offices and employees. For entities registered or licensed under the various Offshore Finance Centre Acts, there are no currency or exchange controls or regulations, and no foreign exchange levies payable on foreign currency transactions. No income tax or other duties, nor any other direct or indirect tax or stamp duty is payable by registered/licensed entities. In addition to the six offshore banks, Samoa currently has 19,000 international business corporations (IBCs), three international insurance companies, six trustee companies, and 175 international trusts. Section 20 of the International Banking Act prohibits any person from applying to be a director, manager, or officer of an offshore bank who has been sentenced for an offense involving dishonesty. The prohibition is also reflected in the application forms and Personal Questionnaire that are completed by prospective applicants that detail the licensing requirements for offshore banks. The application forms list the required supporting documentation for proposed directors of a bank. These include references from a lawyer, accountant, and a bank, police clearances, curriculum vitae, certified copies of passports and personal statements of assets and liabilities (if also a beneficial owner). The Inspector of International Banks must be satisfied with all supporting documentation that a proposed director is fit and proper in terms of his integrity, competence and solvency.

International cooperation can occur only if Samoa has entered into a mutual cooperation agreement with the requesting nation. Under the Act, the MLPA has no powers to exchange information with overseas counterparts. All cooperation under the MLPA is through the Attorney General's Office, which is the Competent Authority under the Act for receiving and implementing information exchange requests. Samoa has reviewed the legal framework for the effective operation of the MLPA in order to further strengthen domestic and international information exchange. In addition, the Office of the Attorney General, in conjunction with the Central Bank, the Ministry of Police and the Division of Customs of the Ministry for Revenue, have prepared amendments to the Money Laundering Prevention Act of 2000 to strengthen and complement legislation that is being drafted or developed, including the Proceeds of Crime Bill, the Mutual Assistance in Criminal Matters Bill, the Extradition Amendment Bill and the Insurance Bill. These Bills are expected to be enacted in the first quarter of 2007.

Samoa is a party to the UN International Convention for the Suppression of the Financing of Terrorism. In 2002, Samoa enacted the Prevention and Suppression of Terrorism Act. The Act defines and criminalizes terrorist offenses, including the financing of terrorist activities. The combined effect of the Money Laundering Prevention Act of 2000 and the Prevention and Suppression of Terrorism Act of 2002 is to make it an offense for any person to assist a criminal in obtaining, concealing, retaining or investing funds, or to finance or facilitate the financing of terrorism.

Since the passage of the Money Laundering Prevention Act in June 2000, Samoa has continued to strengthen its anti-money laundering regime and has issued regulations and guidelines to financial institutions so that they have a clear understanding of their obligations under the Act. Particular emphasis is directed toward regulation of the international financial sector, principally the establishment of due diligence procedures for owners and directors of banks and the elimination of anonymous accounts. The Government of Samoa is strengthening relevant legislation to identify the beneficial owners of IBCs to help ensure that criminals do not use them for money laundering or other financial crimes. Samoa is in the process of adopting amended and additional legislation to allow for international cooperation and information sharing.

The inability of the Money Laundering Prevention Authority simply to exchange information on an administrative level is a material weakness of the current system and is an impediment to international cooperation. To rectify that situation, the Government of Samoa has prepared the necessary changes to the Money Laundering Prevention Act to enable information exchange with overseas counterparts.

Samoa is a member of the Asia/Pacific Group on Money Laundering (APG)_and the Pacific Island Forum. Samoa hosted the annual plenary of the Pacific Island Forum in August 2004. Samoa is a party to the 1988 UN Drug Convention. Samoa has not signed the UN Convention against Transnational Organized Crime.

The Asia Pacific Group on Money Laundering and the Offshore Group of Banking Supervisors (APG/OGBS) undertook a second Mutual Evaluation of Samoa's compliance with international standards in February 2006. The resulting Mutual Evaluation Report (MER) was adopted at the APG Annual Meeting in Manila, the Philippines in July 2006. The MER noted that the GOS has sought to remedy major deficiencies with only partial success. Major deficiencies were noted in the legal and regulatory systems of both the onshore and offshore sectors as well as with what appears to be lack of political will throughout the system. STRs have continuously declined in the past several years and none have been disseminated to the Police for investigation, with the result that there have been no prosecutions or convictions for money laundering. There are serious impediments to exchanging information domestically and internationally. In sum, Samoa's anti-money laundering/counterterrorist regime is not functioning. An offshore sector that enables the anonymous establishment of IBCs violates the fundamental principal of transparency that underlies all international standards. The Government of Samoa should take all necessary steps to establish a regime that comports with all international standards, to which it has committed to adhere by virtue of its membership in the APG. The GOS has stated that the main noncompliance issues raised in the MER will be addressed when the proposed pieces of legislation mentioned above are passed and enacted in early 2007. The Government of Samoa should become a party to the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

## Saudi Arabia

Saudi Arabia is a growing financial center in the Gulf Region of the Middle East. There is little money laundering in Saudi Arabia related to traditional predicate offenses. All eleven commercial banks in Saudi Arabia operate as standard "western-style" financial institutions and all banks operate under the supervision of the Central Bank, the Saudi Arabian Monetary Agency (SAMA). Saudi Arabia is not an offshore financial center. There are no free zones for manufacturing, although there are bonded transit areas for the transshipment of goods not entering the country. The money laundering and terrorist financing that does occur in Saudi Arabia are not primarily related to narcotics proceeds.

Saudi donors and unregulated charities have been a major source of financing to extremist and terrorist groups over the past 25 years. However, the Final Report of the National Commission on Terrorist Attacks Upon the United States ("The 9/11 Commission") found no evidence that either the Saudi Government, as an institution, or senior Saudi officials individually, funded al-Qaida.

Following the al-Qaida bombings in Riyadh on May 12, 2003, the Government of Saudi Arabia (GOSA) has taken significant steps to help counteract terrorist financing.

In 2003, Saudi Arabia approved a new anti-money laundering law that for the first time contains criminal penalties for money laundering and terrorist financing. The law bans conducting commercial or financial transactions with persons or entities using pseudonyms or acting anonymously; requires financial institutions to maintain records of transactions for a minimum of ten years and adopt precautionary measures to uncover and prevent money laundering operations; requires banks and financial institutions to report suspicious transactions (STRs); authorizes government prosecutors to investigate money laundering and terrorist financing; and allows for the exchange of information and judicial actions against money laundering operations with countries with which Saudi Arabia has official agreements.

SAMA guidelines correspond to the Recommendations of the Financial Action Task Force (FATF). On May 27, 2003, SAMA issued updated anti-money laundering and counterterrorist finance guidelines for the Saudi banking system. The guidelines require that: banks have mechanisms to monitor all types of "Specially Designated Nationals" as listed by SAMA; fund transfer systems be capable of detecting specially designated nationals; banks strictly adhere to SAMA circulars on opening accounts and dealing with charity and donation collection; and banks be able to provide the remitter's identifying information for all outgoing transfers. The new guidelines also require banks to use software to profile customers to detect unusual transaction patterns; establish a monitoring threshold of SR 100,000 (approximately $26,670); and develop internal control systems and compliance systems. SAMA also issued "know your customer" guidelines, requiring banks to freeze accounts of customers who do not provide updated account information. Saudi law prohibits nonresident individuals or corporations from opening bank accounts in Saudi Arabia without the specific authorization of SAMA. There are no bank secrecy laws that prevent financial institutions from reporting client and ownership information to bank supervisors and law enforcement authorities. The GOSA provides anti-money laundering training for bank employees, prosecutors, judges, customs officers and other government officials.

In 2003, the GOSA established an anti-money laundering unit in SAMA, and in 2005 the GOSA opened the Saudi Arabia Financial Investigation Unit (SA FIU) under the oversight of the Ministry of Interior. Saudi banks are required to have anti-money laundering units with specialized staff to work with SAMA, the SA FIU, and law enforcement authorities. All banks are also required to report any suspicious transactions in the form of an STR to the SA FIU. The SA FIU collects and analyzes STRs and other available information and makes referrals to the Bureau of Investigation and Prosecution, the Mabahith (the Saudi Intelligence Service), and the Public Security Agency for further investigation and prosecution. The SA FIU is staffed by officers from the Mabahith and SAMA. In September 2006, the SA FIU had its final on-site review by FinCEN, one of the Egmont co-sponsors, for possible Egmont membership in 2007.

Hawala transactions outside banks and licensed money changers are illegal in Saudi Arabia. Reportedly, some money laundering cases that SAMA has investigated in the past decade involved the hawala system. In order to help counteract the appeal of hawala, particularly to many of the approximately six million expatriates living in Saudi Arabia, Saudi banks have taken the initiative to create fast, efficient, high quality, and cost-effective fund transfer systems that have proven capable of attracting customers accustomed to using hawala. An important advantage for the authorities in combating potential money laundering and terrorist financing in this system is that the senders and recipients of fund transfers through this formal financial sector are clearly identified. In 2005, in an effort to further regulate the more than $16 billion in remittances that leave Saudi Arabia every year, in 2005 SAMA consolidated the eight largest money changers into a single bank, Bank Al-Bilad.

In late 2005, the GOSA enacted stricter regulations on the cross-border movement of money and precious metals. Money and gold in excess of $16,000 must be declared upon entry and exit from the country. While the regulations were effective immediately, Customs has not issued new declaration forms, and therefore cannot enforce the current regulation.

Contributions to charities in Saudi Arabia usually consist of Zakat, which refers to an Islamic religious duty with specified humanitarian purposes. According to a 2002 report to the United Nations Security Council, over the past decade al-Qaida and other jihadist organizations collected between $300 and $500 million; and the majority of those funds originated from Saudi charities and private donors. The 9/11 Commission Report noted that the GOSA failed to adequately supervise Islamic charities in the country. To help address this problem, in 2002 Saudi Arabia announced its intention to establish the High Charities Commission to oversee Saudi charities with foreign operations. In 2004, the GOSA issued guidelines for the High Charities Commission (also known as the National Commission for Relief and Charitable Work Abroad). As of October 2006, GOSA has stated it is reviewing the role of the High Charities Commission and its relationship to Sharia law. The High Charities Commission has not been formally established, and the GOSA has made no further announcement of structure, leadership or staffing.

As required by regulations in effect for over 20 years, domestic charities in Saudi Arabia are licensed, registered, audited, and supervised by the Ministry of Social Affairs. The Ministry has engaged outside accounting firms to perform annual audits of charities' books and has established an electronic database to track the operations of the charities. Banking rules implemented in 2003 that apply to all charities include stipulations which require charities to: only open accounts in Saudi Riyals; adhere to enhanced identification requirements; utilize one main consolidated account; and make payments only by checks payable to the first beneficiary and deposited in a Saudi bank. Regulations also forbid charities from using ATM and credit cards for charitable purposes, and making money transfers outside of Saudi Arabia. According to GOSA officials, these regulations apply to international charities as well and are being actively enforced.

Saudi Arabia participates in the activities of the FATF through its membership in the Gulf Cooperation Council (GCC). In July 2004, reporting on the results of a mutual evaluation conducted in September 2003, the FATF concluded that the framework of Saudi Arabia's anti-money laundering regime met FATF recommendations for combating money laundering and financing of terrorism, but noted the need to implement these new laws and regulations. Saudi Arabia also supported the creation of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body inaugurated in Bahrain in November 2004.

Saudi Arabia is working to implement UN Security Council resolutions on terrorist financing. SAMA circulates to all financial institutions under its supervision the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list. In August 2006, the United Nations Security Council Resolution 1267 Sanctions Committee designated the International Islamic Relief Organization's (IIRO) branches in Indonesia and the Philippines, as well as the Kingdom's Eastern Province branch's Director, Abdulhamid Al-Mujil. Saudi Arabia is able to administratively freeze and seize terrorist assets. Saudi Arabia is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime.

The Government of Saudi Arabia is moving to monitor and enforce its anti-money laundering and terrorist finance laws, regulations and guidelines. However, Saudi Arabia should formally establish the High Commission for Charities. As with many countries in this region, there is still an over-reliance on suspicious transaction reporting to generate money laundering investigations. Law enforcement agencies should take the initiative and proactively generate leads and investigations, and be able to follow the financial trails wherever they lead. Saudi Arabia's unwillingness to publicly disseminate statistics regarding money laundering prosecutions impedes the evaluation and design of

enhancements to the judicial aspects of its AML system. Charitable donations in the form of gold, precious stones and other gifts should be scrutinized. International charities should be made subject to the same government oversight as domestic charities, including the rules of both SAMA and the Charities Commission. Saudi Customs should issue cross-border currency declaration forms and enforce the reporting requirements. The GOSA should become a party to the UN International Convention for Suppression of the Financing of Terrorism.

## Senegal

Senegal is vulnerable to money laundering. Reportedly, most money laundering involves domestically-generated proceeds from corruption and embezzlement. Dakar's hot real-estate market is largely financed by cash, and ownership of properties is nontransparent. The building boom and high property prices suggest that an increasing amount of funds with an uncertain origin circulates in Senegal. Other areas of concern include: cash, gold and gems transiting Senegal's airport and porous borders; real estate investment in the Petite Cote south of Dakar; and trade-based money laundering centered in the region of Touba, a largely autonomous and unregulated free-trade zone under the jurisdiction of the Mouride religious authority. This latter region reportedly receives between 550 and 800 million dollars per year in funds repatriated by networks of Senegalese vendors abroad. There is some evidence of increasing criminal activity by foreigners, such as drug trafficking by Latin American groups and illegal immigrant trafficking involving Pakistanis.

Seventeen commercial banks operate alongside a thriving micro-credit sector. Western Union, Money Gram and Money Express, associated with banks, are ubiquitous, suggesting that, while informal remittance systems exist, they are not a large threat to the business of the licensed remitters. The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the countries in the West African Economic and Monetary Union (WAEMU or UEMOA): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal and Togo, all of which use the French-backed CFA franc (CFAF) currency, which is pegged to the euro. The Commission Bancaire, responsible for bank inspections, is based in Abidjan.

In 2004, Senegal became the first WAEMU country to enact the WAEMU Uniform Law on Money Laundering (the Uniform Law). The new legislation meets many international standards with respect to money laundering, but does not comply with all Financial Action Task Force (FATF) recommendations concerning politically-exposed persons, and lacks certain compliance provisions for nonfinancial institutions. The law does not deal with terrorist financing.

Senegal's Financial Intelligence Unit (FIU) became operational in August 2005. Since that date it has received 59 (11 in 2005 and 48 in 2006) suspicious declarations and has referred nine cases (three in 2005, six in 2006) to the Prosecutor General. All but two of the declarations have been made by banks. The other two came from Customs. Of the referrals, one concerns drug trafficking, one concerns diamond trafficking, one relates to tax fraud, and three are corruption related. No cases have concluded, although one arrest has been made. The FIU currently has a staff of 23, including six appointed members: the President of the FIU, who by law is chosen from the Ministry of Economy and Finance, and five others detailed from the Customs Service, the BCEAO, the Judicial Police, and the judiciary. The FIU also relies on liaison officers in relevant governmental institutions that can provide information relevant to the FIU's investigations. With French sponsorship, Senegal's FIU is a candidate for membership in the Egmont Group. Its candidacy is on hold pending the adoption of a terrorist financing law.

Official statistics regarding the prosecution of financial crimes are unavailable. There is one known conviction for money laundering since January 1, 2005. The conviction led to the confiscation of a private villa.

The BCEAO is working on a Directive against Terrorist Financing. If adopted, the member states would be directed to enact a law against terrorist financing, which most likely would be presented as a Uniform Law in the same manner as the AML law. Like the AML law, it is a penal law, and each national assembly must then enact enabling legislation to adopt the new terrorist finance law. In addition, the FATF-style regional body for the 15-member Economic Community of Western African States (ECOWAS), GIABA (African Anti-Money Laundering Inter-governmental Group) has drafted a uniform law, which it hopes to have enacted in all of its member states, not just the WAEMU states.

The UN 1267 Sanctions Committee consolidated list is circulated both by the FIU and by the BCEAO to commercial financial institutions. To date, no assets relating to terrorist entities have been identified. The WAEMU Council of Ministers issued a directive in September 2002 requiring banks to freeze assets of entities designated by the Sanctions Committee.

Senegal has entered into bilateral criminal mutual assistance agreements with France, Tunisia, Morocco, Mali, The Gambia, Guinea Bissau, and Cape Verde. Multilateral ECOWAS treaties deal with extradition and legal assistance. Under the Uniform Law, the FIU may share information freely with other FIUs in WAEMU. However, only Senegal and Niger have operational FIUs. The FIU has signed an MOU to exchange information with the FIUs of Belgium and Lebanon, and is working on other accords. In general, the Government of Senegal (GOS) has demonstrated its commitment and willingness to cooperate with United States law enforcement agencies. In the past the GOS has worked with INTERPOL, Spanish, and Italian authorities on international anticrime operations.

Senegal is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the 1999 UN International Convention for the Suppression of the Financing of Terrorism, and the Convention against Corruption. Senegal is listed as 70 out of 163 countries monitored in Transparency International's 2006 Corruption Perception Index.

Senegal has made considerable progress in establishing an operational FIU and raising the awareness of the threat of money laundering. However, a complicated political climate in advance of the 2007 elections, a generally nontransparent police and judiciary, and conflicting governmental interests in the banking sector threaten to retard any efforts to take this progress to the next level of actual prosecutions and convictions. Recent arrests of opposition politicians, journalists, and a corruption scandal that resulted in the early retirement, rather than prosecution, of the implicated judges, illustrate the weakness of the rule of law in Senegal.

The Government of Senegal should continue to work with its partners in WAEMU and ECOWAS to establish a comprehensive anti-money laundering and counterterrorist financing regime. Senegal should work on achieving transparency in its financial and real estate sectors. Senegal and the region should establish better control of cross-border currency transfers. Senegalese law enforcement and customs authorities should take the initiative to identify and investigate money laundering at the street level and informal economy. Senegal should pass an antiterrorist finance law.

## Serbia

Serbia is not a regional financial center. At the crossroads of Europe and on the major trade corridor known as the "Balkan route," Serbia confronts narcotics trafficking, smuggling of persons, drugs, weapons and pirated goods, money laundering, and other criminal activities. Serbia continues to be a significant black market for smuggled goods. Illegal proceeds are generated from drug trafficking, official corruption, tax evasion and organized crime, as well as other types of crimes. Proceeds from illegal activities are invested in all forms of real estate. Trade-based money laundering, in the form of over- and under-invoicing, is commonly used to launder money.

A significant volume of money flows to Cyprus, reportedly as the payment for goods and services. The records maintained by various government entities vary significantly on the volume and value of

imports from Cyprus. According to official statistics from the National Bank of Serbia, over $1 billion in payments in 2005, coded as being for goods and services, rank Cyprus among the top five exporters of goods or services to Serbia. The Serbian Statistical Office reflected imports from Cyprus of roughly $40 million in 2005. According to Government of the Republic of Serbia (GOS) officials, much of the difference is due to payments made to accounts in Cyprus for goods, such as Russian oil, that actually originate in a third jurisdiction.

Serbia's banking sector is more than 80 percent foreign-owned. There is no provision in the banking law that allows the establishment of offshore banks, shell companies or trusts. Reportedly, there is no evidence of any alternative remittance systems operating in the country. Nor, reportedly, is there evidence of financial institutions engaging in currency transactions involving international narcotics trafficking proceeds. Serbia has 14 designated free trade zones, three of which are in operation. The free trade zones were established to attract investment by providing tax-free areas to companies operating within them. These companies are subject to the same supervision as other businesses in the country.

As the result of a public referendum on May 21, 2006, the State Union of Serbia and Montenegro (SAM) was dissolved and Montenegro became an independent country. The GOS became the legacy member of the Council of Europe and the United Nations. As a result, all treaties and agreements signed by the State Union are now applicable to Serbia, including the1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. The GOS is a party to all 12 UN Conventions and Protocols dealing with terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism, although domestic implementation procedures do not provide the framework for full application. In December 2005, the GOS ratified the UN Convention against Corruption.

In September 2005, Serbia codified an expanded definition of money laundering in the Penal Code. This legislation gives police and prosecutors more flexibility to pursue money laundering charges, as the law broadens the scope of money laundering and aims to conform to international standards. The penalty for money laundering is a maximum of 10 years imprisonment. Under this law and attendant procedure, money laundering falls into the serious crime category and permits the use of Mutual Legal Assistance (MLA) procedures to obtain information from abroad.

On November 28, 2005, Serbia adopted a revised anti-money laundering law (AMLL), replacing the July 2002 Law on the Prevention of Money Laundering. The revised AMLL expands the number of entities required to collect certain information on all cash transactions over EUR 15,000 (approx. $19,500), or the dinar equivalent, and to file currency transaction reports (CTRs) for all such transactions exceeding this threshold to the financial intelligence unit (FIU). Suspicious transactions in any amount must be reported to the FIU. The law expands those sectors subject to reporting and record keeping requirements, adding attorneys, auditors, tax advisors and bank accountants, currency exchanges, insurance companies, casinos, securities brokers, dealers in high value goods and travel agents to those already required to comply with the AMLL provisions. Required records must be maintained for five years. These entities are protected with respect to their cooperation with law enforcement entities. The AMLL requires obligated entities and individuals to monitor customers' accounts when they have a suspicion of money laundering, in addition to reporting to the FIU. The AMLL also eliminates a previous provision limiting prosecution to crimes committed within Serbian territory. Significant improvement has been noted in financial institution compliance, i.e., gathering and keeping records on customers and transactions. The flow of information to the FIU has been steadily increasing, but not all entities are yet subject to implementing bylaws.

The Law on Foreign Exchange Operations, adopted in 2006, criminalizes the use of false or inflated invoices or documents to effect the transfer of funds out of the country. This law was enacted in part to counter the perceived problem of import-export fraud and money laundering. According to the law,

residents and nonresidents are obliged to declare to Customs authorities all currency (foreign or dinars), or securities in amounts exceeding EUR 5,000 being transported across the border.

The National Bank of Serbia (NBS) has supervisory authority over banks, currency exchanges, insurance and leasing companies. The NBS has issued regulations requiring banks to have compliance and know-your-customer (KYC) programs in place and to identify the beneficial owners of new accounts. In June 2006, the NBS expanded its customer identification and record keeping rules by adopting new regulations mandating enhanced due diligence procedures for certain high risk customers and politically exposed persons. Similar regulations are being developed for insurance companies. The Law on Banks includes a provision allowing the NBS to revoke a bank's license for activities related to, among other things, money laundering and terrorist financing. To date, the NBS has not used this revocation authority. The legal framework is in place, but the NBS currently lacks the expertise needed for effective bank supervision. It is building these capacities through training and staff development.

The Securities Commission (SC) supervises broker-dealers and investment funds. The Law on Investment Funds and the Law on Securities and Other Financial Instruments Market provide the SC with the authority to "examine" the source of investment capital during licensing procedures. The SC is also charged with monitoring its obligors' compliance with the AML Laws. Regulations to implement this authority are being developed.

The Administration for the Prevention of Money Laundering serves as Serbia's FIU. The revised AMLL elevates the status of the FIU to that of an administrative body under the Ministry of Finance from its previous status as a "sector" in that Ministry. This provides more autonomy for the agency to carry out its mandate, as well as additional resources. One important change is that the FIU now has its own line item operating budget. The FIU currently has 24 employees. In accordance with the revised AMLL, the FIU developed listings of suspicious activity red flags for banks, currency exchange offices, insurance companies, securities brokers and leasing companies. Other significant changes include the authority of the FIU to freeze transactions for a maximum of 72 hours. The FIU has signed memoranda of understanding (MOU) on the exchange of information with the NBS and Customs and is negotiating one with the Tax Administration.

The FIU received 279 suspicious transaction reports (STRs) in 2005 and 361 through September 1, 2006. Virtually all of the STRs received by the FIU have been filed by commercial banks. Currency exchange offices have filed only seven STRs since 2003, and none in either 2005 or 2006. Since its inception in 2003, the FIU has opened 240 cases, 74 based on the STRs it received and 166 based on CTRs or referrals from other entities; 103 cases were referred to either law enforcement or the prosecutor's office for further investigation. Since 2004, authorities filed 41 criminal charges against 48 persons for money laundering violations. The most common predicate crime is "abuse of office". Of this number, eighteen are currently under investigation, six were dismissed or terminated; fourteen were indicted; and two court decisions have been reached to date. One person has been acquitted and the other was convicted, but has appealed the verdict.

Serbia introduced a value-added tax (VAT) in 2005, and the full impact of refund fraud associated with the administration of the VAT is still not clear. Serbia's Tax Administration lacks the audit and investigative capacity or resources to adequately investigate the large number of suspicious transactions that are forwarded by Serbia's FIU. In addition, current tax law sets a low threshold for auditing purposes and has increased the burden on the Tax Administration. This creates a situation where criminals can spend and invest criminal proceeds freely with little fear of challenge by the tax authorities or other law enforcement agencies.

The difficulty of convicting a suspect of money laundering without a conviction for the predicate crime and the unwillingness of the courts to accept circumstantial evidence to support money laundering or tax evasion charges is hampering law enforcement and prosecutors in following the

movement and investment of illegal proceeds and effectively using the anti-money laundering laws. The Suppression of Organized Crime Service (SOCS) of the Ministry of Interior houses a new Anti-Money Laundering Section to better focus financial investigations.

In August 2005, the GOS established the Permanent Coordinating Group (PCG), an interagency working group originally tasked with developing an implementation plan for the recommendations from MONEYVAL's first-round evaluation in October 2003. A subgroup was tasked with drafting a new law to address the procedures needed to comply with UN Security Council resolutions regarding the freezing, seizing and confiscation of suspected terrorist assets, and to require reporting to the FIU of transactions suspected to be terrorist financing. The PCG meets intermittently as required for completing specific tasks. The government still needs better interagency coordination to improve information sharing, record keeping and statistics.

Under Serbian law, assets derived from criminal activity or suspected of involvement in the financing of terrorism can be confiscated upon conviction for an offense. The FIU is charged with enforcing the UNSCR 1267 provisions regarding suspected terrorist lists. A draft law on terrorist financing, now pending Parliamentary approval, will apply all provisions of the AML laws to terrorist financing and will implement a freezing mechanism based on UNSCR provisions. Although the FIU routinely provides the UN list of suspected terrorist organizations to the banking community, examination for suspect accounts have revealed no evidence of terrorist financing within the banking system and no evidence of alternative remittance systems. The SOCS, the Special Anti-Terrorist Unit (SAJ), and Gendarmarie, in the Ministry of Interior, are the law enforcement bodies responsible for planning and conducting the most complex antiterrorism operations. SOCS cooperates and shares information with its counterpart agencies in all of the countries bordering Serbia. Although Serbia has criminalized the financing of terrorism, the freezing, seizing and confiscation of assets of terrorists in accordance with UN Security Council resolutions still lacks a legal basis, pending enactment of the Anti-terrorism Finance legislation.

Serbia has no laws governing its cooperation with other governments related to narcotics, terrorism, or terrorist financing. Bases for cooperation include participation in Interpol, bilateral cooperation agreements, and agreements concerning international legal assistance. There are no laws at all governing the sharing of confiscated assets with other countries, nor is any legislation under consideration.

Serbia does not have a mutual legal assistance arrangement with the United States, but information exchange via a letter rogatory is standard. The 1902 extradition treaty between the Kingdom of Serbia and the United States remains in force. The GOS has bilateral agreements on mutual legal assistance with 31 countries. As a member of the Council of Europe, the GOS is an active member of the Council's MONEYVAL. In July 2003, the FIU became a member of the Egmont Group and actively participates in information exchanges with counterpart FIUs including FinCEN. The Serbian FIU has also signed information sharing memoranda of understanding (MOUs) with Macedonia, Romania, Belgium, Slovenia, Montenegro, Albania, Georgia, Ukraine, Bulgaria, Croatia, and Bosnia and Herzegovina.

Serbia should continue to work toward eliminating the abuses of office and culture of corruption that enables money laundering and financial crimes. Among the pending legal infrastructure necessary for Serbia to be fully compliant with international standards are laws providing for the liability of legal persons for money laundering and terrorist financing; regulations to apply all requirements of the Revised AML Law to covered nonbank financial institutions; legislation to establish a robust asset seizure and forfeiture regime; and legislation providing for the sharing of seized assets. Serbia also needs to enact and implement proposed legislation needed to comply with UN Security Council resolutions regarding the freezing, seizing and confiscation of suspected terrorist assets and require suspicions of terrorist financing to be reported to the FIU.

The National Bank and other supervisory bodies need training and additional staff. The GOS should enforce regulations pertaining to money service businesses and obligated nonfinancial business and professions. The supervisory scheme should be completed, and implementing regulations should be binding, for the insurance and securities sectors. On an operational level, law enforcement needs audit and investigative capacity in order to investigate the STRs that the FIU disseminates. Training is also required for prosecutors and judges. Rather than address specific tasks as an ad hoc group, the PCG should meet on a regular basis to discuss issues and projects, and work to improve interagency coordination in such areas as information sharing, record keeping and statistics.

## Seychelles

Seychelles is a not a major financial center. The existence of a developed offshore financial sector, however, makes the country vulnerable to money laundering. The Government of Seychelles (GOS), in efforts to diversify its economy beyond tourism, developed an offshore financial sector to increase foreign exchange earnings and actively markets itself as an offshore financial and business center that allows the registration of nonresident companies. As of September 2006, there were 31,000 registered international business companies (IBCs) and 157 trusts that pay no taxes in Seychelles, and are not subject to foreign exchange controls. The Seychelles International Business Authority (SIBA), a body with board members from both the government and the private sector, licenses and regulates offshore activities. The SIBA acts as the central agency for the registration for IBCs and trusts and regulates activities of the Seychelles International Trade Zone.

In addition to IBCs and trusts, Seychelles permits offshore insurance companies, mutual funds, and offshore banking. The GOS is currently in the process of establishing the Non-Bank Financial Services Authority, which will be responsible for regulating these sectors under the Mutual Funds Act, the Securities Act, and the Insurance Act. Three offshore insurance companies have been licensed: one for captive insurance and two for general insurance. Seychelles has one offshore bank to date: the Barclays Bank (Offshore Unit). The International Corporate Service Providers Act 2003, designed to regulate all activities of corporate and trustee service providers, entered into force in 2004.

In 1996, the GOS enacted the Anti-Money Laundering Act (AMLA), which criminalized the laundering of funds from all serious crimes, required covered financial institutions and individuals to report to the Central Bank transactions involving suspected cases of money laundering, and established safe harbor protection for individuals and institutions filing such reports. The AMLA also imposed record keeping and customer identification requirements for financial institutions, and provided for the forfeiture of the proceeds of crime. In October 2004, the International Monetary Fund (IMF) released a report on its 2002 financial sector assessment of the Seychelles. The IMF report noted deficiencies in the AMLA and practice, and recommended closing existing loopholes as well as updating the AMLA to reflect current international standards and best practices.

In May 2006, the Anti-Money Laundering Act 2006 came into force. This new legislation replaces the AMLA of 1996 and addresses many of the deficiencies cited by the IMF report. Under the new AMLA, money laundering controls, including the obligation to submit suspicious transaction reports (STRs), are applied to the same financial intermediaries as under the 1996 law, as well as nonbanking financial institutions, including exchange houses, stock brokerages, insurance agencies, lawyers, notaries, accountants, and estate agents. Offshore banks are also explicitly covered. Gaming operations, including internet gaming, are also obligated, but the law does not state explicitly that offshore gaming is covered in an identical manner. Currently, no offshore casinos or Internet gaming sites have been licensed to operate. There is no cross-border currency reporting requirement. The 2006 AMLA discusses record-keeping and institutional protocol requirements, sets a maximum delay of two working days to file a suspicious transaction report, criminalizes tipping off, and sets safe harbor provisions. The new law also requires the identification of beneficial owners, but leaves open

exceptions for "an existing and regular business relationship with a person who has already produced satisfactory evidence of identity"; for "an occasional transaction under R50,000" ($9,200); and in other cases "as may be prescribed".

Under the AMLA, anyone who engages directly or indirectly in a transaction involving money or other property (or who receives, possesses, conceals, disposes of, or brings into Seychelles any money or property) associated with a crime, knowing or having reasonable grounds to know that the money or property is derived from an illegal activity, is guilty of money laundering. In addition, anyone who aids, abets, procures, or conspires with another person to commit the crime, while knowing, or having reasonable grounds for knowing that the money was derived from an illegal activity, is likewise guilty of money laundering. Money laundering is sanctioned by imprisonment for up to fifteen years and/or R3,000,000 ($554,500) in penalties. While there have been about thirty investigations, there have been no arrests or prosecutions for money laundering or terrorist financing since January 1, 2003. This is problematic.

The Financial Institutions Act of 2004, imposes more stringent rules on banking operations. The law, which was drafted in consultation with the International Monetary Fund, aims to ensure greater transparency in financial transactions and regulating the financial activities of both domestic and offshore banks in line with international standards. One provision of the law requires that banks change their auditors every five years. Auditors must notify the Central Bank if they uncover criminal activity such as money laundering in the course of an audit.

The Central Bank of the Seychelles has been acting as the financial intelligence unit (FIU) for the Seychelles in that it receives and analyzes suspicious activity reports and disseminates them to the competent authorities. It cannot freeze or confiscate property, but can get a court order to effect an asset freeze. The courts have the authority to freeze or confiscate money or property. Section 16 of the 2006 AMLA provides for the creation of an FIU within the Central Bank. This FIU will receive reports, have access to information in public or governmental databases and may request information from reporting entities, supervisory bodies and law enforcement agencies. The FIU will analyze the information and disseminate information to the appropriate entities if the FIU deduces that there is unlawful activity. The law provides for the FIU to have a proactive targeting section that will research trends and developments in not only money laundering, but also terrorism financing. The FIU will also perform examinations of the reporting entities and, in concert with regulators, issue guidance related to customer identification, identification of suspicious transactions, and record keeping and reporting obligations. The law provides for the possibility that the FIU would in the future perform training related to these matters. Authorities are also discussing the establishment of an AML interagency Task Force that would incorporate the FIU, Police, Customs, Immigration, and Internal Affairs.

Judges in the Supreme Court have the authority to restrain a target from moving or disposing of his or her assets, and will do so if a law enforcement officer requests it, provided that the Court is "satisfied that there are reasonable grounds" for doing so. The Court also has the authority to determine the length of time for the restraint order and the disposition of assets, should it become necessary. Should the target violate the order, he or she becomes subject to financial penalties. Law enforcement may seize property subject to this order to prevent property from being disposed of or moved contrary to the order. The Court also is authorized to order the forfeiture of assets.

In 2004, the GOS enacted the Prevention of Terrorism Bill. The legislation specifically recognizes the government's authority to identify, freeze, and seize terrorist finance-related assets. The 2006 AMLA also makes the legal requirements applicable to money laundering applicable to suspected terrorist financing transactions. Assets used in the commission of a terrorist act can be seized and legitimate businesses can be seized if used to launder drug money, support terrorist activity, or support other criminal activities. Both civil and criminal forfeiture are allowed under current legislation.

The Mutual Assistance in Criminal Matters Act of 1995 empowers the Seychelles Central Authority to provide assistance in connection with a request to conduct searches and seizures relating to serious offenses under the law of the requesting state. The Prevention of Terrorism Act extends the authority of the GOS to include the freezing and seizing of terrorism-related assets upon the request of a foreign state. To date, no such assets have been identified, frozen, or seized.

The Government of Seychelles is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. Seychelles underwent a mutual evaluation review conducted by ESAAMLG in November 2006. The Seychelles is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. Seychelles circulates to relevant authorities the updated lists of names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224.

Seychelles should expand its anti-money laundering efforts by prohibiting bearer shares and clarifying the new legislation regarding the complete identification of beneficial owners. Seychelles should also clarify the legislation to state explicitly that all offshore activity is covered in the same manner and to the same degree as onshore. Seychelles should continue to work towards the establishment of its FIU, ensuring that it develops with a degree of independence and autonomy from its parent agency, the Central Bank. The GOS should also consider codifying the ability to freeze assets rather than issuing restraining orders, and develop a currency reporting requirement for entry into its borders. Seychelles should continue to participate in ESAAMLG, and when the mutual evaluation report is finalized, work to address any further deficiencies outlined therein.

## Sierra Leone

Sierra Leone has a cash-based economy and is not a regional financial center. Government of Sierra Leone (GOSL) officials have reportedly stated that money laundering activities are pervasive, particularly in the diamond sector. Although there have been some attempts at tighter regulation, monitoring, and enforcement, in some areas significant diamond smuggling still exists. Loose oversight of financial institutions, weak regulations, pervasive corruption, and a widespread informal money-exchange and remittance system also work to create an atmosphere conducive to money laundering.

The President signed the Anti-Money Laundering Act (AMLA) in July 2005. The AMLA incorporates international standards, including setting safe harbor provisions, know your customer and identification of beneficial owner requirements, as well as mandatory five-year record-keeping. There is a currency reporting requirement for deposits larger than 25 million leones (approximately $8,330) and no minimum for suspicious transaction reporting. The law requires that international financial transfers over $10,000 go through formal financial institution channels. The AMLA calls for cross-border currency reporting requirements for cash or securities in excess of $10,000. The law designates the Governor of the Bank of Sierra Leone as the national Anti-Money Laundering Authority.

The AMLA applies to Sierra Leone's financial sector institutions such as depository and credit institutions, money transmission and remittance service centers, insurance brokers, investment banks and businesses including securities and stock brokerage houses, and currency exchange houses. Designated nonfinancial businesses and professions such as casinos, realtors, dealers in precious metals and stones, notaries, legal practitioners, and accountants are also included.

A financial intelligence unit (FIU) exists but lacks the capacity to effectively monitor and regulate financial institution operations. Law enforcement and customs have limited resources and lack

training. There have reportedly been a small number of arrests under the AMLA but no convictions due to lack of capacity by police investigators and judicial authorities.

The AMLA empowers the courts to freeze assets for seventy-two hours if a suspect has been charged with money laundering or if a charge is imminent. Upon a conviction for money laundering, all property is treated as illicit proceeds and can be forfeited unless the defendant can prove that possession of some or all of the property was obtained through legal means. The AMLA also provides for mutual assistance and international cooperation.

In July 2006, the Bank of Sierra Leone hosted a United Nations Office on Drugs and Crime and Group for Action Against Money Laundering (GIABA)-sponsored training workshop on strategy development for anti-money laundering and combating financing of terrorism. Workshop participants recommended that the Bank of Sierra Leone draft a national strategy and regulations for the operations of the FIU, establish a system for the receipt, analysis, and dissemination of financial disclosures, and develop a formal system to report suspicious financial transactions to the FIU.

Workshop participants also recommended creating a special unit comprised of two staff from the police's organized crime unit and two from the counterterrorism unit to deal with issues pertaining to anti-money laundering issues. They also recommended creating protocols to improve the exchange of information between government offices, including the Attorney General's Office, Police, National Revenue Authority, and Anti-Corruption Commission.

Sierra Leone is member of GIABA. It is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Sierra Leone is a party to the UN Convention against Corruption. Sierra Leone is listed 148 of 162 countries monitored in Transparency International's 2006 Corruption Perception Index.

Although the Government of Sierra Leone has passed anti-money laundering legislation, it remains to be effectively implemented or harmonized with other legislation relating to anti-money laundering and combating financing of terrorism, including the Anti-Corruption Act, National Drug Control Act, and Anti-Terrorism Act. The GOSL should ensure its antiterrorist finance countermeasures adhere to world standards, including the regular distribution to financial institutions of the UNSCR 1267 Sanctions Committee's consolidated list. The GOSL must increase the level of awareness of money laundering issues and allocate the necessary human, technical, and financial resources. Sierra Leone should continue its efforts to counter the smuggling of diamonds. Sierra Leone should take steps to combat corruption at all levels of commerce and government. It needs to ratify the UN Convention against Transnational Organized Crime.

## Singapore

As a significant international financial and investment center and, in particular, as a major offshore financial center, Singapore is vulnerable to potential money launderers. Bank secrecy laws and the lack of routine currency reporting requirements make Singapore an attractive destination for drug traffickers, transnational criminals, terrorist organizations and their supporters seeking to launder money, as well as for flight capital.

Structural gaps remain in financial regulation that may hamper efforts to control these crimes. To address some of these deficiencies, Singapore is beginning to map out legal and regulatory changes to implement the Financial Action Task Force's (FATF) revised recommendations on anti-money laundering (AML) and countering the financing of terrorism (CFT).

Singapore amended the Corruption, Drug Trafficking, and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) in May 2006 to add 108 new categories to its "Schedule of Serious Offenses."

The CDSA criminalizes the laundering of proceeds from narcotics transactions and other predicate offenses, including ones committed overseas that would be serious offenses if they had been committed in Singapore. Included among the new offenses are crimes associated with terrorist financing, illicit arms trafficking, counterfeiting and piracy of products, environmental crime, computer crime, insider trading, and rigging in commodities and securities markets. With an eye on Singapore's two new multibillion-dollar casinos slated to be operational in 2009, the list also addresses a number of gambling-related crimes. However, tax and fiscal offenses are still absent from the expanded list.

Singapore has a sizeable offshore financial sector. As of September 2006, there were 109 commercial banks in operation, including five local and 24 foreign-owned full banks, 45 offshore banks, and 35 wholesale banks. All offshore and wholesale banks are foreign-owned. Singapore does not permit shell banks in either the domestic or offshore sectors. The Monetary Authority of Singapore (MAS), a semi-autonomous entity under the Prime Minister's Office, serves as Singapore's central bank and financial sector regulator, particularly with respect to Singapore's AML/CFT efforts. MAS performs extensive prudential and regulatory checks on all applications for banking licenses, including whether banks are under adequate home country banking supervision. Banks must have clearly identified directors. Unlicensed banking transactions are illegal.

Singapore has increasingly become a center for offshore private banking and asset management. Total assets under management in Singapore grew 26 percent between 2004 and 2005 to $450 billion, according to MAS. Private wealth managers estimate that total private banking and asset management funds increased nearly 300 percent between 1998 and 2004.

Beginning in 2000, MAS began issuing a series of regulatory guidelines ("Notices") requiring banks to apply "know your customer" standards, adopt internal policies for staff compliance and cooperate with Singapore enforcement agencies on money laundering cases. Similar guidelines exist for securities dealers and other financial service providers. Banks must obtain documentation such as passports or identity cards from all personal customers to verify names, permanent contact addresses, dates of births and nationalities, and to check the bona fides of company customers. The regulations specifically require that financial institutions obtain evidence of the identity of the beneficial owners of offshore companies or trusts. They also mandate specific record-keeping and reporting requirements, outline examples of suspicious transactions that should prompt reporting, and establish mandatory intra-company point-of-contact and staff training requirements. Similar guidelines and notices exist for finance companies, merchant banks, life insurers, brokers, securities dealers, investment advisors, futures brokers and advisors, trust companies, approved trustees, and money changers and remitters.

Singapore is in the process of revising its AML/CFT regulations for banks and other financial institutions. The relevant Notices should further align certain parts of Singapore's AML/CFT regime more closely with FATF recommendations. Among the proposed regulations are new provisions that would proscribe banks from entering into, or continuing, correspondent banking relationships with shell banks; require originator information on cross-border wire transfers; clarify procedures for customer due diligence (CDD), including adoption of a risk-based approach; and mandate enhanced CDD for foreign politically exposed persons. Terrorist financing activities will also be addressed in the Notices for the first time. As part of this process, MAS issued for public comments draft regulations for banks in January 2005. In August 2006, it issued for public comments revised draft regulations for banks and new draft regulations for other financial institutions. Singapore is also considering regulations governing designated nonfinancial businesses and professions to bring them into conformity with FATF recommendations.

In addition to banks that offer trust, nominee, and fiduciary accounts, Singapore has 12 trust companies. All banks and trust companies, whether domestic or offshore, are subject to the same

regulation, record-keeping, and reporting requirements, including for money laundering and suspicious transactions. In August 2005, Singapore introduced regulations under the new Trust Companies Act (enacted in January 2005 to replace the Singapore Trustees Act) that mandated licensing of trust companies and MAS approval for appointments of managers and directors. In August 2006, MAS issued for public comments draft regulations that would require approved trustees and trust companies to complete all mandated CDD procedures before they could establish relations with customers. Other financial institutions are allowed to establish relations with customers before completing all CDD-related measures.

Singapore amended its Moneylenders Act in April 2006 to require moneylenders under investigation to provide relevant information or documents. The Act imposes new penalties for giving false or misleading information and for obstructing entry and inspection of suspected premises.

In April 2005, Singapore lifted its ban on casinos, paving the way for development of two integrated resorts scheduled to open in 2009. Combined total investment in the resorts is estimated to exceed $5 billion. In June 2006, Singapore implemented the Casino Control Act. The Act establishes the Casino Regulatory Authority of Singapore, which will administer the system of controls and procedures for casino operators, including certain cash reporting requirements. Internet gaming sites are illegal in Singapore.

Any person who wishes to engage in for-profit business in Singapore, whether local or foreign, must register under the Companies Act. Every Singapore-incorporated company is required to have at least two directors, one of whom must be a resident in Singapore, and one or more company secretaries who must be resident in Singapore. There is no nationality requirement. A company incorporated in Singapore has the same status and powers as a natural person. Bearer shares are not permitted.

Financial institutions must report suspicious transactions and positively identify customers engaging in large currency transactions and are required to maintain adequate records. However, there is no systematic reporting of large currency transactions. There are no reporting requirements on amounts of currency brought into or taken out of Singapore. Singapore is considering legal changes that would allow for implementation of FATF Special Recommendation Nine, which requires either a declaration or disclosure system for monitoring cross-border movement of currency and bearer negotiable instruments.

The Singapore Police's Suspicious Transaction Reporting Office (STRO) has served as the country's Financial Intelligence Unit (FIU) since January 2000. Procedural regulations and bank secrecy laws limit STRO's ability to provide information relating to financial crimes. In December 2004, STRO concluded a Memorandum of Understanding (MOU) concerning the exchange of financial intelligence with its U.S. counterpart, FinCEN. STRO has also signed MOUs with counterparts in Australia, Belgium, Brazil, Canada, Greece, Hong Kong, Italy, Japan and Mexico. To improve its suspicious transaction reporting, STRO has developed a computerized system to allow electronic online submission of STRs, as well as the dissemination of AML/CFT material. It plans to encourage all financial institutions and relevant professions to participate in this system.

Singapore is an important participant in the regional effort to stop terrorist financing in Southeast Asia. The Terrorism (Suppression of Financing) Act that took effect January 29, 2003, criminalizes terrorist financing, although the provisions of the Act are actually much broader. In addition to making it a criminal offense to deal with terrorist property (including financial assets), the Act criminalizes the provision or collection of any property (including financial assets) with the intention that the property be used (or having reasonable grounds to believe that the property will be used) to commit any terrorist act or for various terrorist purposes. The Act also provides that any person in Singapore, and every citizen of Singapore outside Singapore, who has information about any transaction or proposed transaction in respect of terrorist property, or who has information that he/she believes might be of

material assistance in preventing a terrorism financing offense, must immediately inform the police. The Act gives the authorities the power to freeze and seize terrorist assets.

The International Monetary Fund/World Bank assessment of Singapore's financial sector published in April 2004 concluded that, because it is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the country imposes few restrictions on intergovernmental terrorist financing-related mutual legal assistance even in the absence of a Mutual Legal Assistance Treaty. However, the IMF urged Singapore to improve its mutual legal assistance for other offenses, noting serious limitations on assistance through the provision of bank records, search and seizure of evidence, restraints on the proceeds of crime, and the enforcement of foreign confiscation orders.

Based on regulations issued in 2002, MAS has broad powers to direct financial institutions to comply with international obligations related to terrorist financing obligations. The regulations bar banks and financial institutions from providing resources and services of any kind that will benefit terrorists or terrorist financing. Financial institutions must notify the MAS immediately if they have in their possession, custody or control any property belonging to designated terrorists or any information on transactions involving terrorists' funds. The regulations apply to all branches and offices of any financial institutions incorporated in Singapore or incorporated outside of Singapore, but located in Singapore. The regulations are periodically updated to include names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list.

Singapore's approximately 600,000 foreign guest workers are the main users of alternative remittance systems. As of September 2006, there were 395 money-changers and 95 remittance agents. All must be licensed and are subject to the Money-Changing and Remittance Businesses Act (MCRBA), which includes requirements for record-keeping and the filing of suspicious transaction reports. Firms must submit a financial statement every three months and report the largest amount transmitted on a single day. They must also provide information concerning their business and overseas partners. Unlicensed informal networks, such as hawala, are illegal. In August 2005, Singapore amended the MCRBA to apply certain AML/CFT regulations to remittance licensees and money-changers engaged in inward remittance transactions. The Act eliminated sole proprietorships and required all remittance agents to incorporate under the Companies Act with a minimum paid-up capital of S$100,000 (approximately $60,000). In August 2006, MAS issued for public comments draft regulations that would require licensees to establish the identity of all customers; currently, no such identification is mandatory for transactions in aggregate of up to S$5,000 (approximately US$3,000). MAS would also be required to approve any non face-to-face transactions.

Singapore has five free trade zones (FTZs), four for seaborne cargo and one for airfreight, regulated under the Free Trade Zone Act. The FTZs may be used for storage, repackaging of import and export cargo, assembly and other manufacturing activities approved by the Director General of Customs in conjunction with the Ministry of Finance.

Charities in Singapore are subject to extensive government regulation, including close oversight and reporting requirements, and restrictions that limit the amount of funding that can be transferred out of Singapore. Singapore had a total of 1,807 registered charities as of December 2005. All charities must register with the Commissioner of Charities which, since September 1, 2006, has reported to the Minister for Community Development, Youth and Sports instead of the Minister for Finance. Charities must submit governing documents outlining their objectives and particulars of all trustees. The Commissioner of Charities has the power to investigate charities, search and seize records, restrict the transactions into which the charity can enter, suspend staff or trustees, and/or establish a scheme for the administration of the charity. Charities must keep detailed accounting records and retain them for at least seven years.

Singapore will implement tighter regulations under the Income Tax Act governing public fund-raising by charities, effective January 1, 2007. Charities authorized to receive tax-deductible donations will be

required to disclose the amount of funds raised in excess of S$1 million (approximately $600,000), expenses incurred, and planned use of funds. Under the Charities (Fund-raising Appeals for Foreign Charitable Purposes) Regulations 1994, any charity or person that wishes to conduct or participate in any fund-raising for any foreign charitable purpose must apply for a permit. The applicant must demonstrate that at least 80 percent of the funds raised will be used in Singapore, although the Commissioner of Charities has discretion to allow for a lower percentage. Permit holders are subject to additional record-keeping and reporting requirements, including details on every item of expenditure, amounts transferred to persons outside Singapore, and names of recipients. The government issued 36 permits in 2005 related to fund raising for foreign charitable purposes. There are no restrictions or direct reporting requirements on foreign donations to charities in Singapore.

To regulate law enforcement cooperation and facilitate information exchange, Singapore enacted the Mutual Assistance in Criminal Matters Act (MACMA) in March 2000. Parliament amended the MACMA in February 2006 to allow the government to respond to requests for assistance even in the absence of a bilateral treaty, MOU or other agreement with Singapore. The MACMA provides for international cooperation on any of the 292 predicate "serious offenses" listed under the CDSA. In November 2000, Singapore and the United States signed the Agreement Concerning the Investigation of Drug Trafficking Offenses and Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking (Drug Designation Agreement or DDA). This was the first agreement concluded pursuant to the MACMA. The DDA, which came into force in early 2001, facilitates the exchange of banking and corporate information on drug money laundering suspects and targets, including access to bank records. It also entails reciprocal honoring of seizure/forfeiture warrants. This agreement applies only to narcotics cases, and does not cover non-narcotics-related money laundering, terrorist financing, or financial fraud.

In May 2003, Singapore issued a regulation pursuant to the MACMA and the Terrorism Act that enables the government to provide legal assistance to the United States and the United Kingdom in matters related to terrorism financing offenses. Singapore concluded mutual legal assistance agreements with Hong Kong in 2003 and with India in 2005. Singapore is a party to the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters along with Malaysia, Vietnam, Brunei. Cambodia, Indonesia, Laos, the Philippines, Thailand, and Burma. The treaty will come into effect after ratification by the respective governments. Singapore, Malaysia, Vietnam and Brunei have ratified thus far.

In addition to the UN International Convention for the Suppression of the Financing of Terrorism, Singapore is also party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. In addition to FATF, Singapore is a member of the Asia/Pacific Group on Money Laundering, the Egmont Group, and the Offshore Group of Banking Supervisors. Singapore hosted the June 2005 Plenary meeting of the FATF, the first time a FATF Plenary was held in Southeast Asia. FATF is slated to review Singapore's AML/CFT regime, most likely in 2007.

Singapore should continue close monitoring of its domestic and offshore financial sectors. As a major financial center, it should also adopt measures to regulate and monitor large currency and bearer negotiable instrument movements into and out of the country, in line with FATF Special Recommendation Nine, adopted in October 2004, that mandates countries implement measures such as declaration systems in order to detect cross-border currency smuggling. Singapore should add tax and fiscal offenses to its schedule of serious offenses.

The conclusion of broad mutual legal assistance agreements is also important to further Singapore's ability to work internationally to counter money laundering and terrorist financing. Singapore should lift its rigid bank secrecy restrictions to enhance its law enforcement cooperation in areas such as information sharing and to conform to international standards and best practices.

## Slovak Republic

Slovakia is not an important regional financial center. The geographic, economic, and legal conditions that shape the money laundering environment in Slovakia are typical of those in other Central European transition economies. Slovakia's location along the major lines of communication connecting Western, Eastern, and Southeastern Europe makes it a transit country for smuggling and trafficking in narcotics, mineral oils, and people. Organized crime activity and the opportunities to use gray market channels also lead to a favorable money laundering environment. Financial crimes such as fraud, tax evasion, embezzlement, and illegal business activity have been quite problematic for Slovak authorities.

In response to these problems, Slovakia has gradually strengthened the financial provisions of its criminal and civil codes through a series of amendments since 2000, which have resulted in an increased number of money laundering prosecutions. In 2006 a new Confiscation Law came into effect, strengthening the government's ability to seize assets gained through criminal activity. However, international monitors have suggested that the new law still contains significant loopholes. Despite a slight decline in staff resources, Slovakia's financial intelligence unit (FIU) and regional financial police have continued to increase filings, inspections, and the number of cases forwarded for prosecution.

Slovakia's original anti-money laundering legislation, Act No. 249/1994 (later amended by Act No. 58/1996) came into effect in 1994. Article 252 of the Slovak Criminal Code, Legalization of Proceeds from Criminal Activity, came into force at the same time. These measures criminalize money laundering for all serious crimes, and impose customer identification, record keeping, and suspicious transaction reporting requirements on banks. A money laundering conviction does not require a conviction for the predicate offense, and a predicate offense does not have to occur in Slovakia to be considered as such. The failure of a covered entity to report a suspicious transaction and "tipping off" are criminal offenses.

As a result of amendments made to the Slovak Civil Code in 2001, all banks in Slovakia were ordered to stop offering anonymous accounts. All existing owners of anonymous accounts were required to disclose their identity to the bank and to close the anonymous account by December 31, 2003. Owners of accounts that were not closed may withdraw money for an additional three-year non-interest-bearing grace period. However, funds remaining after January 1, 2007 will be confiscated and deposited in a fund for the administration of the Ministry of Finance, where they will be available for collection by the account holder for another five years. As of January 1, 2007, bearer passbook accounts will cease to exist.

Act No. 367/2000, On Protection against the Legalization of Proceeds from Criminal Activities, which came into force in January 2001, replaces the standard for suspicious transactions with an expanded definition of unusual business activity. According to this modified definition, an unusual business activity is any transaction that could result in the legalization of income, the source of which is suspected to be criminal. Such transactions include the attempted disposal of income or property with the knowledge or suspicion that it was acquired through criminal activity in Slovakia or a third country. Designated transactions also include the acquisition, possession, or use of real estate, moveable property, securities, money, or any other property with monetary value, for the purpose of concealing or disguising its ownership. However, the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) sent a team to perform a third-round mutual evaluation in May 2005; the resulting September 2006 Mutual Evaluation Report (MER) called for guidelines for each sector, noting that some sectors, such as gaming, do not have an understanding of what "unusual" is for that sector. The National Bank of Slovakia (NBS) or the Financial Market Authority (FMA), in addition to the Financial Police, have supervisory authority over the various financial institutions.

Act No. 367/2000 also expands the list of entities subject to reporting requirements to include foreign bank subsidiaries, the Slovak Export-Import Bank, nonbank financial institutions such as casinos, post offices, brokers, stock exchanges, commodity exchanges, securities markets, asset management companies, insurance companies, real estate companies, tax advisors, auditors, credit unions, leasing firms, auctioneers, foreign exchange houses, and pawnshops, all of which have been particularly susceptible to money laundering. The 2005 MONEYVAL MER stated that there was generally no reporting on the part of the designated nonfinancial business and professions (DNFBP), and that casinos and exchange houses had not reported at all. The Slovakian FIU estimated that out of approximately 100,000 obliged entities, only the banks and insurance companies have reported regularly, and the securities sector has produced a small number of reports. It is unclear whether the reporting obligations are understood by all the covered entities. Non profit organizations are generally exempt from reporting requirements.

As recommended in 2001 by a previous MONEYVAL (then called PC-R-EV) team in its second-round evaluation of Slovakia, the Government of Slovakia (GOS) amended Act No. 367/2000 in order to address shortcomings of the original legislation, and in order to comply with European Directive 2001/97/EC. As a result, Slovakian legislation is now in full harmony with the Second European Union (EU) Directive. The FATF's 2002-3 Annual Report stated that the amended legislation provided a "basically sound preventive legal structure." However, the recent MONEYVAL MER noted that there was no apparent national strategy and an absence of leadership in the overall national fight against money laundering and terrorist financing.

Amendments to Act No. 367/2000 in 2002 further extend reporting requirements to: antique, art, and collectible brokers; dealers in precious metals or stones, or other high-value goods; legal advisors; consultants; securities dealers; foundations; financial managers and consultants; and accounting services. Covered persons are required to identify all customers, including legal entities, if they find that the customers prepared or conducted transactions deemed to be suspicious, or if a sum or related sums exceeding approximately $19,000 within a 12-month period is involved. Insurance sellers must identify all clients whose premium exceeds approximately $1,200 in a year or whose one-time premium exceeds approximately $3,200. Casinos are obligated to identify all customers. Transactions may be delayed by the covered entities up to 48 hours, with another 24-hour extension allowed if authorized by the Financial Police. If the suspicion turns out to be unfounded, the state assumes the burden of compensation for losses stemming from the delay.

As a result of these modifications, money laundering convictions under Article 252 of the Criminal Code have increased gradually in recent years, with 33 confirmed cases between 2002-2005. Detailed statistics on money laundering convictions are not available, but, according to the financial police, auto theft is the most commonly prosecuted money laundering offense. There were no autonomous cases of money laundering convictions, since the FIU and regional financial police tend to forward for prosecution money laundering cases that are tied with broader organized crime activities. Corporate liability for money laundering is still inapplicable in Slovakia.

Slovak law is less than effective regarding the beneficial ownership of legal persons. The 2005 MONEYVAL MER stated that "Slovakian law does not require adequate transparency concerning beneficial ownership and control of legal persons." The law does not mandate identification on the Commercial Register for beneficial owners of a company purchasing or holding shares in another registered company, and information is unavailable for foreign companies registered in Slovakia. According to the MER, corporate liability is inapplicable under Slovakian law. There is no broad requirement to give any special attention to business relationships or transactions with legal or actual persons from countries not applying, or insufficiently applying, the FATF recommendations.

Spravodasjaká Jednotka Financnej Policie, was established on November 1, 1996, as a law enforcement style financial intelligence unit within the Police. Under a 2005 police reorganization, the

FIU, which had been a department within the Financial Police, was downgraded to one of eight divisions of the Bureau of Organized Crime. As a result, it is no longer headed at the director level, and has seen its numbers of staff decrease. The MONEYVAL team questioned the degree of autonomy and operational independence of the FIU since the change.

The FIU, or the Office to Fight Organized Crime (OFOC), focuses on all forms of organized crime, including narcotics, money laundering, human trafficking, and prostitution. The OFOC has four regional units of financial police, each responsible for a different part of Slovakia (Bratislava, Eastern Slovakia, Western Slovakia, and Central Slovakia), and four substantive units: the unusual business transactions unit, the obliged entities supervision unit, the unit for international cooperation and the unit for property checks. The FIU has jurisdictional responsibility over money laundering violations, receives and evaluates suspicious transaction reports (STRs), and collects additional information to establish the suspicion of money laundering. If justified, the unit forwards the case to one of the regional financial police units. All supervisory authorities must inform the FIU of any violation immediately upon discovery. Once enough information has been obtained to warrant suspicion that a criminal offense has occurred, the FIU takes appropriate measures, including asking a financial institution or bank to delay business or a financial transaction for 48 hours; however, the decision to delay transactions comes at the discretion of the financial institution and authorities acknowledge that transactions are rarely delayed. The FIU can also submit the case to the state prosecutor's office for investigation and prosecution. The MONEYVAL team found that the FIU's powers and duties were not clearly defined in legislation and not made distinct from other police powers and duties.

In 2005, the FIU received 1,273 reports alleging unusual financial transactions worth $341 million. It submitted 16 proposals for criminal prosecution (including six from previous years) with a value of $612 million and 341 proposals for tax prosecution (including 137 from previous years). In addition, the Financial Police regional units submitted 159 proposals for criminal prosecutions. In 2005, the OFOC conducted or started 97 on-site inspections of "obliged persons" and levied penalties in 36 cases with a total value of $143,000. Most criminal prosecution cases involved credit fraud. Most tax prosecution and on-site inspections uncovered abuse of Slovakia's value added tax system by local business owners.

Through the first ten months of 2006, the FIU received 1,158 reports with a total value of $315,000. Eight of these cases were submitted for prosecution, plus two outstanding cases from 2005. Financial Police regional units have submitted a further 177 cases for prosecution. A growing number of these cases involve organized groups transferring funds from neighboring countries (primarily Ukraine and Hungary) to Slovakia. The OFOC has carried out 68 on-site inspections during this timeframe, resulting in fines with a total value of $45,000.

The OFOC also has a supervisory role. Under section 10 of the AML law, the FIU has supervisory duty over the implementation of AML measures in financial institutions, and to this end, inspects these institutions. It also has sole supervisory authority over designated nonfinancial covered entities. The FIU has six officers in this unit, exercising supervisory responsibility over 100,000 institutions.

The Public Prosecutor Service is independent from executive power and supervises criminal prosecution measures performed by police and investigators. According to the MONEYVAL team, there is some cooperation and coordination taking place at the working level, but overall, this is a weakness in Slovakia's AML regime. The team also concluded that law enforcement is empowered, but needs more training, as well as policy and practical guidance, to ensure proactive financial investigations as well as to generate more cases and obtain convictions and confiscation orders.

In 2003, a law amending and supplementing the Criminal Procedure Code and Criminal Code entered into force. The amendment strengthens the competencies of law enforcement by granting investigators the authority to conduct sting operations and introduces provisions regarding corporate criminal liability. In addition, crown witnesses (a criminal who voluntarily opts to cooperate with law

enforcement bodies) are now protected by the law and can be granted immunity or receive a shortened sentence. This rule does not apply to those that organized or instigated the crime. To clarify ambiguities related to *inter alia* seizure and confiscation of proceeds, Slovakia amended both the Criminal Procedure Code and the Criminal Code in late 2005. The new law provides for mandatory forfeiture of proceeds of crime. It does not, however, allow for forfeiture from third party beneficiaries, and there are some concerns about the legal structure of the asset freezing and seizure regime to ensure that all indirect proceeds may be liable for confiscation. Shortly after the law entered into force on January 1, 2006, police officers involved with criminal investigations, as well as prosecutors and judges, were trained in substantive provisions of the new laws. The new laws also provides for specific sentencing guidelines for crimes, including 2-20 years for legalization of proceeds from criminal activity, and 2-8 years for not reporting unusual business transactions by obliged persons. No criminal prosecutions under the new law have been completed as of yet, though several have been forwarded by the FIU this year.

The Public Prosecutor Service also provides orders for the seizure of accounts within the pre-trial proceedings stage, and can order the use of information technology for enhanced investigations under Criminal Procedure Code Articles 79c,88 and 88e. There is also a Special Prosecutor Office and a Special Court, established by Act 258/2003 and which began operations on September 1, 2004. Act 258/2003 amends the Criminal Procedure Code to give this new Special Prosecutor jurisdiction over public officials, but also over the general public, for corruption; establishing, plotting, and supporting criminal and terrorist groups; extremely serious criminal offenses including those committed with a terrorist group; and economic criminal offense in excess of a designated threshold. Some money laundering cases have met these parameters and have been adjudicated by the Special Prosecutor's Office.

On June 23, 2005, Parliament approved the Law on Proving the Origin of Property, which came into force on September 1, 2005. According to the law, an undocumented increase in property exceeding an amount 200 times the minimum monthly wage would be scrutinized and could be considered illegal. Anyone who has suspicions that property that may have been acquired illegally may report it to the police. The police are then obliged to investigate the allegations, ultimately reporting to the Office of the Attorney General if findings are conclusive. The Attorney General's Office may then order the property to be confiscated. Despite its approval, the new law was still controversial, and its implementation was frozen by the Constitutional Courts on October 6, 2005. The Constitutional Court has not yet taken a final decision on this law.

Slovakia has responded to the problem of the financing of terrorism by amending its money laundering law with Act No. 445/2002, which criminalizes terrorist financing and obliges covered entities to report transactions possibly linked to terrorist financing. However, the reporting obligation with respect to terrorist financing is not sufficiently clear in the law. In addition, covered institutions have not received any guidance and no reports involving terrorist financing have been filed. The Criminal Code provides for an offense covering someone who "supports" a terrorist group. Authorities have acknowledged the possibility of proceeding for the aiding and abetting an offense of terrorism or the establishment of a terrorist group, but there is no jurisprudence on these points. The MONEYVAL team advised the authorities that the criminalization of terrorist financing solely on aiding and abetting is not in line with the standards set forth in the methodology. The MER also stated that the provisions are not wide enough to clearly criminalize collections of funds: with intention to carry out terrorist acts (whether they are used or not), for any activities undertaken by terrorist organizations, and with unlawful intent to be used by an individual terrorist.

All competent authorities in the Slovak Republic have full power to freeze or confiscate terrorist assets consistent with UNSCR 1373. According to Act No. 367/2000 and its later amendments, financial institutions are required to report to the regional financial police when they freeze or identify suspected terrorist-linked assets. The Government of Slovakia (GOS) has agreed to freeze

immediately all accounts owned by entities listed on the UNSCR 1267 Sanctions Committee's, the EU's consolidated lists, and those provided by the United States. The lists, however, are not distributed, but posted online. Obliged institutions have the responsibility to look at the names on the website and report if they have a match to any names on the list. Guidance and communication with the financial intermediaries and DNFBP community is weak. No terrorist finance-related accounts have been frozen or seized in Slovakia, but were a terrorism-related account to be identified, the financial police could hold any related financial transaction for up to 48 hours, and then gather evidence to freeze the account and seize any assets.

The GOS is a party to all 12 of the UN conventions and protocols against terrorism. However, as reported in its 2004 self-assessment questionnaire on anti-money laundering efforts for the Council of Europe (COE), Slovakia is still not fully compliant with the Financial Action Task Force's (FATF's) Special Recommendations on Terrorist Financing. The COE's Committee of Experts gave Slovakia a rating of "partial compliance" in 2004 with regard to Special Recommendation I (Implementation of UNSCR 1373) and Special Recommendation VII (enhanced scrutiny of transfers lacking originator information).

In late 2005, following its official release, Slovak authorities started to prepare for implementation of the Third EU Money Laundering Directive. After consultations with the Ministry of Finance, the Ministry of Interior, and the National Bank of Slovakia, the FIU has been tasked with drafting new legislation to comply with the Third Directive. The new legislation would also grant the FIU broader authority to work directly with prosecutors, tax authorities, and the regular police.

In 2002, the GOS ratified the UN International Convention for the Suppression of the Financing of Terrorism. The provisions of the Convention have been incorporated into amendments of the Bank Act, Penal Code, and Act No. 367/2000 and in March 2003, Slovakia elected to fully incorporate into its laws several optional terms of the convention. The FIU is a member of the Egmont Group and has signed memoranda of understanding (MOUs) with the FIUs of Slovenia, Monaco, Ukraine, Australia, Belgium, Poland, and the Czech Republic. The GOS also hopes to sign MOUs with Albania and Taiwan in 2006. Slovakia's FIU is the responsible authority for international exchange of information regarding money laundering under the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

Slovakia is a party to the European Convention on Mutual Legal Assistance in Criminal Matters, the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, the 1988 UN Drug Convention, and the UN Convention against Transnational Organized Crime. In June 2006, it also ratified the UN Convention against Corruption. Slovakia became a member of the Organization for Economic Cooperation and Development (OECD) in December 2000, thereby expanding its opportunities for multilateral engagement.

Slovakia is a member of the Group of States Against Corruption (GRECO), a platform of the Council of Europe to fight against corruption. GRECO carried out its Second Evaluation Round in early 2006, based on 17 recommendations made by GRECO in 2004. In its report issued in May 2006, GRECO concluded that Slovakia had implemented satisfactorily or dealt with in a satisfactory manner just under half of the 17 recommendations made by GRECO in 2004. GRECO evaluators were particularly concerned with the lack of mechanisms to fight corruption in the public sphere. Slovakia is a member of the Council of Europe and since 1997 has actively participated in the MONEYVAL Committee.

The Government of Slovakia (GOS) should continue to improve its anti-money laundering regime. Continued implementation of the provisions of Slovakia's anti-money laundering legislation will give the Slovak financial system greater protection by helping it prevent and detect money laundering in all financial sectors. Authorities should ensure that property and proceeds are equivalent in Article 252 and that this definition is contained in the law to avoid confusion on this issue. Slovakia should also provide guidance to, and improve supervision of its nonfinancial sectors to ensure that reporting

requirements are followed. Slovakia should implement formal AML supervision for exchange houses. Slovakia should provide adequate resources to assure that its FIU, law enforcement, and prosecutorial agencies are adequately funded and trained to effectively perform their various responsibilities, and work to enhance cooperation and coordination among these agencies and other competent authorities. Although all supervisory authorities need more staff and training, the FIU in particular needs to increase the number of staff so that the staffing is commensurate with its supervisory role. Slovakia should also take steps to include in its legislative framework the FATF-prescribed definition and treatment of beneficial owners. Authorities should consider criminal, civil or administrative sanction for money laundering in relation to legal persons.

With regard to fighting terrorism financing, the GOS should hone its legal framework to clarify the reporting obligation with respect to terrorist financing and issue guidance to covered institutions. Authorities can also amend the Criminal Code to ensure that criminalization of terrorist financing parallels international standards, including widening the parameters to sanction criminally collections of funds: with intention to carry out terrorist acts (used or not), for any activities undertaken by terrorist organizations, and with unlawful intent to be used by an individual terrorist.

In addition, the GOS can make the lists produced and circulated by the UN and the U.S. more readily accessible to obliged institutions by distributing them to the institutions instead of posting them online. This would also serve to enhance communication and provide an opportunity to give guidance to covered institutions.

## South Africa

South Africa's position as the major financial center in the region, its relatively sophisticated banking and financial sector, and its large cash-based market, all make it a very attractive target for transnational and domestic crime syndicates. Nigerian, Pakistani, and Indian drug traffickers, Chinese triads, Taiwanese groups, Lebanese trading syndicates, and the Russian mafia have all been identified as operating in South Africa, along with South African criminal groups. The fact that a high number of international crime groups operate in South Africa and that there are few reported money laundering prosecutions indicate that South Africa remains a money laundering jurisdiction of concern. Although the links between different types of crime have been observed throughout the region, money laundering is primarily related to the illicit narcotics trade. Other common types of crimes related to money laundering are: fraud, theft, corruption, currency speculation, illicit dealings in precious metals and diamonds, human trafficking, stolen cars, and smuggling. Most criminal organizations are also involved in legitimate business operations. There is a significant black market for smuggled goods.

South Africa is not an offshore financial center, nor does it have free trade zones. It does, however, operate Industrial Development Zones (IDZs). The South African revenue service monitors the customs control of these zones. Imports and exports that are involved in manufacturing or processing in the zone are duty-free, provided that the finished product is exported. South Africa maintains IDZs in Port Elizabeth, East London, Richards Bay, and Johannesburg International Airport.

The Proceeds of Crime Act (No. 76 of 1996) criminalizes money laundering for all serious crimes. This act was supplemented by the Prevention of Organized Crime Act (no. 121 of 1998), which confirms the criminal character of money laundering, mandates the reporting of suspicious transactions, and provides a "safe harbor" for good faith compliance. Violation of this act carries a fine of up to rand 100 million (approximately $16,700,000) or imprisonment for up to 30 years. Regulations require suspicious transaction reports to be sent to the South African financial intelligence unit (FIU), the Financial Intelligence Centre (FIC). Both of these Acts contain criminal and civil forfeiture provisions.

In 2005, the Protection of Constitutional Democracy Against Terrorist and Related Activities Act came into effect. The Act criminalizes terrorist activity and terrorist financing and gave the government investigative and asset seizure powers in cases of suspected terrorist activity. The Act is applicable to charitable and nonprofit organizations operating in South Africa. The Act requires financial institutions to report suspected terrorist activity to the FIC. The FIC distributes the list of individuals and entities included on the United Nations 1267 Sanctions Committee's consolidated list.

The FIC began operating in February 2003. The mandate of the FIC is to coordinate policy and efforts to counter money laundering activities. The FIC similarly acts as a centralized repository of information and statistics on money laundering. The FIC is a member of the Egmont Group of financial intelligence units. In addition to the FIC, South Africa has a Money Laundering Advisory Council (MLAC) to advise the Minister of Finance on policies and measures to combat money laundering.

The Financial Intelligence Centre Act (FICA) requires a wide range of financial institutions and businesses to identify customers, maintain records of transactions for at least five years, appoint compliance officers to train employees to comply with the law, and report transactions of a suspicious or unusual nature. Regulated businesses include companies and firms considered particularly vulnerable to money laundering activities, such as banks, life insurance companies, foreign exchange dealers, casinos, and real estate agents. If the FIC has reasonable grounds to suspect that a transaction involves the proceeds of criminal activities, it forwards this information to the investigative and prosecutorial authorities. If there is suspicion of terrorist financing, that information is to be forwarded to the National Intelligence Service. There are no bank secrecy laws in effect that prevent the disclosure of ownership information to bank supervisors and law enforcement authorities. However, the lack of actual cases prosecuted indicates problems in reporting process, analysis, investigations, and/or commitment.

From March 2005 through March 2006, the FIC received 19,793 suspicious transaction reports (STRs), an increase of 25 percent from the previous year's 15,757 STRs. The FIC reports that this increase is due to the development and distribution of its batch-reporting tool and not related to an increase in financial institutions detecting suspicious transactions. Precise information is not available on how many of these STRs led to criminal investigations. However, the number of financial crime and terrorist finance investigations, prosecutions, and convictions is believed to be extremely low. In addition, the quality and consistency of the STRs remains uneven. This is problematic for a country which has vast experience in implementing international banking standards. The FIC and South Africa's banks struggle to provide effective and comprehensive training programs relating to STR reporting and there has been no evidence of an increase in the quality of suspicious transaction reports. This calls into question the political will of the South African government towards implementing an effective and transparent AML/CFT regime

Many banks state that the reporting requirements hamper their efforts to attract new customers. For example, if the customer has never traveled outside the country, they may not have supporting documentation (no driver's license or passport) to properly satisfy the due diligence laws. Also, retroactive due diligence requirements mean those account holders who do not present identifying documents in person risk having their accounts frozen. These requirements were fully implemented in September 2006, after which date transactions with accounts owned by still-unidentified persons were blocked. Reporting requirements were specifically waived for brokers assisting clients with a one-time amnesty offer according to the Exchange Control and Amnesty and Amendment of Taxation Laws of 2003.

Because of the cash-driven nature of the South African economy, alternative remittance systems that bypass the formal financial sector exist, used largely by the strong local Islamic community. Hawala networks in South Africa have direct ties to South Asia and the Middle East. Currently, there is no

legal obligation requiring alternative remittance systems to report cash transactions within the country. The South African Revenue Service (SARS) requires large cash amounts to be declared only at entry and exit points. Smuggling and border enforcement are major problems in South Africa.

The Financial Action Task Force (FATF) conducted a mutual evaluation of South Africa in 2003 and made several recommendations regarding controls on cross-border currency movement, thresholds, and amendments to the Exchange Control Act. While legislation has been adopted in response to the recommendations, full implementation has yet to take place.

South Africa has cooperated with the United States in exchanging information related to money laundering and terrorist financing. The two nations have a mutual legal assistance treaty and a bilateral extradition treaty. In June 2003, South Africa became the first African nation to be admitted into the Financial Action Task Force (FATF), and it held the FATF Presidency for the period June 2005-June 2006. South Africa is also an active member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body.

South Africa is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

The South African Government should implement FATF Special Recommendation Nine and establish control over cross-border currency movement. It should regulate and investigate the country's alternative remittance systems. South Africa should increase steps to bolster border enforcement and should examine forms of trade-based money laundering and informal value transfer systems. It should fully implement the new law (Protection of Constitutional Democracy against Terrorist and Related Activities Act) against terrorist activity and terrorist financing. South Africa should publish the annual number of money laundering and terrorist financing investigations, prosecutions, and convictions.

## Spain

Spain is not a European financial center. Spain plays a significant role in money laundering as a key point of entry and European base for the proceeds of Colombian narcotics trafficking organizations. Drug proceeds from other regions enter Spain as well, particularly proceeds from hashish trafficking and smuggling entering from Morocco and heroin money entering from Turkey.

Tax evasion in internal markets and smuggling of goods along the coastline also continue to be sources of illicit funds in Spain. Reportedly, Spanish authorities believe that tax evasion in cell phone and property industries is currently the most serious financial crime. The smuggling of electronics and tobacco from Gibraltar remains an ongoing issue. Airline personnel traveling between Spain and Latin America smuggle out bulk cash. Additional money laundering methodologies found in Spain include Colombian companies purchasing goods in Asia and sell them legally at drug cartel-run stores in Europe. Credit card balances are paid in Spanish banks for charges made in Latin America, and money deposited in Spanish banks is withdrawn in Colombia through ATM networks

An unknown percentage of the proceeds from drug-trafficking is invested in Spanish real estate, particularly in the booming coastal areas in the south and east of the country. Twenty-five percent of the 500 euro notes in use in Europe are in circulation in Spain. Reportedly, this is directly linked to the purchase of real estate to launder money. There are no known currency transactions of significance involving large amounts of U.S. currency and/or direct narcotics proceeds from U.S. sales.

In September 2006, Spanish police arrested eight people of Spanish and Colombian nationality for drug trafficking and money laundering. Government of Spain (GOS) officials estimate that the individuals may have laundered more than 13.5 million euro (approximately 17.8 million dollars). The

investigation began at the end of 2003 after a money laundering organization was dismantled when a vessel carrying 412 kilos of cocaine was intercepted in Togo.

In May 2006, 21 people were arrested and accused of being members of an international money laundering and drug-trafficking gang. Police seized 193 kilos of cocaine, weapons, money, and luxury vehicles imported from Germany and then sold in Spain to launder the proceeds. It is estimated that the criminal organization had laundered a total of 360 million euro (approximately 475 million dollars) since 2000. The arrested members are also implicated in other offenses such as corruption of minors, forgery, and fraud.

Although little of the money laundered in Spain is believed to be used for terrorist financing, money from the extortion of businesses in the Basque region is moved through the financial system and used to finance the Basque terrorist group. ETA informal nonbank outlets (such as "Locutorios"), make small international transfers for the immigrant community, and continue to be used to move money in and out of Spain. Spanish regulators also note the presence of hawala networks in the Islamic community.

Spain is not considered to be an offshore financial center, and does not operate any Free Trade Zones. Spanish law states that an entity can perform banking activity if its registered office, administration, and management reside within Spanish territory. Spanish law does not prohibit financial institutions from entering into banking relationships with shell banks. Financial institutions have no requirement to determine whether a respondent financial institution in a foreign country allows accounts used by shell banks. The GOS has no accurate estimate of the numbers of offshore banks, offshore international business companies, exempt companies, or shell companies. Spanish law does not recognize trusts, including those created in foreign countries. Offshore casinos and internet gaming sites are forbidden. However, online casinos often run from servers located outside of Spanish territory. GOS politicians have been critical of Gibraltar's role in this regard. Regulation can only occur through mutual judicial assistance or international agreements.

Money laundering was criminalized by Article 301 of the Penal Code. The criminalization of money laundering was added to the penal code in 1988 when laundering the proceeds from narcotics trafficking was made a criminal offense. The law was expanded in 1995 to cover all serious crimes that required a prison sentence greater than three years. Amendments to the code on November 25, 2003, which took effect on October 1, 2004, made all forms of money laundering financial crimes; any property, of any value, can form the basis for a money laundering offence, and a conviction or a prosecution for a predicate offense is not necessary to prosecute or obtain a conviction for money laundering. The penal code can also apply to individuals in financial firms if their institutions have been used for financial crimes. An amendment to the penal code in 1991 made such persons culpable for both fraudulent acts and negligence connected with money laundering. Spanish authorities can also prosecute money laundering from a predicate offense in another country, if the offense would be illegal in Spain.

Law 19/2003 regulating the movements of capital and foreign transactions implements the European Union (EU) Money Laundering Directive. The law obligates financial institutions to make monthly reports on large transactions. Banks are required to report all international transfers greater than 30,000 euros (approximately $39,600). The law also requires the declaration and reporting of internal transfers of funds greater than 80,500 euros (approximately $106,300). Individuals traveling internationally are required to report the importation or exportation of currency greater than 6,000 euros (approximately $7,900). Foreign exchange and money remittance entities must report on transactions above 3,000 euro (approximately $3,960). Reporting on transactions exceeding 30,000 euro from or with persons in countries or territories considered to be tax havens is also required. Law 19/2003 allows the seizure of up to 100 percent of the currency if illegal activity under financial crimes ordinances can be proven. Spanish authorities claim they have seen a drop in cash couriers

since the law's enactment in July 2003. For cases where the money cannot be connected to criminal activity, and has not been declared, the authorities may seize the money until the origin of the funds is proven.

The financial sector is required to identify customers, keep records of transactions, and report suspicious financial transactions. Spanish banks are required by law to maintain fiscal information for five years and mercantile records for six years.

Money laundering controls apply to most entities active in the financial system, including banks, mutual savings associations, credit companies, insurance companies, financial advisers, brokerage and securities firms, postal services, currency exchange outlets, casinos, and individuals and unofficial financial institutions exchanging or transmitting money. The 2003 amendments add lawyers and notaries as covered entities. Previously, notaries and lawyers were required to report suspicious cases, but now they are considered part of the financial system that is under the supervision of appropriate regulators. As of April 2005, most categories of designated nonfinancial businesses and professions (DNFBP) are subject to the same core obligations as the financial sector. The list of DNFBPs includes casinos, realty agents, dealers in precious metals and stones, as well as in antiques and art, legal advisors, accountants and auditors.

Article 3.2 of Law 19/1993 mandates that reporting entities should examine and commit to writing the results of an examination of any transaction, irrespective of amount, which by its nature may be linked to laundering of proceeds. Law 12/2003 reaffirms the obligation of reporting suspicious activities. Reporting entities are required to report to suspicious individual transactions to the Financial Intelligence Unit, or FIU. Financial institutions also have an obligation to undertake systematic reporting of unusual transactions, including physical movements of cash, travelers' checks, and other bearer instruments/checks drawn on credit institutions above 30,000 euro (approximately $39,600). The reporting obligation applies to the laundering of proceeds of all illicit activity punishable by a minimum of three years imprisonment, including terrorism or terrorist financing. Non Bank Financial Institutions (NBFIs) such as insurers, investment services firms, collective investment schemes, pension fund managers, and others are subject to these requirements.

Article 4 of Law 19/1993 and Article 15 of RD 925/1995 protect financial institutions and their staff for breach of any restriction on disclosure of information when reporting suspicious transactions. Reporting units must also take appropriate steps to conceal the identity of employees or managers making suspicious transaction reports.

Law 19/1993 and RD 925/1995 established The Executive Service of the Commission for the Prevention of Money Laundering (SEPBLAC), to act as Spain's FIU. SEPBLAC has the primary responsibility for any investigation in money laundering cases and directly supervises the anti-money laundering procedures of banks and financial institutions. SEPBLAC is an interdepartmental body chaired by the Secretary for Economic Affairs, and all of the agencies involved in the prevention of money laundering participate. The representatives include the National Drug Plan Office, the Ministry of Economy, Federal Prosecutors (Fiscalia), Customs, Spanish National Police, Civil Guard, CNMV (equivalent to the SEC), Treasury, Bank of Spain, and the Director General of Insurance and Pension Funds.

SEPBLAC coordinates the fight against money laundering in Spain. Its primary mission is to receive, analyze and disseminate suspicious and unusual transaction reports from financial institutions and DNFBPs. SEPBLAC also has supervisory and inspection functions and is directly responsible for the supervision of a large number of regulated institutions. For this reason, SEPBLAC has memoranda of understanding with the Bank of Spain, the National Securities Market Commission, and the Director General of Insurance and Pension Funds, in order for these regulators to supervise their sectors.

In June 2006, the Financial Action Task Force (FATF) released the third-round mutual evaluation report (MER) for Spain. The evaluation team noted some areas where Spain is not in full compliance with the Forty Recommendations and Nine Special Recommendations. The FATF MER called the FIU's supervisory capabilities ineffective because of limited resources; it also expressed concern regarding SEPBLAC's independence from the Bank of Spain.

SEPBLAC has access to the records and databanks of other government entities, financial institutions, and has formal mechanisms in place to share information domestically and with other FIUs, including FINCEN. SEPBLAC has been an active member of the Egmont Group since 1995. SEPBLAC received 493 requests for information from other FIUs in 2005, and made 143 requests to Egmont members. SEPBLAC received 2,502 suspicious transaction reports (STRs) in 2005. Thirty-seven STRs were used to initiate investigations.

Any member of the Commission may request an investigation. However, the FATF MER noted some concerns about the effectiveness of SEPBLAC's investigations, stating that at certain stages of the investigative process, obtaining account files can be time-consuming. The National Police and Anticorruption Police informed the evaluation team that they receive too many reports, and the reports they do receive are not adequate to serve as the basis for an investigation. SEPBLAC delegates responsibility to two additional organizations. The first is a secretariat in the Treasury, located in the Ministry of Economy. Following investigation and a guilty verdict by a court, this regulating body carries out penalties. Sanctions can include closure, fines, account freezes, or seizures of assets. Law 19/2003 allows seizures of assets of third parties in criminal transactions, and a seizure of real estate in an amount equivalent to the illegal profit.

Under Spain's currency control system, individuals and companies must declare the amount, origin, and destination of incoming and outgoing funds. Cash smuggling reports are shared between host government agencies. Provisional measures and confiscation provisions apply to persons smuggling cash or monetary instruments that are related to money laundering or terrorist financing. Gold, precious metals, and precious stones are considered to be merchandise and are subject to customs legislation. Failing to file a declaration for such goods may constitute a case of smuggling and would fall under the responsibility of the customs authorities.

All legal charities are placed on a register maintained by the Ministry of Justice. Responsibility for policing registered charities lies with the Ministry of Public Administration. If the charity fails to comply with the requirements, sanctions or other criminal charges may be levied.

The Penal Code provides for two types of confiscation: generic (Article 127) and specific, for drug-trafficking offences (Article 374). Article 127 of the Penal Code allows for broad confiscation authorities by applying it to all crimes or summary offenses under the Code. The effects, instruments used to commit the offense, and the profits derived from the offence can all be confiscated. Article 127 also provides for the confiscation of property intended for use in the commission of any crime or offence. It also applies to property that is derived directly or indirectly from proceeds of crime, regardless of whether the property is held or owned by a criminal defendant or by a third party. Article 374 of the Penal Code calls for the confiscation of goods acquired through drug trafficking-related crimes, and of any profit obtained. This allows for the confiscation of instruments and effects used for illegal drug dealing, as well as the goods or proceeds obtained from the illicit traffic. Consequently, all assets held by a person convicted of drug trafficking may be confiscated if those assets are the result of unlawful conduct.

A judge may impose provisional measures concerning seizures from any type of offense by virtue of the code of criminal procedure. Effects may be seized and stored by the judicial authorities at the beginning of an investigation. The Fund of Seized Goods of Narcotics Traffickers receives seized assets. This agency was established under the National Drug Plan. The proceeds from the funds are divided, with equal amounts going to drug treatment programs and to a foundation that supports

officers fighting narcotics trafficking. The division of assets from seizures involving more than one country depends on the relationship with the country in question. EU working groups determine how to divide the proceeds for member countries. Outside of the EU, bilateral commissions are formed with countries that are members of Financial Action Task Force (FATF), FATF-like bodies, and the Egmont Group, to deal with the division of seized assets. With other countries, negotiations are conducted on an ad hoc basis.

The banking community cooperates with enforcement efforts to trace funds and seize/freeze bank accounts. The law is unclear as to whether or not civil forfeitures are allowed. The GOS enforces existing drug-related seizure and forfeiture laws. Spain has adequate police powers and resources to trace, seize, and freeze assets. Spain disseminates limited statistics on money laundering and terrorist financing investigations, prosecutions and convictions as well as on property frozen, seized and confiscated. As of mid 2005, 36,105,720 euro (approximately 47.6 million dollars) had been seized.

The FATF MER team noted some shortcomings in the areas of customer due diligence, beneficial ownership of legal persons, and bearer shares. Anonymous accounts and accounts in fictitious names are precluded by Spanish legislation. Bearer shares are permitted in Spain, although not as many as in the past. Spanish authorities have taken steps to neutralize them, since 1998 ensuring that mere possession cannot serve as proof of ownership. However, they still exist, and it appears that the authorities are learning more about legal persons using such shares. The MER team cited the requirements to determine the beneficial owner as "inadequate."

The FATF MER gives Spain a good overall review with regard to terrorist financing. Spain has long been engaged in fighting terrorist organizations, including ETA, GRAPO and more recently, al-Qaida. Spanish law enforcement entities have identified several methods of terrorist financing: donations to finance nonprofit organizations (including ETA and Islamic groups); establishment of publishing companies that print and distribute books or periodicals for the purposes of propaganda, which then serve as a means for depositing funds obtained through kidnapping or extortion; fraudulent tax and subvention collections; the establishment of "cultural associations" used to facilitate the opening of accounts and provide a cover for terrorist finance activity; and alternate remittance system transfers.

Spain complies with all EU regulations concerning the freezing of terrorist assets. Crimes of terrorism are defined in Article 571 of the Penal Code, and penalties are set forth in Articles 572 and 574. Sanctions range from ten to thirty years' imprisonment with longer terms if the terrorist actions were directed against government officials. On March 6, 2001, Spain's Council of Ministers adopted a decision requesting the implementation of UNSCR 1373 in the Spanish legal framework. EU Council Regulation (EC) 881/2002, which obliges covered countries such as Spain to execute UNSCR 1373, is implemented through EC No. 2580/of 27 December 2001. Terrorist financing issues are governed by a separate code of law and commission, the Commission of Vigilance of Terrorist Finance Activities (CVAFT). This commission was created under Law 12/2003 on the Prevention and Blocking of the Financing of Terrorism. In addition to the EU Council Regulations, Law 12/2003, when implemented, will allow the freezing of any type of financial flow so as to prevent the funds from being used to commit terrorist acts. Spanish authorities' ability to freeze accounts granted in the most recent law is more aggressive than that of most of their European counterparts. Though many laws are transposed from European Union (EU) directives, Law 12/2003 on the prevention and freezing of terrorist financing surpasses EU Council requirements. However, the implementing regulations have yet to be announced.

As with all of the European Union countries, the obligation to freeze assets under UNSCR 1267 has also been implemented through the Council. Spain regularly circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee consolidated list. There were six actions taken against individuals or entities in 2005 under 1267

and/or 1373, for a total value of 83.75 euro ($106). The Terrorist Finance Watchdog Commission is charged with issuing freezing orders.

Spain is a member of the FATF, and co-chairs the FATF Terrorist Finance Working Group. Spain is a participating and cooperating nation to the South American Financial Action Task Force (GAFISUD), and a cooperating and supporting nation to the Caribbean Financial Action Task Force (CFATF). Spain is a major provider of counterterrorism assistance. SEPBLAC is a member of the Egmont Group and currently chairs the Outreach Committee Working Group. Spain provides anti-money laundering and counterterrorist finance assistance, particularly to Spanish speaking countries in Latin America.

The GOS has signed criminal mutual legal assistance agreements with Argentina, Australia, Canada, Chile, the Dominican Republic, Mexico, Morocco, Uruguay, and the United States. Spain's Mutual Legal Assistance Treaty with the United States has been in effect since 1993, and provides for sharing of seized assets, provided the request is made to the Spanish court hearing the case, rather than administratively. Spain has also entered into bilateral agreements for cooperation and information exchange on money laundering issues with fourteen countries around the world, as well as with the United States. SEPBLAC has bilateral agreements for cooperation and information exchange on money laundering issues with twenty-one FIUs around the world.

Spain actively collaborates with Europol, supplying and exchanging information on terrorist groups. In 2006, U.S. law enforcement agencies also reported excellent cooperation with their Spanish counterparts.

Spain is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism. Spain adheres to all EC policy directives on crime, money laundering, and the financing of terrorism.

The scale of money laundering and the sophisticated methods used by criminals create a significant law enforcement problem in Spain. The Government of Spain (GOS) has passed and enacted legislation designed to help eliminate and prosecute financial crimes. In light of the findings of the 2006 FATF mutual evaluation, Spain should review its supervisory regime with a view toward maximizing the coordination of inspections as well as interagency cooperation . Spain should also review the resources available for industry supervision. The GOS should work to close potential loopholes that FATF identified, including those in the areas of customer due diligence, beneficial ownership of legal persons, and bearer shares. . Spain should also work to implement Law 12/2003, which will greatly enhance Spain's capabilities to combat terrorism financing. Spain should maintain and disseminate statistics on investigations, prosecutions and convictions, including the amounts and values of assets frozen or confiscated.

## St. Kitts and Nevis

The Government of St. Kitts and Nevis (GOSKN) is a federation composed of two islands in the Eastern Caribbean. The federation is at major risk for corruption and money laundering, due to the high volume of narcotics trafficking activity and the presence of known traffickers on the islands. The offshore financial sectors of both islands are vulnerable to money laundering. An inadequately regulated economic citizenship program compounds the problem.

Each island has the authority to organize its own financial structure. As a Federation, there is offshore legislation governing both St. Kitts and Nevis. However, with most of the offshore financial activity concentrated in Nevis, it has developed its own offshore legislation independently. As of September 2006, Nevis has one offshore bank (a subsidiary of a domestic bank), 61 licensed insurance companies, 1,014 international trusts, 29 foundations and 54 corporate service providers. There are two types of international companies eligible for incorporation: international business companies

(IBCs) and limited liability companies (LLCs). Current figures indicate there are 12,773 IBCs and 3,732 LLCs registered in Nevis. Reports from 2006 indicate that St. Kitts' offshore sector consists of 1,019 exempt companies, 203 exempt foundations, four trust companies, two investment companies, 21 corporate service providers, and three licensed internet gaming companies that must incorporate as IBCs. According to reports from 2004-2005, St. Kitts also has four domestic banks, 120 credit unions, four domestic insurance companies, and two money remitters. There are no free trade zones in St. Kitts and Nevis.

The GOSKN licenses offshore banks and businesses. Bearer shares are permitted, provided that bearer share certificates are retained in the safe custody of persons or financial institutions authorized by the Minister of Finance as approved custodians. Authorized service providers serve as a company's first directors or trustees; this information is made public. Subsequent to incorporation or registration, the authorized persons transfer such duties to other persons. This information is restricted to only the regulator and authorized persons who have access to the information. Reportedly, extensive background checks on all proposed licensees are conducted by a third party on behalf of the GOSKN before a license is granted. Under the Nevis Offshore Banking Ordinance 1996, as amended in 2002, the Eastern Caribbean Central Bank (ECCB) is required to review all applications for licenses and report its recommendations to the Minister of Finance prior to consideration of the application. By law, all licensees are required to have a physical presence in St. Kitts and Nevis. All authorized persons are required to obtain proper documents on shareholders or beneficial owners before incorporating IBCs or other offshore companies.

The Proceeds of Crime Act (POCA) 2000 criminalizes money laundering for serious offenses and imposes penalties ranging from imprisonment to monetary fines. The POCA also overrides secrecy provisions that may have constituted obstacles to the access of administrative and judicial authorities to information with respect to account holders or beneficial owners. Other anti-money laundering measures include the Financial Services Commission Act 2000, the Nevis Offshore Banking (Amendment) 2000, the Anti-Money Laundering Regulations 2001, the Companies (Amendment) Act 2001, the Anti-Money Laundering (Amendment) Regulations 2001, the Nevis Business Corporation (Amendment) 2001, and the Nevis Offshore Banking (Amendment) 2001.

The ECCB has direct responsibility for regulating and supervising the offshore bank in Nevis, as it does for domestic banks in St. Kitts and Nevis, and for making recommendations regarding approval of offshore bank licenses. The St. Kitts and Nevis Financial Services Commission, with regulators on both islands, regulates nonbank financial institutions for anti-money laundering compliance. The GOSKN has issued regulations requiring financial institutions to identify their customers upon request, maintain a record of transactions for up to five years, report suspicious transactions, and establish anti-money laundering training programs. The Financial Services Commission has issued guidance notes on the prevention of money laundering, pursuant to the Anti-Money Laundering Regulations. The Commission is authorized to carry out anti-money laundering examinations. The St. Kitts and Nevis Gaming Board is responsible for ensuring compliance of casinos.

The Financial Intelligence Unit (FIU) Act No. 15 of 2000 authorized the creation of an FIU. The FIU began operations in 2001 and receives, analyzes and investigates suspicious activity reports (SARs) from reporting entities in both St. Kitts and Nevis. All financial institutions, including nonbank financial institutions, are required by law to report suspicious transactions. Anti-money laundering regulations and the FIU Act provide protection for reporting entities and its employees, officers, owners or representatives who forward SARs to the FIU. In 2006, the FIU received 50 SARs. Of these, 20 SARs were referred to law enforcement for appropriate action. There have been no reports of further action taken on these referrals. The Royal St. Kitts and Nevis Police Force is responsible for investigating financial crimes, but does not have adequate staff or training to effectively execute its mandate. The FIU has direct and indirect access to records of other government agencies through

memoranda of understanding (MOU). The FIU Act has provisions for sharing information, both domestically and with foreign counterparts and law enforcement agencies.

Under the POCA legitimate businesses can be seized by the FIU if proven to be connected to money laundering activities. The FIU can freeze an individual's bank account for a period not to exceed five days in the absence of a court order. The freeze orders obtained from the court at times ascribe an expiration of six months or more. The law only allows for criminal forfeiture; civil forfeiture is considered unconstitutional. The POCA provides for a forfeiture fund under the administration and control of the Financial Secretary in St. Kitts and the Permanent Secretary in the Ministry of Finance in Nevis. All monies and proceeds from the sale of property forfeited or confiscated are placed in the fund to be used for the purpose of anti-money laundering activities in both St. Kitts and Nevis.

The POCA limits and monitors the international transportation of currency and monetary instruments. Any person importing or exporting a value exceeding US$10,000 or its equivalent in Eastern Caribbean currency needs to declare it with Customs. In addition, the Customs Control and Management Act criminalizes cash smuggling. Customs and law enforcement share cash smuggling reports.

St. Kitts and Nevis enacted the Anti-Terrorism Act (ATA) No. 21, effective November 27, 2002. Sections 12 and 15 of the Act criminalize the financing of terrorism. Under the ATA, the FIU and Director of Public Prosecutions have the authority to identify, freeze, and/or forfeit assets related to terrorist financing. The ATA also implements various UN Conventions against terrorism. The GOSKN circulates to financial institutions the names of individuals and entities that have been included on the UN 1267 Sanctions Committee's lists. To date, no terrorist-related funds have been identified. The ATA does not provide the FIU with the authority to receive disclosures relating to potential financing of terrorism from reporting entities. The GOSKN has some existing controls that apply to alternative remittance systems, but has not undertaken initiatives that apply directly to the potential terrorist misuse of charitable and nonprofit entities.

A Mutual Legal Assistance Treaty (MLAT) between the GOSKN and the United States entered into force in early 2000, but cooperation over the last three years has been stalled by the GOSKN. St. Kitts and Nevis is a member of the Caribbean Financial Action Task Force (CFATF) and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. St. Kitts and Nevis is a party to the UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. The GOSKN has signed, but not yet ratified, the Inter-American Convention against Terrorism, and has neither signed nor ratified the UN Convention against Corruption. The FIU became a member of the Egmont Group in 2004.

St. Kitts and Nevis should devote sufficient resources to effectively implement its anti-money laundering regime, giving particular attention to its offshore financial sector. St. Kitts and Nevis should determine the exact number of Internet gaming companies present on the islands and provide the necessary oversight of these entities. St. Kitts and Nevis should amend the Anti-Terrorism Act to provide the FIU with the authority to receive disclosures relating to potential financing of terrorism from reporting entities. Additionally, St. Kitts and Nevis should improve its cooperation with foreign counterparts, particularly the timely information sharing on money laundering and financial crime activity and the implementation of bilateral agreements. St. Kitts should become a party to the UN Convention against Corruption.

## St. Lucia

St. Lucia has developed an offshore financial service center that increases the island's vulnerability to money laundering and other financial crimes. Transshipment of narcotics (cocaine and marijuana),

unregulated money remittance businesses, cash smuggling, and bank fraud, such as counterfeit U.S. checks and identity theft, are among the other primary vulnerabilities for money laundering in St. Lucia.

Currently, St. Lucia has four offshore banks, 1,912 international business companies (IBCs), seven private mutual funds, two public mutual funds, 43 international trusts, 24 international insurance companies, 24 trust companies, two money remitters, three mutual fund administrators, 13 registered agents and four registered trustees (service providers), and a total of 30 domestic financial institutions. Shell companies are not permitted. The Government of St. Lucia (GOSL) also has one free trade zone where investors may establish businesses and conduct trade and commerce within the free trade zone or between the free trade zone and foreign countries. There are no casinos or internet gaming sites in St. Lucia. Reportedly, the GOSL does not plan to consider the establishment of gaming enterprises.

In 1999, the GOSL enacted a comprehensive inventory of offshore legislation, consisting of the International Business Companies (IBC) Act, the Registered Agent and Trustee Licensing Act, the International Trusts Act, the International Insurance Act, the Mutual Funds Act and the International Banks Act. An IBC may be incorporated under the IBC Act. Only a person licensed under the Registered Agent and Trustee Licensing Act as a licensee may apply to the Registrar of IBCs to incorporate and register a company as an IBC. The registration process involves submission of the memorandum and articles of the company by the registered agent, payment of the prescribed fee, and the Registrar's determination of compliance with the requirements of the IBC Act. IBCs can be registered online through the GOSL's web page. IBCs intending to engage in banking, insurance or mutual fund business may not be registered without the approval of the Minister responsible for international financial services. An IBC may be struck off the register on the grounds of carrying on business against the public interest.

The GOSL established the Committee on Financial Services in 2001. The Committee, which meets monthly, is designed to safeguard St. Lucia's financial services sector. The Committee is composed of the Minister of Finance, the Attorney General, the Solicitor General, the Director of Public Prosecutions, the Director of Financial Services, the Registrar of Business Companies, the Commissioner of Police, the Deputy Permanent Secretary of the Ministry of Commerce, the police officer in charge of the Special Branch, the Comptroller of Inland Revenue and others. The GOSL announced in 2003 its intention to form an integrated regulatory unit to supervise the onshore and offshore financial institutions the GOSL currently regulates. As of October 31, 2006, administrative procedures were implemented, but the unit is not yet fully functional. The Eastern Caribbean Central Bank regulates St. Lucia's domestic banking sector.

The 1993 Proceeds of Crime Act criminalizes money laundering with respect to narcotics. The Proceeds of Crime Act also provides for a voluntary system of reporting account information to the police or prosecutor when such information may be relevant to an investigation or prosecution. Reporting individuals (bankers and other financial institutions) are protected by the law with respect to their cooperation with law enforcement entities. In addition, the Act requires financial institutions to retain information on new accounts and transactions for seven years. In September 2003, legislation was adopted that extends anti-money laundering compliance requirements to credit unions, money remitters and pawnbrokers, as well as strengthens criminal penalties for money laundering.

Many of the 1993 Proceeds of Crime Act provisions are superseded by the 1999 Money Laundering (Prevention) Act (MLPA), which criminalizes the laundering of proceeds with respect to 15 predicate offenses, including abduction, blackmail, counterfeiting, extortion, firearms and narcotics trafficking, forgery, corruption, fraud, prostitution, trafficking in persons, tax evasion, terrorism, gambling and robbery. The MLPA mandates suspicious transaction reporting requirements and imposes record keeping requirements. In addition, the MLPA imposes a duty on financial institutions to take reasonable measures to establish the identity of customers, and requires accounts to be maintained in

the true name of the holder. It also requires an institution to take reasonable measures to identify the underlying beneficial owner when an agent, trustee or nominee operates an account. These obligations apply to domestic and offshore financial institutions, including credit unions, trust companies, and insurance companies. In April 2000, the Financial Services Supervision Unit issued detailed guidance notes, entitled "Minimum Due Diligence Checks, to be conducted by Registered Agents and Trustees." Currently steps are being taken to implement legislation to regulate money remitters.

The Financial Intelligence Authority Act No. 17 of 2002 authorizes the establishment of St. Lucia's financial intelligence unit (FIU), which became operational in October 2003. Pursuant to legislation passed in September 2003, the Money Laundering (Prevention) Authority, which had previously been responsible for monitoring compliance with the anti-money laundering provisions of the MLPA, was merged with the FIU. The FIU is responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs) from obligated financial institutions, and has regulatory authority to monitor compliance with anti-money laundering requirements. The FIU is also able to compel the production of information necessary to investigate possible offenses under the 1993 Proceeds of Crime Act and the MLPA. Failure to provide information to the FIU is a crime, punishable by a fine or up to ten years imprisonment. The Financial Intelligence Authority Act permits the sharing of information obtained by the FIU with foreign FIUs. The FIU has access to relevant records and databases of all St. Lucian government entities and financial institutions. However, no formal agreement exists for sharing information domestically and with other FIUs.

In 2006, the FIU received 27 STRs. There are no recorded cases of money laundering within St. Lucia's banking sector for 2006. However, there has been an increase in bank fraud, such as counterfeit U.S. checks and identity theft.

Customs laws criminalize cash smuggling, and customs officials are aware of cash courier problems. Cash smuggling reports are shared with the FIU, Police, Director of Public Prosecutions and the Attorney General.

Under current legislation, instruments of crime, such as conveyances, farms, and bank accounts, can be seized by the FIU. Substitute assets can also be seized. The legislation also applies to legitimate businesses if used to launder drug money, support terrorist activity, or are otherwise used in a crime. There is no legislation for civil forfeiture or sharing of seized narcotics assets. If the individual or business is not charged, then assets must be released within seven days. Approximately $100,000 of nonterrorist related assets were frozen in 2006.

The GOSL has not criminalized the financing of terrorism. However, St. Lucia circulates lists to financial institutions of terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O 13224. The Government of St. Lucia has the legislative power to freeze, seize and forfeit terrorist finance related assets. To date, no accounts associated with terrorists or terrorist entities have been found in St. Lucia. The GOSL has not taken any specific initiatives focused on the misuse of charitable and nonprofit entities.

The GOSL has been cooperative with the USG in financial crime investigations. In February 2000, St. Lucia and the United States brought into force a Mutual Legal Assistance Treaty. St. Lucia also has a Tax Information Exchange Agreement with the United States.

St. Lucia is a member of the Caribbean Financial Action Task Force (CFATF) and the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The FIU is not yet a member of the Egmont Group. St. Lucia is a party to the 1988 UN Drug Convention and has signed, but has not yet ratified, the UN Convention against Transnational Organized Crime and the Inter-American Convention against Terrorism. The GOSL has not signed the

UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Corruption.

The Government of St. Lucia should become a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. In order to meet international standards, St. Lucia should criminalize the financing of terrorism. The GOSL should continue to enhance and implement its money laundering legislation and programs, including adopting civil forfeiture legislation and ensuring that its FIU meets the Egmont Group membership requirements. The rapid expansion of the island's offshore financial services sector should be counterbalanced by efforts that increase transparency. The GOSL also needs to improve their record of investigating, prosecuting and sentencing money launderers and those involved in other financial crimes.

## St. Vincent and the Grenadines

As a result of their status as a transit point for illicit narcotics and its growing offshore sector, St. Vincent and the Grenadines (SVG) are vulnerable to money laundering and other financial crimes. Money laundering is most often associated with the production and trafficking of marijuana in SVG, as well as the trafficking of other narcotics from South America. The illicit narcotics proceeds are laundered through various financial institutions, including banks (both domestic and offshore), money remitters, cash couriers and casinos. Over the past year, there has been an increase in fraud and the use of counterfeit instruments, such as tendering counterfeit checks or cash.

The domestic sector is comprised of two commercial banks, a development bank, two savings and loan banks, a building society, 16 insurance companies, 10 credit unions and two money remitters. The offshore sector includes 6 offshore banks; 7,655 international business corporations (IBCs), an increase of more than 1,000 IBCs since 2005; 16 offshore insurance companies; 39 mutual funds; 33 registered agents; and 126 international trusts. No physical presence is required for offshore financial institutions and businesses. Nominee directors are not mandatory except when an IBC is formed to carry out banking business. Bearer shares are permitted for IBCs but not for banks. There are no free trade zones in SVG. There are no offshore casinos, and no internet gaming licenses have been issued. The Government of St. Vincent and the Grenadines (GOSVG) eliminated its economic citizenship program in 2001.

The Eastern Caribbean Central Bank (ECCB) supervises SVG's domestic banks. The International Banks (Amendment) Act 2002 provides the ECCB with the authority to review and make recommendations regarding the approval of offshore bank licenses. The International Financial Services Authority (IFSA) regulates the international financial sector and oversees the process of licensing and supervision of the sector, which includes conducting on-site inspections to evaluate the financial soundness and anti-money laundering programs of offshore banks.

The International Banks (Amendment) Act of October 2000 provides the GOSVG with access to the name or title of a customer account and any other confidential information about the customer that is in the possession of a licensee. In 2002, the International Business Companies Amendment Act No. 26 of 2002 was enacted to immobilize and register bearer shares. The Exchange of Information Act No. 29 of 2002 authorizes and facilitates the exchange of information, particularly among regulatory bodies.

The Proceeds of Crime and Money Laundering (Prevention) Act 2001 criminalizes money laundering, and requires financial institutions and other regulated businesses to report suspicious transactions. Customers are required to complete a source of funds declaration for any cash transaction over $10,000 ECD (approximately $3,800). However, it is not mandatory to report other noncash transactions exceeding $10,000 ECD. The Proceeds of Crime (Money Laundering) Regulations were

published in January 2002 and establish mandatory record keeping rules and limited customer identification requirements. Financial institutions are required to maintain all records relating to transactions for a minimum of seven years.

The Financial Intelligence Unit Act No. 38 of 2001 (FIU Act) establishes the financial intelligence unit (FIU). Operational as of 2002, the FIU investigates and prosecutes money laundering cases. As of November 2006, the FIU had received 97 suspicious transaction reports (STRs) for the year and almost 600 STRs since its inception. The FIU is also the main body that supervises the compliance of financial and nonfinancial institutions with anti-money laundering and counterterrorist financing laws and regulations. The FIU conducts anti-money laundering and counterterrorist financing awareness training to educate these entities of the legal reporting requirements. Reporting entities are protected by law if fully cooperative with the FIU. There were five money laundering cases pending in 2005. Two of these cases resulted in convictions in 2006.

The FIU Act, as amended, permits the sharing of information at the investigative or intelligence stage, but the FIU does not have direct access to the records or databases of other government agencies. The FIU Act allows for the exchange of information with other FIUs. An updated extradition treaty and a Mutual Legal Assistance Treaty (MLAT) between the United States and the GOSVG entered into force in September 1999. The FIU executes the MLAT requests. In 2003, the GOSVG reintroduced a customs declaration form to be completed by incoming travelers. Incoming travelers are required to declare currency over $10,000 ECD (approximately $3,800).

Existing anti-money laundering legislation allows for the forfeiting of intangible and tangible property. Drug trafficking offenses may also be liable to forfeiture pursuant to the Drug (Prevention and Misuse) Act and the Criminal Code. There is no period of time during which the assets must be released. Frozen assets are confiscated by the FIU upon conviction of the defendant. Proceeds from asset seizures and forfeitures are placed by the FIU into the Confiscated Assets Fund established by the Proceeds of Crime and Money Laundering (Prevention) Act. Legitimate businesses can also be seized if used to launder drug money, support terrorist activity, or are otherwise used in a crime. At this time, only criminal forfeiture is permitted; however, a civil forfeiture bill is currently being debated. In 2006 the GOSVG froze or seized approximately 666,693 ECD (approximately $251,600) in assets. Of this amount, approximately 51,000 ECD ($19,200) worth of assets were forfeited.

The GOSVG enacted the United Nations Terrorism Measures Act in 2002. In July 2006, parliament enacted amendments to the Act and the FIU Act to ensure compliance with international standards and require financial institutions to report suspicious activity related to the financing of terrorism to the FIU. The GOSVG circulates lists of terrorists and terrorist entities to all financial institutions in SVG. To date, no accounts associated with terrorists have been found. The GOSVG has not undertaken any specific initiatives focused on the misuse of charitable and nonprofit entities.

The GOSVG is a member of the Caribbean Financial Action Task Force (CFATF) and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The FIU became a member of the Egmont Group in 2003. The GOSVG is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The GOSVG has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the Inter-American Convention against Terrorism. The GOSVG has not signed the UN Convention against Corruption.

The GOSVG has strengthened its anti-money laundering regime through legislation and the establishment of an effective FIU. The GOSVG should insist that the beneficial owners of IBCs are known and listed in a registry available to law enforcement; immobilize all bearer shares; and properly supervise and regulate all aspects of its offshore sector. The GOSVG should continue to provide training to its regulatory, law enforcement, and FIU personnel in money laundering operations and

investigations. The GOSVG should pass civil forfeiture legislation and consider the utility of special investigative techniques.

## Switzerland

Switzerland is a major international financial center, with some 338 banks and a large number of nonbank financial intermediaries. Authorities suspect that Switzerland is vulnerable at the layering and integration stages of the money laundering process. Switzerland's central geographic location, relative political, social, and monetary stability, wide range and sophistication of available financial services, and long tradition of bank secrecy—first codified in 1934—are all factors that make Switzerland a major international financial center. These same factors also make Switzerland attractive to potential money launderers. However, Swiss authorities are aware of these issues and are sensitive to the importance of financial services to the Swiss economy. Total assets and liabilities in Swiss banking institutions were over 2.4 trillion Swiss francs ($1.8 trillion) in 2004, with foreigners accounting for over half of this figure. By comparison, Switzerland's GDP in 2004 was approximately $250 billion.

Reporting indicates that criminals attempt to launder proceeds in Switzerland from a wide range of illegal activities conducted worldwide, particularly financial crimes, narcotics trafficking, arms trafficking, organized crime, terrorism financing, and corruption. Although both Swiss and foreign individuals or entities conduct money laundering activities in Switzerland, narcotics-related money laundering operations are largely controlled by foreign narcotics trafficking organizations, often from the Balkans or Eastern Europe. Some of the money generated by Albanian narcotics trafficking rings in Switzerland has been funneled to armed Albanian extremists in the Balkans.

Swiss bank accounts also frequently figure in investigations of fraud and corruption of government officials and leaders, most often from foreign countries. Due to the large amount of foreign asset management within Switzerland, the likelihood of illicit funds being held in Switzerland is relatively high, despite measures taken to combat this phenomenon. Recent examples of public figures that have been the subject of money laundering allegations or investigations include a former President of Kyrgyzstan, a former Russian Minister of Atomic Energy, and the family of the Nigerian dictator Sani Abacha in connection with the funds (approximately$748 million) that Abacha had hidden in Swiss banks between 1993 and 1998. In June 2005, the former Swiss Ambassador to Luxembourg was sentenced to three and a half years in jail for money laundering and other crimes.

The Financial Action Task Force (FATF) conducted a mutual evaluation of Switzerland's anti-money laundering and counterterrorist financing regime in 2005. The mutual evaluation report (MER) concluded that Switzerland was at least partially compliant in most areas. However, the evaluators found Switzerland's anti-money laundering regime to be less than compliant with respect to correspondent banking and cash couriers.

Money laundering has been a criminal offense in Switzerland since 1998, when the Federal Act on the Prevention of Money Laundering in the Financial Sector (MLA) entered into effect. Swiss law, however, currently does not recognize certain types of criminal offenses as part of the eighty "serious crimes" that serve as predicate offenses for money laundering, including illegal trafficking in migrants, counterfeiting and pirating of products, smuggling, insider trading, and market manipulation. The adoption of anti-money laundering (AML) regulations planned for 2007 will make these crimes predicate offenses. Fiscal offenses do not constitute "serious crimes," so they are not considered to be predicate offenses.

Switzerland has significant AML legislation in place, subjecting banks and other financial intermediaries to strict know-your-customer (KYC) and reporting requirements, including the requirement to identify the beneficial owner of accounts. Negligence in this area is punishable under Swiss law. Switzerland has also implemented legislation for identifying, tracing, freezing, seizing, and

forfeiting narcotics-related assets. Legislation that aligns the Swiss supervisory arrangements with the Basel Committee's "Core Principles for Effective Banking Supervision" is contained in the Swiss Money Laundering Act.

Swiss money laundering laws and regulations apply to both banks and nonbank financial institutions. The Federal Banking Commission (FBC), the Federal Office of Private Insurance, and the Swiss Federal Gaming Board serve as the primary oversight authorities for a number of financial intermediaries, including banks, securities dealers, insurance institutions, and casinos. Other financial intermediaries are required to either come under the direct supervision of the Money Laundering Control Authority (MLCA) of the Federal Finance Department or join an accredited self-regulatory organization (SRO). SROs are nongovernmental self-regulating organizations authorized by the Swiss government to oversee implementation of AML measures by their members. SROs must be independent of the management of the intermediaries they supervise and must enforce compliance with due diligence obligations. Noncompliance can result in a fine or a revoked license. About 6,000 financial intermediaries are associated with SROs; the majority of these are financial management companies.

The Swiss Bankers Association (SBA) had employed customer due diligence (CDD) provisions as part of the industry standard in its Code of Conduct prior to any anti-money laundering legislation. The Code of Conduct was implemented by the SBA and enforced by the FBC, the supervisory authority over the banks. The FBC later implemented a "Policy on Prevention and Fight Against Money Laundering," establishing guidelines for the banking industry to employ in fighting money laundering. With the MLA, the Code of Conduct, CDD provisions and money laundering policy were extended to the entire financial sector. The Swiss Federal Banking Commission's AML regulations were revised in 2002 and became effective in 2003. These regulations, aimed at the banking and securities industries, codify a risk-based approach to suspicious transaction and client identification and install a global know-your-customer risk management program for all banks, including those with branches and subsidiaries abroad. In the case of higher-risk business relationships, additional investigation by the financial intermediary is required. The regulations require increased due diligence in the cases of politically exposed persons by ensuring that decisions to commence relationships with such persons be undertaken by at least one member of the senior executive body of a firm. All provisions apply to correspondent banking relationships as well. Swiss banks may not maintain business relationships with shell banks (banks with no physical presence at their place of incorporation), but there is no requirement that banks ensure that foreign clients do not authorize shell banks to access their accounts in Swiss banks.

The 2002 Banking Commission regulations mandate that all cross-border wire transfers must contain identifying details about the funds' remitters, though banks and other covered entities may omit such information for "legitimate reasons." The Federal Banking Commission has said that there are no plans at the moment to follow EU regulations aimed at registering names, addresses, and account numbers of those making even small money transfers between EU member states.

In July 2003, the government-sponsored Zimmerli Commission, tasked by the Department of Finance with examining reform of finance market regulators, presented 46 recommendations. Among the most far-reaching of these was the recommendation to merge the Federal Banking Commission and the Federal Office for Private Insurance-the institutions supervising the banking and insurance sectors-into a single, integrated financial market supervision body, to be called FINMA. In November 2004, the Cabinet instructed the Department of Finance to draft a parliamentary bill providing for the establishment of FINMA. Under the Cabinet's proposal, MLCA would also be included within FINMA. The draft bill is expected to be adopted by Parliament during the 2007 winter session, and enforced 12-18 months later, possibly by the end of 2008.

Switzerland's banking industry offers the same account services for both residents and nonresidents. Banks offer certain well-regulated offshore services, including permitting nonresidents to form offshore companies to conduct business, which can be used for tax reduction purposes. Pursuant to an agreement signed by the EU and Switzerland in 2004, EU residents have tax withheld on interest payments from savings accounts. This measure, enacted in concert with the EU's Savings Directive (2003/48/EC), was implemented on July 1, 2005, and may reduce the use of Swiss bank accounts by EU residents.

Swiss commercial law does not recognize any offshore mechanism per se and its provisions apply equally to residents and nonresidents. The stock company and the limited liability company are two standard forms of incorporation offered by Swiss commercial law. The financial intermediary is required to verify the identity of the beneficial owner of the stock company and must also be informed of any change regarding the beneficial owner. Bearer shares may be issued by stock companies but not by limited liability companies.

Switzerland has duty free zones. The customs authorities supervise the admission into and the removal of goods from customs warehouses. Warehoused goods may only undergo manipulations necessary for their maintenance, such as repacking, splitting, sorting, mixing, sampling and removal of the external packaging. Any further manipulation is subject to authorization. Goods may not be manufactured in the duty free zones. Swiss law has full force in the duty free zones; for example, export laws on strategic goods, war material, and medicinal products, as well as laws relating to anti-money laundering prohibitions, all apply. In view of the fact that customs authorities may and frequently do enter any customs warehouse area they choose, they believe they would be aware of the nature of any "value added" activity taking place in duty free zones.

Switzerland ranks fifth in the highly profitable artwork trading market, exporting $686 million worth of artwork worldwide in 2004. The Swiss market offers opportunities for organized crime to transfer stolen art or to use art to launder criminal funds. The United States is Switzerland's most important trading partner in this area, having purchased $253 million worth of art from Swiss sources in 2004. The 2003 Cultural Property Transfer Act, implemented in 2005, codifies in Swiss law elements of the 1970 United Nations Educational, Scientific, and Cultural Organization (UNESCO) Convention. This measure increases from five to thirty years the time period during which stolen pieces of art may be confiscated from those who purchased them in good faith. The law also allows police forces to search bonded warehouses and art galleries.

In January 2005, the Federal Council submitted a proposal for revisions based on the amended FATF Recommendations; the Federal Council revised this proposal in September. The October FATF mutual evaluation followed, and identified areas for improvement. In September 2006, the Federal Council instructed the Federal Department of Finance (FDF) to submit two papers addressing the FATF's proposal for improvements in the Swiss system; the proposal is designed to keep Swiss money laundering legislation current in the face of new challenges posed by international financial crime and to allow Swiss legislation to more thoroughly conform to international standards. The first paper, released at the end of 2006, addressed the proposal for revision of insider criminal law provisions on an accelerated basis. The second, due in mid-2007, will address other points from the FATF proposal. These points include: the creation of new predicate offenses for money laundering; the extension of the MLA to terrorist financing; the introduction of the obligation to report, if money laundering is suspected, that which prevents the establishment of a business relationship; and better legal protections against reprisals for financial intermediaries who report suspected money laundering. The paper also seeks to add some measures, including the introduction of an information system on cross-border transportation of currency valued in excess of CHF 25,000 ($20,500); the obligation to verify identification for financial intermediaries of representatives of legal entities; the obligation for the financial intermediary to establish the purpose and nature of the business relationship desired by the customer; and unlimited extension of the ban on tipping-off.

Established in 1998 by the MLA, the Money Laundering Reporting Office Switzerland (MROS) is Switzerland's financial intelligence unit (FIU), charged with receiving, processing and disseminating suspicious transaction reports (STRs). Although it is located in the Federal Office of Police, MROS is an administrative unit and does not have any investigative powers of its own, nor can it obtain additional information from reporting entities after receiving a STR. Under the MLA, MROS has five working days to process reports. In 2005, MROS received 729 reports involving approximately $536 million, an 11.2 per cent decrease in the number of reports compared to 2004. Whereas the decline in the number of reports in 2004 was mainly in the category of money transmitters, the decrease in 2005 was evident in nearly all categories of regulated entities. Unlike in the period 2002-2004, in 2005 the number of STRs filed by banks decreased.

Under the 2002 Efficiency Bill, the Swiss Attorney General is vested with the power to prosecute crimes addressed by Article 340bis of the Swiss Penal Code, which also covers money laundering offenses. In the past, the individual cantons (administrative components of the Swiss Confederation) were charged with investigating money laundering offenses. Additional legislation, effective January 1, 2002, increased the effectiveness of the prosecution of organized crime, money laundering, corruption, and other white-collar crime, by increasing the personnel and financing of the criminal police section of the federal police office. The law confers on the federal police and Attorney General's Office the authority to take over cases that have international dimensions, involve several cantons, or which deal with money laundering, organized crime, corruption, or white collar crime.

If financial institutions determine that assets were derived from criminal activity, the assets must be frozen immediately until a prosecutor decides on further action. Examining magistrates may order accounts to be frozen. Under Swiss law, suspect assets may be frozen for five days while a prosecutor investigates the suspicious activity. Since the MLA entered into force, CHF 423m ($348 million) have been frozen. Articles 58-60 of the Criminal Code outline measures relation to the confiscation of illicitly-obtained assets. Switzerland cooperates with the United States to trace and seize assets, and has shared a large amount of funds seized with the U.S. Government (USG) and other governments. The Government of Switzerland has worked closely with the USG on numerous money laundering cases.

Revisions to the Swiss Penal Code regarding terrorist financing entered into force on October 1, 2003. Article 260quinquies of the Penal Code provides for a maximum sentence of five years' imprisonment for terrorist financing. Article 100quater of the Penal Code, also added in 2003, extends criminal liability for terrorist financing to include companies. The FATF 2005 mutual evaluation team found Switzerland to be "largely compliant" with FATF Special Recommendation II regarding the criminalization of terrorist financing. The FATF team noted, however, that the Swiss Penal Code criminalizes the financing of an act of criminal violence but not the financing of an individual, independent of a particular act.

Since September 11, 2001, Swiss authorities have been alerting Swiss banks and nonbank financial intermediaries to check their records and accounts against lists of persons and entities with links to terrorism. The accounts of these individuals and entities are to be reported to the Ministry of Justice as suspicious transactions. Based on the "state security" clause of the Swiss Constitution, the authorities have ordered banks and other financial institutions to freeze the assets of suspected terrorists and terrorist organizations on the United Nations Security Council Resolution 1267 Sanctions Committee's consolidated list.

Along with the U.S. and UN lists, the Swiss Economic and Finance Ministries have drawn up their own list of approximately 44 individuals and entities connected with international terrorism or its financing. Swiss authorities have thus far blocked about 82 accounts totaling $25 million from individuals or companies linked to Usama Bin Laden and al-Qaida under relevant UN resolutions. Switzerland has also participated in joint task forces targeting the financing of al-Qaida cells. The

Swiss Attorney General also separately froze 41 accounts representing approximately $25 million on the grounds that they were related to terrorism financing, but the extent to which these funds overlap with the UN consolidated list is not clear.

MROS received 20 STRs relating to terrorist financing in 2005; the aggregate sum of money associated with these reports was 46 million Swiss francs (approximately$58 million). This represents an increase over the 11 reports related to terrorist financing submitted in 2004; these 11 reports involved a total of 900,000 Swiss francs (approximately $700,000). The higher number of reports in 2005 can be explained by the fact that several reports involved the same people or families and that one report alone involved 28.5 million Swiss francs (approximately $36 million). With the exception of 2 cases, MROS forwarded all the reports to the respective law enforcement agencies, which, in 6 of the 18 cases, did not investigate further.

Switzerland has ratified the Council of Europe's Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and is a party to the UN International Convention for the Suppression of the Financing of Terrorism. Switzerland ratified the 1988 UN Drug Convention on September 14, 2005, and the UN Convention against Transnational Organized Crime on October 27, 2006. Switzerland has signed, but not yet ratified, the UN Convention against Corruption and the International Convention for the Suppression of Acts of Nuclear Terrorism.

Swiss authorities cooperate with counterpart bodies from other countries. Switzerland has a mutual legal assistance treaty in place with the United States, and Swiss law allows authorities to furnish information to U.S. regulatory agencies, provided it is kept confidential and used for law enforcement purposes. Switzerland has been a member of FATF since its inception, and helped to shape the CDD and identification standards that the FATF adopted. Switzerland is also actively involved with the Basel Committee on Banking Supervision, establishing through it in 1988 the first international code of conduct for banks to prevent abuse of the industry by money laundering. MROS is a member of the Egmont Group. Swiss legislation permits "spontaneous transmittal," a process allowing the Swiss investigating magistrate to signal to foreign law enforcement authorities the existence of evidence in Switzerland. The Swiss used this provision in 2001 to signal Peru that they had uncovered accounts linked to former Peruvian presidential advisor Vladimiro Montesinos. However, on the principles of dual criminality, Switzerland has no legal basis to grant mutual legal assistance to foreign states where money laundering is based on fiscal offenses, because these do not serve as predicate offenses for money laundering in Switzerland.

The Government of Switzerland has stated that it hopes to correct the country's image as a haven for illicit banking services and works to improve its oversight on the banking and financial service sectors . The Swiss believe that their system of self-regulation, which incorporates a "culture of cooperation" between regulators and banks, equals or outperforms that of other countries. The primary orientation of the Swiss system is the aversion of risk at the account-opening phase, where due diligence and know-your-customer procedures address the issues, rather than relying on an early-warning system on all filed transactions. The Swiss Government believes that because of the due diligence approach the Swiss have taken, there are fewer STRs filed than in some other countries. At the same time, in 2005 MROS forwarded 69 percent of the STRs to law enforcement for further investigation.

While generally positive, Switzerland's recent FATF mutual evaluation report nonetheless identified weaknesses in the Swiss anti-money laundering and counterterrorist financing regime, including problems with correspondent banking, identification of beneficial owners, and the cross-border transportation of currency. The Government of Switzerland should continue to improve on its regime by enacting the revisions developed in response to the FATF mutual evaluation. Switzerland should also continue to work toward full implementation of existing laws and regulations and should ratify the UN Convention against Corruption.

## Syria

Syria is not an important regional or offshore financial center, due primarily to its still under-developed private banking sector and the fact that the Syrian pound is not a fully convertible currency. However, there continue to be significant money laundering and terrorism financing vulnerabilities in Syria's financial and nonbank financial sectors that have not been addressed by necessary legislation or other government action. In addition, Syria's black market moneychangers are not adequately regulated, and the country's borders remain porous. Regional hawala networks are intertwined with smuggling and trade-based money laundering and raise significant concerns, including involvement in the finance of terrorism. Most of the indigenous money laundering threat involves Syria's political and business elite, whose corruption and extra-legal activities represent the biggest obstacle to Syria fully choking off money laundering and terrorist financing activities. Syria is ranked 97 out of 163 countries on Transparency International's 2006 Corruption Perception Index. The U.S. Department of State has designated Syria as a State Sponsor of Terrorism.

Syria's free trade zones also may provide an easy entry or transit point for the proceeds of criminal activities. There are seven free zones in Syria, serviced mostly by subsidiaries of Lebanese banks, including BLOM Bank, BEMO (Banque Europeenne Pour le Moyen-Orient Sal), and BBAC (Bank of Beirut and Arab Countries), with four additional public free zones scheduled to begin operation in 2007, including in Homs, Dayr al Zu, the Port of Tartous, and al-Hasakeh near the northeastern segment of the Syrian-Iraqi border.

An Iranian free trade zone is to be co-located within the Homs free trade zone, and a Chinese free trade zone will shortly be operating within the Adra free trade zone. In May 2005 the first private free zone was licensed to be established in al-Kesweh, a Damascus areas suburb, but has not started operations. The volume of goods entering the free zones is estimated to be in the billions of dollars and is growing, especially with the increasing demand for automobiles and automotive parts, which enter the zones free of customs tariffs before being imported into Syria. While all industries and financial institutions in the free zones must be registered with the General Organization for Free Zones, which is part of the Ministry of Economy and Trade, the Syrian General Directorate of Customs continues to lack strong procedures to check country of origin certification or the resources to adequately monitor goods that enter Syria through the zones. There are also continuing reports of Syrians using the free zones to import arms and other goods into Syria in violation of USG sanctions under the Syrian Accountability and Lebanese Sovereignty Act.

The banking sector is dominated by the Commercial Bank of Syria (CBS), which holds approximately 75 percent of all deposits and controls most of the country's foreign currency reserves. With growing competition from the private banks, the CBS and the country's four other specialized public banks—the Agricultural Cooperative Bank, the Industrial Bank, the Real Estate Bank, and the People's Credit Bank—have been preparing a broader range of retail services and more competitive interest rates.

However, these banks still primarily focus on financing Syria's ill-performing public enterprises. In April 2006 the U.S. Department of Treasury issued a final ruling that imposes a special measure against the CBS, along with its subsidiary, the Syrian Lebanese Commercial Bank, as a financial institution of "primary money laundering concern," pursuant to Section 311 of the USA PATRIOT Act, due to information that the CBS has been used by terrorists or persons associated with terrorist organizations, as a conduit for the laundering of proceeds generated from the illicit sale of Iraqi oil, and continued concerns that the CBS is exploited by criminal enterprises.

The Syrian Arab Republic Government (SARG) began taking steps to develop a private banking sector in April 2001, with Law No. 28, which legalized private banking, and Law No. 29, which established rules on bank secrecy. Bank of Syria and Overseas, a subsidiary of Lebanon's BLOM Bank, was the first private bank to open in Syria in January 2004. There are now seven private banks, including Banque BEMO Saudi Fransi, the International Bank for Trade and Finance, Bank Audi,

Arab Bank, Byblos Bank, and Syria Gulf Bank. The sector's total capitalization is more than approximately $300 million, reported an approximate 95 percent in growth in 2006 in their deposit accounts, and are playing an increasing role in providing the business sector with foreign currency to finance imports and as a source of credit for businesses and individuals. However, the sector's development is hampered by the continuing lack of human capacity in the finance sector, regulations that limit Syrian banks' ability to make money on their liquidity, and restrictions on foreign currency transactions. A new law was enacted in May 2005 that allows for the establishment of Islamic banks, and three have already obtained licenses, including the Syrian International Islamic Bank, the Al-Sham Islamic Bank, and the Al-Baraka Bank. While these Islamic banks are expected to begin operations by early 2007, they potentially face problems because of the lack of an adequate regulatory and auditing structure in Syria's finance sector.

Legislation approved in the last few years provides the Central Bank of Syria with new authority to oversee the banking sector and investigate financial crimes. The SARG passed Decree 59 in September 2003 to criminalize money laundering and create an Anti-Money Laundering Commission (Commission), which was established in May 2004. In response to international pressure to improve its anti-money laundering and counterterrorism financing (AML/CTF) regulations, the SARG passed Decree 33 in May 2005, which strengthens the Commission and empowers it to act as a Financial Intelligence Unit (FIU). The Decree finalized the Commission's composition to include the Governor of the Central Bank, a Supreme Court Judge, the Deputy Minister of Finance, the Deputy Governor for Banking Affairs, the SARG's Legal Advisor, and will include the Chairman of the Syrian Stock Market once the Market is operational.

Under Decree 33, all banks and nonfinancial institutions are required to file Suspicious Activity Reports (SARs) with the Commission for transactions over $10,000, as well as suspicious transactions regardless of amount. They are also required to use "know your customer" (KYC) procedures to follow up on their customers every three years and maintain records on closed accounts for five years. The chairmen of Syria's private banks continue to report that they are employing internationally recognized KYC procedures to screen transactions and also employ their own investigators to check suspicious accounts. Nonbank financial institutions must also file SARs with the Commission, but many of them continue to be unfamiliar with the requirements of the law. The Commission has organized workshops for these institutions over the past year, but more time is needed for the information to penetrate the market.

Once a SAR has been filed, the Commission has the authority to conduct an investigation, waive bank secrecy on specific accounts to gather additional information, share information with the police and judicial authorities, and direct the police to carry out a criminal investigation. In addition, Decree 33 empowers the Governor of the Central Bank, who is the chairman of the Commission, to share information and sign Memoranda of Understanding (MOUs) with foreign FIUs. In November 2005, the Prime Minister announced that the Commission had completed an internal reorganization, creating four specialized units to: oversee financial investigations; share information with other SARG entities including customs, police and the judiciary; produce AML/CTF guidelines and verify their implementation; and develop a financial crimes database.

Decree 33 provides the Commission with a relatively broad definition of what constitutes a crime of money laundering, but one that does not fully meet international standards. The definition includes acts that attempt to conceal the proceeds of criminal activities, the act of knowingly helping a criminal launder funds, and the possession of money or property that resulted from the laundering of criminal proceeds. In addition, the law specifically lists thirteen crimes that are covered under the AML legislation, including narcotics offenses, fraud, and the theft of material for weapons of mass destruction. It is unclear whether terrorist financing is a predicate offense for money laundering or otherwise punishable under Decree 33.

While a SAR is being investigated, the Commission can freeze accounts of suspected money launderers for a nonrenewable period of up to eighteen days. The law also stipulates the sanctions for convicted money launderers, including a three to six-year jail sentence and a fine that is equal to or double the amount of money laundered. Further, the law allows the SARG to confiscate the money and assets of the convicted money launderer. The Commission circulates among its private and public banks the names of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanction Committee's consolidated list, and it has taken action to freeze the assets of designated individuals, including freezing the assets of one Syrian individual listed on the 1267 list in 2006.

In the first 11 months of 2006, the Commission reported 162 suspicious transactions cases, 24 from banks, up from approximately 90 cases in 2005. The Commission has investigated and sent approximately 5 cases from 2005 and 33 cases in 2006 to the court system; however, all of these cases are still pending and there have not yet been arrests or convictions. Most Syrian judges are not yet familiar with the evidentiary requirements of the law. Furthermore, the slow pace of the Syrian legal system and political sensitivities are delaying quick adjudication of these issues. The Commission itself continues to be seriously hampered by human resource constraints, although it has increased its staff from six in 2005 to ten in 2006, and hopes to expand to 30 by the end of 2007. The Commission has also organized multiple training sessions, including with the World Bank, over the course of 2006, in Syria and abroad, on issues of AML/CTF detection. A small number of customs officials attended these sessions. However, the lack of expertise on AML/CTF issues, further undermined by a lack of political will, continues to impede effective implementation of existing AML/CTF regulations.

Although Decree 33 provides the Central Bank with a foundation to combat money laundering, most Syrians still do not maintain bank accounts or use checks, credit cards, or ATM machines. The Syrian economy remains primarily cash-based, and Syrians use moneychangers, some of whom also act as hawaladars, for many financial transactions. Estimates of the volume of business conducted in the black market by Syrian moneychangers range between $15-70 million a day. Even the SARG admits that it does not have visibility into the amount of money that currently is in circulation. The SARG has begun issuing new regulations to entice people to use the banking sector, including offering high interest certificates of deposit and allowing Syrians to access more foreign currency from banks when they are traveling abroad. The SARG also passed a Moneychangers Law in 2006 to try to regulate the sector, requiring moneychangers to receive a license. However, it is unlikely that black market currency transactions will enter the formal sector because the SARG has still not offered adequate incentives; there is a 25 percent tax on these transactions, inadequate enforcement mechanisms, and continuing restrictions on foreign currency transfers. The Commission does have the authority to monitor the sector under Decree 33, but it reports that as moneychangers have until the end of 2006 to license their operations, they have not yet begun investigating these operations. The hawaladars in Syria's black market remain a source of concern for money laundering and terrorist financing.

The SARG has not updated its laws regarding charitable organizations to include strong AML/CTF language. A promised updated draft law is still pending. The SARG decided at the end of 2004 to restrict charitable organizations to only distributing nonfinancial assistance, but the current laws do not require organizations to submit detailed financial information or information on their donors. While the Commission says that it is seeking to increase cooperation with the Ministry of Social Affairs and Labor, which is supposed to approve all charitable transactions, to-date this remains a largely unregulated area.

While the SARG maintains strict controls on the amount of money that individuals can take with them out of the country, there is a high incidence of cash smuggling across the Lebanese, Iraqi, and Jordanian borders. Most of the smuggling involves the Syrian pound, as a market for Syrian currency exists among expatriate workers and tourists in Lebanon, Jordan, and the Gulf countries. U.S. dollars are also commonly smuggled in the region. Some of the smuggling may involve the proceeds of narcotics and other criminal activity. In addition to cash smuggling, there also is a high rate of

commodity smuggling out of Syria, particularly of diesel fuel, prompted by individuals buying diesel domestically at the low subsidized rate and selling it for much higher prices in neighboring countries. There are reports that some smuggling is occurring with the knowledge of or perhaps even under the authority of the Syrian security services.

The General Directorate of Customs lacks the necessary staff and financial resources to effectively handle the problem of smuggling. And while it is has started to enact some limited reforms, including the computerization of border outposts and government agencies, problems of information-sharing remain. Customs also announced in 2005 that it planned to develop a special office to combat AML/CTF in coordination with the Ministry of Finance and Syria's security services, but this has not yet become operational. Additionally, Customs currently lacks the infrastructure to effectively monitor or control even the legitimate movement of currency across its borders. The Commission and Customs have developed a joint form for individuals to declare currency when entering or exiting the country, but it has not yet been implemented. Additionally, once the new form is in place, it will remain a voluntary procedure. To combat corruption among customs officers, the General Directorate of Customs announced in December 2005 that it planned to ban all cash transactions at the borders, including the payment of customs duties, and will replace cash transactions with a system that utilizes pre-paid cards; however these programs have still not been realized.

Syria is one of the fourteen founding members of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body. In 2006, Syria underwent a mutual evaluation by its peers in MENAFATF which will be released shortly. Syria participated as an observer at the Egmont Group meeting in June 2006 and has formally applied to become a full member. Syria is a party to the 1988 UN Drug Convention. In April 2005, it became a party to the International Convention on the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime.

While Syria has made some effort in 2006 to implement AML/CTF regulations that govern its formal financial sector, including ratifying a law to regulate black market currency transactions, nonbank financial institutions and the black market continue to be vulnerable to money laundering and terrorist financiers. Syria should continue to modify its AML/CTF legislation and enabling regulations so that they adhere to global standards. The General Directorate of Customs, the Central Bank, and the judicial system in particular continue to lack the resources and the political will to effectively implement AML/CTF measures. Although the SARG has stated its intention to create the technical foundation through which different government agencies could share information about financial crimes, this does not exist to date. Syria should ratify the UN Convention against Transnational Organized Crime. It should criminalize terrorist financing. In addition, it is doubtful that the SARG has the political will to punish terrorist financing, to classify what it sees as legitimate resistance groups as terrorist organizations, or to address the corruption that exists at the highest levels of government and business. All these issues remain obstacles to developing a comprehensive and effective AML/CTF regime in Syria.

## Taiwan

Taiwan's modern financial sector and its role as a hub for international trade make it susceptible to money laundering. Its location astride international shipping lanes makes it vulnerable to transnational crimes such as narcotics trafficking and smuggling. There is a significant volume of informal financial activity through unregulated nonbank channels. Most illegal or unregulated financial activities are related to tax evasion, fraud, or intellectual- property violations. According to suspicious activity reports (SARs) filed by financial institutions on Taiwan, the predicate crimes commonly linked to SARs include financial crimes, corruption, and other general crimes.

Taiwan's anti-money laundering legislation is embodied in the Money Laundering Control Act (MLCA) of April 23, 1997, which was amended in 2003. Its major provisions include a list of predicate offenses for money laundering, customer identification and record keeping requirements, disclosure of suspicious transactions, international cooperation, and the creation of a financial intelligence unit, the Money Laundering Prevention Center (MLPC). In 2006, the Ministry of Justice began drafting another amendment to the MLCA, which would revise the scope of predicate crimes for money laundering, among other proposed changes.

The Legislative Yuan (parliament) amended the MLCA in 2003 to expand the list of predicate crimes for money laundering, widen the range of institutions subject to suspicious transaction reporting, and mandate compulsory reporting to the MLPC of significant currency transactions of over New Taiwan Dollars (TDW)1 million (approximately $30,000). Between August 2003, when the amended MLCA came into force, and May 31, 2004, the MLPC received over one million such reports on currency transactions-with 99 percent of them reported electronically. In 2005, the MLPC received 1,028,834 currency transaction reports. As a result of the 2003 MLCA amendments, the list of institutions subject to reporting requirements was expanded, to include casinos, automobile dealers, jewelers, boat and plane dealers, real estate brokers, credit cooperatives, consulting companies, insurance companies, and securities dealers, as well as traditional financial institutions.

Taiwan also set up a single financial regulator, the Financial Supervisory Commission (FSC) on July 1, 2004. The FSC consolidates the functions of regulatory monitoring for the banking, securities, futures and insurance industries, and also conducts financial examinations across these sectors. In mid-December 2005, the FSC began an incentive program for the public to provide information on financial crimes. The reward for information on a financial case with fines of TDW 10 million (approximately $300,000) or at least a one-year sentence is up to TDW 500,000 (approximately $15,000). The reward for information on a case with a fine of between TDW 2-10 million (approximately $60,000-$300,000) or less than a one-year sentence is up to TDW 200,000 (approximately $6,000).

Two new articles added to the 2003 amendments to the MLCA granted prosecutors and judges the power to freeze assets related to suspicious transactions and gave law enforcement more powers related to asset forfeiture and the sharing of confiscated assets. The proposed second amendment to the MLCA would prolong the permitted period of freezing the proceeds of money laundering from 6 months to 1 ½ years. In terms of reporting requirements, financial institutions are required to identify, record, and report the identities of customers engaging in significant or suspicious transactions. There is no threshold amount specified for filing suspicious transaction reports. The time limit for reporting cash transactions of over TDW 1 million (approximately $39,000) is within five business days. Banks are barred from informing customers that a suspicious transaction report has been filed. Reports of suspicious transactions must be submitted to the MLPC within 10 business days after the transaction took place. From January to October 2006, the MLPC received 1,085 suspicious transaction reports and 443 of them resulted in prosecutions.

Institutions are also required to maintain records necessary to reconstruct significant transactions, for an adequate amount of time. Bank secrecy laws are overridden by anti-money laundering legislation, allowing the MPLC to access all relevant financial account information. Financial institutions are held responsible if they do not report suspicious transactions. In May 2004, the Ministry of Finance issued instructions requiring banks to demand two types of identification and to retain photocopies of the identification cards when bank accounts are opened upon request for a third party, in order to prove the true identity of the account holder. Individual bankers can be fined TDW 200,000-1 million ($7,800-$39,000) for not following the MLPA.

All foreign financial institutions and offshore banking units follow the same regulations as domestic financial entities. Offshore banks, international businesses, and shell companies must comply with the

disclosure regulations from the Central Bank, Bureau of Monetary Affairs (CB), and MLPC. These supervisory agencies conduct background checks on applicants for banking and business licenses. Offshore casinos and internet gambling sites are illegal. According to Taiwan's Central Bank of China (CBC), from January to August 2006, Taiwan hosted 33 local branches of foreign banks, two trust and investment companies, and 67 offshore banking units.

On January 5, 2006, the Offshore Business Unit (OBU) Amendment was ratified to allow expansion of OBU operations to the same scope as Domestic Business Units (DBU). This was done to assist China-based Taiwan businesspeople in financing their offshore business operations. DBUs engaging in cross-strait financial business must follow the regulations of the "Act Governing Relations between Peoples of the Taiwan Area and the Mainland Area" and "Regulations Governing Approval of Banks to Engage in Financial Activities between the Taiwan Area and the Mainland Area." The Competent Authority, as referred to in these Regulations, is the Ministry of Finance.

Taiwan prosecuted 688 cases involving money laundering from January to October 2006, compared with 947 cases involving financial crimes during the same period of 2005. Among the 688 cases, 631 involved unregistered stock trading, credit card theft, currency counterfeiting or fraud. Among the 57 other money laundering cases, 11 were corruption-related and one was drug-related.

Individuals are required to report currency transported into or out of Taiwan in excess of TDW 60,000 (approximately $1,850); or $10,000 in foreign currency; 20,000 Chinese renminbi; or gold worth more than $20,000. When foreign currency in excess of TDW 500,000 (approximately $15,400) is brought into or out of Taiwan, the bank customer is required to report the transfer to the Central Bank, though there is no requirement for Central Bank approval prior to the transaction. Prior approval is required, however, for exchanges between New Taiwan dollars and foreign exchange when the amount exceeds $5 million for an individual resident and $50 million for a corporate entity. Effective September 2003, the Directorate General of Customs assumed responsibility for providing the MLPC on a monthly basis with electronic records of travelers entering and exiting the country carrying any single foreign currency amounting to TDW 1.5 million (approximately $58,500). Starting August 1, 2006, those who transfer funds over TDW 30,000 at any bank in Taiwan must produce a photo ID and the bank must record the name, ID number and telephone number of the client.

The authorities on Taiwan are actively involved in countering the financing of terrorism. In 2003, a new "Counter-Terrorism Action Law" (CTAL) was drafted, although as of July 2006 it was still under review by the Legislative Yuan. The new law would explicitly designate the financing of terrorism as a major crime. Under the proposed CTAL, the National Police Administration, the MJIB, and the Coast Guard would be able to seize terrorist assets even without a criminal case in Taiwan. Also, in emergency situations, law enforcement agencies would be able to freeze assets for three days without a court order.

Assets and income obtained from terrorist-related crimes could also be permanently confiscated under the proposed CTAL, unless the assets could be identified as belonging to victims of the crimes. Taiwan officials currently have the authority to freeze and/or seize terrorist-related financial assets under the MLCA promulgated in 1996 and amended in February 2003 to cover terrorist finance activities. Under the Act, the prosecutor in a criminal case can initiate freezing assets, or without criminal charges, the freezing/seizure can be done in response to a request made under a treaty or international agreement.

The Bureau of Monetary Affairs (BOMA) has circulated to all domestic and foreign financial institutions in Taiwan the names of individuals and entities included on the UN 1267 Sanctions Committee's consolidated list. Taiwan and the United States have established procedures to exchange records concerning suspicious terrorist financial activities. After receiving financial terrorist lists from the American Institute in Taiwan, BOMA conveys the list to relevant financial institutions. Banks are required to file a report on cash remittances if the remitter/remittee is on a terrorist list. Although as

noted above Taiwan does not yet have the authority to confiscate the assets, the MLCA was amended to allow the freezing of accounts suspected of being linked to terrorism.

Alternative remittance systems, or underground banks, are considered to be operating in violation of Banking Law Article 29. Authorities in Taiwan consider these entities to be unregulated financial institutions. Foreign labor employment brokers are authorized to use banks to remit income earned by foreign workers to their home countries. These remittances are not regulated or reported. Thus, money laundering regulations are not imposed on these foreign labor employment brokers. However, if the brokers accept money in Taiwan dollars for delivery overseas in another currency, they are violating Taiwan law. It is also illegal for small shops to accept money in Taiwan dollars and remit it overseas. Violators are subject to a maximum of three years in prison, and/or forfeiture of the remittance and/or a fine equal to the remittance amount.

Authorities in Taiwan do not believe that charitable and nonprofit organizations in Taiwan are being used as conduits for the financing of terrorism, and there are currently no plans to investigate such entities further for terrorist financing. Such organizations are required to register with the government. The Ministry of Interior (MOI) is in charge of overseeing foundations and charities. In 2004 and in 2006, the MOI assigned public accountants to audit the financial management of nationwide foundations.

Article 3 of Taiwan's Free Trade Zone Establishment and Management Act defines a Free Trade Zone (FTZ) as a controlled district of an international airport or an international seaport approved by the Executive Yuan. The FTZ coordination committee, formed by the Executive Yuan, has the responsibility of reviewing and examining the development policy of the FTZ; the demarcation and designation of FTZs; and inter-FTZ coordination.

There are five FTZs in Taiwan which have opened since 2004, including Taipei Free Trade Zone, Taichung Free Trade Zone, Keelung Free Trade Zone, Kaohsiung Free Trade Zone, and Taoyuan Air Cargo Free Trade Zone. These FTZs were designated with different functions, so that Keelung and Taipei FTZs focus on international logistics; Taoyuan FTZ on adding value to high value added industries; Taichung FTZ on warehousing, transshipment and processing of cargo; and Kaohsiung FTZ on mature industrial clusters. According to the Center for Economic Deregulation and Innovation (CEDI) under the Council for Economic Planning & Development, by September 2006 there were 11 shipping and logistics companies listed in the Kaohsiung Free Trade Zone, seven logistics companies in Taichung Free Trade Zone, eight logistics and shipping companies in Keelung Free Trade Zone, one logistics company in Taipei Free Trade Zone, and 46 manufacturers and enterprises in Taoyuan Air Cargo Free Trade Zone. There is no indication that FTZs in Taiwan are being used in trade-based money laundering schemes or by the financiers of terrorism. According to Article 14 of the Free Trade Establishment and Management Act, any enterprise applying to operate within an FTZ shall apply to the management authorities of the particular FTZ by submitting a business operation plan, the written operational procedures for good control, customs clearance, and accounting operations, together with relevant required documents. Financial institutions may apply to establish a branch office inside the FTZ and conduct foreign exchange business, in accordance with the Banking Law of the ROC, Securities and Exchange Law, Statute Governing Foreign Exchange, and the Central Bank of China Act.

According to Taiwan's Banking Law and Securities Trading Law, in order for a financial institution to conduct foreign currency operations, Taiwan's Central Bank must first grant approval. The financial institution must then submit an application to port authorities to establish an offshore banking unit (OBU) in the free-trade zone. No financial entity has yet applied to establish such an OBU in any of the five free trade zones. An offshore banking unit may operate a related business under the Offshore Banking Act, but cannot conduct any domestic financial, economic, or commercial transaction in New Taiwan Dollars.

Taiwan has promulgated drug-related asset seizure and forfeiture regulations which provide that in accordance with treaties or international agreements, Taiwan's Ministry of Justice shall share seized assets with foreign official agencies, private institutions or international parties that provide Taiwan with assistance in investigations or enforcement. Assets of drug traffickers, including instruments of crime and intangible property, can be seized along with legitimate businesses used to launder money. The injured parties can be compensated with seized assets. The Ministry of Justice distributes other seized assets to the prosecutor's office, police or other anti-money laundering agencies. The law does not allow for civil forfeiture. In March, 2006, Taiwan authorities announced that they had confiscated $625 million, arrested 22 men and had frozen approximately NT$1.7 billion ($438 million), in the island's largest money laundering operation, A mutual legal assistance agreement between the American Institute in Taiwan (AIT) and the Taipei Economic and Cultural Representative Office in the United States (TECRO) entered into force in March 2002. It provides a basis for the law enforcement agencies of the people represented by AIT and TECRO to cooperate in investigations and prosecutions for narcotics trafficking, money laundering (including the financing of terrorism), and other financial crimes.

Although Taiwan is not a UN member and cannot be a party to the 1988 UN Drug Convention, the authorities in Taiwan have passed and implemented laws in compliance with the goals and objectives of the Convention. Similarly, Taiwan cannot be a party to the UN International Convention for the Suppression of the Financing of Terrorism, as a nonmember of the United Nations, but it has agreed unilaterally to abide by its provisions. Taiwan is a founding member of the Asia/Pacific Group on Money Laundering (APG) and in 2005, was elected to the APG steering committee. The MLPC is a member of the Egmont Group of Financial Intelligence Units. The Investigation Bureau of the Ministry of Justice expanded information exchanges with various countries/jurisdictions from 17 jurisdictions in 2004 to 20 in 2005.

Over the past five years, Taiwan has created and implemented an anti-money laundering regime that comports with international standards. The MLCA amendments of 2003 address a number of vulnerabilities, especially in the area of asset forfeiture. The authorities on Taiwan should continue to strengthen the existing anti-money laundering regime as they implement the new measures. Taiwan should endeavor to pass the proposed Counter-Terrorism Action Law to better address terrorist financing issues. The authorities on Taiwan should also enact legislation regarding alternate remittance systems. Taiwan should enact legislation pending since 2003 that explicitly criminalizes the financing of terrorism.

## Tanzania

Tanzania is not an important regional financial center. Tanzania, however, is vulnerable to money laundering. Tanzania has weaknesses in its anti-money laundering/counterterrorism financing (AML/CTF) regime, specifically in its financial institutions and law enforcement capabilities. A weak financial sector along with an under-trained, under-funded law enforcement apparatus and the lack of a functioning financial intelligence unit (FIU) make money laundering impossible to track and prosecute. Real estate and used car businesses appear to be vulnerable trade industries involved in money laundering. With little or lax regulations and enforcement, the emerging casino industry is becoming an area of concern for money laundering. Money laundering is even more likely to occur in the informal nonbank financial sector, as opposed to the formal sector, which is largely undeveloped. Front companies are used to launder funds including hawaladars and bureaux de change, especially on the island of Zanzibar, where few federal regulations apply. Officials indicate that money laundering schemes in Zanzibar generally take the form of foreign investment in the tourist industry and bulk cash smuggling. The likely sources of illicit funds are from Asia and the Middle East and, to a lesser extent, Europe. Such transactions rarely include significant amounts of U.S. currency. There are no

indications that Tanzania's two free trade zones are being used in trade-based money laundering schemes or by financiers of terrorism.

The Proceeds of Crime Act of 1991 criminalizes narcotics-related money laundering; however, the Act does not adequately define money laundering. The law has been used only to prosecute corruption cases and over the past year there have been no arrests or prosecutions for money laundering or terrorist financing. The law requires financial institutions to maintain records of financial transactions exceeding 100,000 shillings (approximately $109) for a period of 10 years.

Current law does not include due diligence or negligence laws for banks. If an institution has reasonable grounds to believe that a transaction relates to money laundering, it may communicate this information to the police for investigation, although such reporting is voluntary, not mandatory. The Central Bank, the Bank of Tanzania (BOT), has issued regulations requiring financial institutions to file suspicious transaction reports (STRs), but this requirement is not being enforced, and no mechanism currently exists for receiving and analyzing the STRs.

The 2002 Prevention of Terrorism Act criminalizes terrorist financing. It requires all financial institutions to inform the government each quarter in a calendar year of any assets or transactions that may be associated with a terrorist group. The implementing regulations for this provision have not yet been drafted. Under the Act, the government may seize assets associated with terrorist groups. The BOT circulates to Tanzanian financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanction Committee's consolidated list, but to date no assets have been frozen under this provision. In 2004, the Government of Tanzania (GOT) took action against one charitable organization on the list by closing its offices and deporting its foreign directors; however, it is not clear whether Tanzania has the investigative capacity to identify and seize related assets. Tanzania has cooperated with the U.S. in investigating and combating terrorism and exchanges counterterrorism information. There are no specific laws in place allowing Tanzania to exchange records with the U.S. on narcotics transactions or narcotics-related money laundering.

Tanzania made progress in 2006 with its proposed anti-money laundering (AML) legislation. The national multi-disciplinary committee, established with the help of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), finalized the AML bill in 2005 after gaining input from a wide range of stakeholders. In June 2006, President Kikwete's Cabinet approved the AML bill and tabled it in Parliament. Reportedly, officials expect Parliament to pass the bill by February 2007. Among its other provisions, the proposed legislation provides for the creation of a FIU that will collect mandatory suspicious transaction reporting from financial institutions and will be empowered to share this information with other FIUs and foreign law enforcement agencies.
Money laundering controls and reporting requirements do not currently apply to nonbank financial institutions, such as cash couriers, casinos, hawaladars and bureaux de change. The draft AML bill includes the expansion of money laundering controls to cover such institutions. Currently, the BOT supervises bureaux de change through the use of annual audits and inspections, while the National Gaming Authority supervises casinos and other gaming activities involving large sums of money, including lotteries. There are no legal requirements for nonbank financial institutions to report suspicious transactions. There is currently no cross-border currency reporting requirement, even for cash couriers, although the Proceeds of Crime Act does characterize cash smuggling as a "predicate offense." The draft AML bill includes strengthened provisions to criminalize cash smuggling in and out of Tanzania.

The GOT is a party to the 1988 UN Drug Convention; the UN International Convention for the Suppression of the Financing of Terrorism; and the UN Convention Against Corruption. In May 2006, the GOT became a party to the UN Convention against Transnational Organized Crime. In 2006, Tanzania was listed 93 out of 163 countries in Transparency International's Corruption Perception Index. Tanzania is a member of ESAAMLG and continues to play a leading role in the operation of

this FATF-style regional body. Tanzania also continues to host the annual ESAAMLG task force meetings and has detailed personnel to the ESAAMLG Secretariat which it hosts.

The Government of Tanzania should enact and implement the anti-money laundering law that has been under review for several years. Tanzania should also increase the reporting requirements for informing the government of assets or transactions that may be associated with a terrorist group. Currently the GOT requires quarterly reporting requirements regarding terrorist financing. The importance of stopping terrorist acts should mandate a shorter reporting interval in this arena. The GOT should continue to work through the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) to establish the FIU mandated in the draft law and to develop a comprehensive anti-money laundering regime that comports with international standards. Per the Financial Action Task Force Special Recommendation Nine, the GOT should enact mandatory cross-border currency reporting requirements. Tanzania should also enact and enforce anti-money laundering regulations within the casino industry.

## Thailand

Thailand is vulnerable to money laundering from its significant underground economy as well as from all types of cross-border crime including illicit narcotics, contraband, and smuggling. Money launderers use both the banking and nonbanking financial institutions and private businesses to move funds from narcotics trafficking and other criminal enterprises. As the amount of opium and heroin produced in the Golden Triangle region of Burma, Laos, and Thailand decreased during the past decade, drug traffickers transitioned to importing and distributing methamphetamine tablets, and began using commercial banks to hide and move their proceeds. Thailand is a significant destination and source country for international migrant smuggling and trafficking in persons, a production and distribution center for counterfeit consumer goods, and increasingly a center for the production and sale of fraudulent travel documents. Banks and alternative remittance systems are illegally used to shelter and move funds produced by all of these activities as well as by illegal gambling and prostitution. The majority of reported money laundering cases is narcotics-related, and there is no pervasive evidence of money laundering ties in Thailand with international terrorist groups. The Thai black market for smuggled goods includes pirated goods as well as automobiles from neighboring nations.

Thailand's anti-money laundering legislation, the Anti-Money Laundering Act (AMLA) B.E. 2542 (1999), criminalizes money laundering for the following predicate offenses: narcotics trafficking, trafficking in women or children for sexual purposes, fraud, financial institution fraud, public corruption, customs evasion, extortion, public fraud, blackmail, and terrorist activity. On August 11, 2003, as permitted by the Thai constitution, the Royal Thai Government (RTG) issued two Emergency Decrees to enact measures related to terrorist financing that had been under consideration by the Executive Branch and Parliament for more than a year and a half. The first of these Decrees amended Section 135 of the Penal Code to establish terrorism as a criminal offense. The second Decree amended Section 3 of the AMLA to add the newly established offense of terrorism and terrorist financing as an eighth predicate offense for money laundering. The Decrees took effect when they were published. Parliament endorsed their status as legal acts in April 2004.

The current list of predicate offenses in the AMLA does not comport with international best practices, consistent with Recommendations 1 and 2 of the Forty Recommendations of the Financial Action Task Force (FATF), to apply the crime of money laundering to all serious offenses or with the minimum list of acceptable designated categories of offenses. Additionally, the definition of "property involved in an offense" in the AMLA is limited to proceeds of predicate offenses and does not extend to instrumentalities of a predicate offense or a money laundering offense. Proposed amendments pending with the Cabinet since 2004 would expand the list of predicate offenses to include

environmental crimes, foreign exchange violations, illegal gambling, arms trafficking, labor fraud, bid rigging, share manipulation, and excise tax offenses. However, even with the enactment of these additional predicate offenses, the list will still be deficient under international standards as it excludes, among other crimes, murder, migrant smuggling, counterfeiting, and intellectual property rights offenses. The proposed amendments to AMLA would also create a forfeiture fund and authorize international asset sharing with cooperating jurisdictions.

The AMLA created the Anti-Money Laundering Office (AMLO). Among other functions it serves as Thailand's financial intelligence unit (FIU), which became fully operational in 2001. When first established, AMLO reported directly to the Prime Minister. In October 2002, pursuant to a reorganization of the executive branch following criticisms that AMLO had been politicized, AMLO was designated as an independent agency under the Minister of Justice. AMLO receives, analyzes, and processes suspicious and large transaction reports, as required by the AMLA. In addition, AMLO is responsible for investigating money laundering cases for civil forfeiture and for the custody, management, and disposal of seized and forfeited property. AMLO is also tasked with providing training to the public and private sectors concerning the AMLA. The law also created the Transaction Committee, which operates within AMLO to review and approve disclosure requests to financial institutions and asset restraint/seizure requests. The AMLA also established the Anti-Money Laundering Board, which is comprised of ministerial-level officials and agency heads and serves as an advisory board that meets periodically to set national policy on money laundering issues and to propose relevant ministerial regulations.

AMLO, the Royal Thai Police (RTP) Special Branch, and the Royal Thai Police Crimes Suppression Division are responsible for investigating financial crimes. They initiated 1,215 financial crimes investigations in 2005 resulting in a total of 57 convictions. During the 2006 fiscal year (10/05-09/06), AMLO prosecuted 79 cases of civil asset forfeiture and realized Bt459 million or $11.8 million. Eleven cases remain under investigation. In criminal cases, the forfeiture and seizure of assets is governed by the 1991 Act on Measures for the Suppression of Offenders in an Offense relating to Narcotics (Assets Forfeiture Law). The Property Examination Committee has filed 1,865 cases with assets valued at 1.64 billion baht (approximately $4 million) and 1,644 cases are on trial. Thai authorities seized the equivalent of $18.7 million in nonterrorist assets during 2005, compared to $16.52 million in 2004, and $56.3 million in 2003. The high success rate in 2003 occurred during the Prime Minister's much-criticized war on drugs that year, in which more than 2,000 extra-judicial killings occurred.

The Ministry of Justice also houses a criminal investigative agency, the Department of Special Investigations (DSI), which is separate from the RTP although many DSI personnel originally were RTP officers. DSI has responsibility for investigating the criminal offense of money laundering (as distinct from civil asset forfeiture actions carried out by AMLO), and for many of the money laundering predicates defined by the AMLA, including terrorism. The DSI, AMLO, and the RTP all have authority to identify, freeze, and/or forfeit terrorist finance-related assets.

AMLO shares information with other Thai law enforcement agencies and vice versa. It has a memorandum of understanding with the Royal Thai Customs, pursuant to which Royal Thai Customs shares information and evidence of smuggling and customs evasion involving goods or cash exceeding Bt 1 million (approximately USD25,600).

The AMLA requires customer identification, record keeping, the reporting of large and suspicious transactions, and provides for the civil forfeiture of property involved in a money laundering offense. Financial institutions are also required to keep customer identification and specific transaction records for a period of five years from the date the account was closed, or from the date the transaction occurred, whichever is longer. Reporting individuals (banks and others) who cooperate with law enforcement entities are protected from liability. Thailand does not have stand-alone secrecy laws but

the Commercial Bank Act B.E. 2505 (1962), regulated by Bank of Thailand, has a provision providing for bank secrecy to prevent disclosure of client financial information. However, AMLA overrides this provision. Therefore, financial institutions must disclose their client and ownership information to AMLO if requested. .

The Bank of Thailand (BOT), Securities and Exchange Commission (SEC), and AMLO are empowered to supervise and examine financial institutions for compliance with anti-money laundering/counterterrorist financial laws and regulations. Although the Bank of Thailand regulates financial institutions in Thailand, bank examiners are prohibited, except under limited circumstances, from examining the financial transactions of a private individual. This prohibition acts as an impediment to the BOT's auditing of a financial institution's compliance with the AMLA or BOT regulations. Besides this lack of power to conduct transactional testing, BOT does not currently examine its financial institutions for anti-money laundering compliance. The BOT is working closely with AMLO to train officers in conducting compliance audits, and in 2007 AMLO is expecting to setup an on-and-off site audit team with assistance from the BOT, although no such audits have yet to occur.

Anti-money laundering controls are also enforced by other Royal Thai Government regulatory agencies, including the Board of Trade and the Department of Insurance. Financial institutions that are required to report suspicious activities are broadly defined by the AMLA as any business or juristic person undertaking banking or nonbanking business. The land registration offices are also required to report on any transaction involving property of Bt5 million or greater, or a cash payment of Bt2 million or greater, for the purchase of real property.

The Exchange Control Act of B.E. 2485 (1942) states that foreign currencies can be brought into Thailand without limit. However, any person receiving foreign currencies is required to surrender foreign currencies to an authorized bank or to deposit the same in a foreign currency account within 7 days from receipt, except foreigners temporarily staying in Thailand for not more than three months, foreign embassies, and international organizations. (In November 2006, the BOT amended the surrender period from 7 days to 15 days but the amendment is pending the Ministry of Finance's approval.) Meanwhile, there is no restriction on the amount of Thai currency (Baht) that may be brought into the country. However, a person traveling to Thailand's bordering countries including Vietnam is allowed to take out Thai Baht up to Bt500,000 or $12,820 and to other countries up to Bt50,000 ($1,282) without authorization.

Thailand is not an offshore financial center nor does it host offshore banks, shell companies, or trusts. Licenses were first granted to Thai and foreign financial institutions to establish Bangkok International Banking Facilities (BIBFs) in March 1993. BIBFs may perform a number of financial and investment banking services, but can only raise funds offshore (through deposits and borrowing) for lending in Thailand or offshore. The United Nations Drug Control Program and the World Bank listed BIBFs as potentially vulnerable to money laundering activities, because they serve as transit points for funds. BIBFs are subject to the AMLA. However, in mid October 2006, the last BIBF license was returned to the Bank of Thailand due to the BOT's "one presence" policy for all financial institutions. Some of these qualified stand alone BIBFs have upgraded to either full branches or subsidiaries, while Thai commercial banks with BIBF licenses had to surrender their licenses to the BOT. Most BIBFs simply exited the market.

The Stock Exchange of Thailand (SET) requires securities dealers to have "know your customer" procedures; however, the SET does not check anti-money laundering compliance during its reviews. The Department of Insurance (DOI), under the Ministry of Commerce, is responsible for the supervision of insurance companies, which are covered under the AMLA definition of a financial institution, but there are no anti-money laundering regulations for the insurance industry. Similarly, the Cooperative Promotion Department (CPD) is responsible for supervision of credit cooperatives,

which are required under the Cooperatives Act to register with the CPD. Currently, around 6,000 cooperatives are registered, with approximately 1,348 thrift and credit cooperatives engaged in financial business. Thrift and credit cooperatives are engaged in deposit taking and providing loans to the members, and are covered under the definition of a financial institution, but, as with the securities and insurance sectors, there are no anti-money laundering compliance mechanisms currently in place.

Financial institutions (such as banks, finance companies, savings cooperatives, etc.), land registration offices, and persons who act as solicitors for investors, are required to report significant cash, property, and suspicious transactions. Reporting requirements for most financial transactions (including purchases of securities and insurance) exceeding Bt2 million (approximately $52,000), and property transactions exceeding Bt5 million (approximately $130,000), have been in place since October 2000. In 2007, the AMLO Board will again consider the issuance of an announcement or regulation to subject gold shops, jewelry stores, and car dealers to either mandatory transactional reporting requirements and/or suspicious transactions reporting requirements. Previous proposals would have imposed mandatory reporting requirements regarding transactions with nonregular customers involved in business transactions worth more than Bt1 million (or $25,600) or would have imposed mandatory reporting requirements on shops engaging in annual transactions in excess of Bt 100 million (or $2,560,000). The relevant ministries and regulatory authorities would then issue orders consistent with the AMLO Board pronouncement. Thailand has more than 6,000 gold shops and 1,000 gem traders that would be subject to these reporting requirements.

Thailand acknowledges the existence and use of alternative remittance systems (hawala, etc.) that attempt to circumvent financial institutions. There is a general provision in the AMLA that makes it a crime to transfer, or to receive a transfer, that represents the proceeds of a specified criminal offense (including terrorism). Remittance and money transfer agents, including informal remittance businesses, require a license from the Ministry of Finance. Guidelines issued in August 2004 by the Ministry of Finance and the BOT prescribe that before the grant of a license, both money changers and money transfer agents are subject to onsite examination by the BOT, which also consults with AMLO on the applicant's criminal history and AML record. At present, moneychangers have to report financial transactions to the Anti-Money Laundering Office while remittance agents do not. Licensed agents are subject to monthly transaction reporting and a 3-year record maintenance requirement. At present, there are about 270 authorized moneychangers and five remittance agents. The Bank of Thailand limited in 2004 the annual transaction volume for agents to $60,000 for offices in the Bangkok area and $30,000 for offices located in other areas. Moneychangers frequently act as illegal remittance agents.

Money and property may be seized under Section 3 of the AMLA if derived from commission of a predicate offense, from aiding or abetting commission of a predicate offense, or if derived from the sale, distribution, or transfer of such money or asset. AMLO is responsible for tracing, freezing, and seizing assets. Instruments that are used to facilitate crime such as vehicles or farms (when not proceeds) cannot be forfeited under AMLA and are subject to seizure under the Criminal Asset Forfeiture Act of 1991, and unlike the AMLA, require a criminal conviction as a pre-requisite to a final forfeiture. The AMLA makes no provision for substitute seizures if authorities cannot prove a relationship between the asset and the predicate offense. Overall, the banking community in Thailand provides good cooperation to AMLO's efforts to trace funds and seize/freeze bank accounts.

The Bank of Thailand (BOT) does not have any regulations that give it explicit authorization to control charitable donations, but it is working with AMLO to monitor these transactions under the Exchange Control Act of 1942.

In 2004, Regulations on Payment of Incentives and Rewards in Proceedings Against Assets Under the Anti-Money Laundering Act went into effect in Thailand. Under this system, investigators from AMLO and other investigative agencies receive personal commissions on the property they seize that

is ultimately forfeited. The United States as well as several other countries and international organizations, including the UNODC, have criticized this system of personal rewards on the grounds that it threatens the integrity of its AML regime and creates a conflict of interest by giving law enforcement officers a direct financial stake in the outcome of forfeiture cases. The United States and others have called on the RTG to rescind the reward regulation. Despite continuing promises to end the system of personal commissions to law enforcement officers, Thailand has been disappointingly slow to address and correct this discredited practice. As a consequence, the U.S. Government (USG) has ceased providing training and other assistance to AMLO while the rewards practice remains in place. However, in November 2006, the Minister of Justice recommended that the Prime Minister rescind the reward regulation, and the U.S. is encouraged that appropriate action will occur in early 2007 to eliminate this system.

Thailand is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed (December 2000), but not yet ratified, the UN Convention against Transnational Organized Crime. It has also signed (December 2003), but not yet ratified the UN Convention against Corruption. Implementing legislation must be enacted before Thailand can ratify either Convention. The RTG has issued instructions to all authorities to comply with UNSCR 1267, including the freezing of funds or financial resources belonging to suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list. To date, Thailand has not identified, frozen, and/or seized any assets linked to individuals or entities included on the UNSCR 1267 Sanctions Committee's consolidated list. However, AMLO has identified some suspicious transaction reports derived from financial institutions as possibly terrorist-related and has initiated investigations of possible terrorist activities using nongovernmental or nonprofit organizations as a front.

Thailand has Mutual Legal Assistance Treaties (MLATs) with 10 countries, including the United States and is a party to the regional ASEAN Mutual Legal Assistance Agreement. AMLO has memoranda of understanding on money laundering cooperation with 27 other financial intelligence units (Belgium, Brazil, Lebanon, Indonesia, Romania, UK, Finland, Republic of Korea, Australia, Portugal, Andorra, Estonia, Italy, Philippines, Poland, Mauritius, Netherlands, Georgia, Monaco, Malaysia, Bulgaria, St. Vincent and the Grenadines, Ukraine, Myanmar, Nigeria, Japan, and Ireland). AMLO is currently pursuing FIU agreements with 15 more FIUs. It nonetheless actively exchanges information with nations with which it has not entered into an MOU, including the United States, Singapore, and Canada. Thailand cooperates with USG and other nations' law enforcement authorities on a range of money laundering and illicit narcotics related investigations. AMLO responded to 99 requests for information from foreign FIUs in 2005. Thailand became a member of the Asia/Pacific Group on Money Laundering (APG), a FATF-style regional body, in April 2001. The AMLO joined the FATF's Egmont Group of financial intelligence units in June 2001.

The Government of Thailand should continue to implement its anti-money laundering program. The money laundering law should be amended to include the minimum list of acceptable designated categories of offenses prescribed by FATF and to make the "structuring" of transactions an offense. While the AMLA already captures proceeds of crime, it should be amended to include instrumentalities of offenses. Nonbank financial institutions and businesses such as gold shops, jewelry stores and car dealers should be subject to suspicious transaction reporting requirement without regard to a threshold. The insurance and securities sectors should institute AML compliance programs. AMLO should undertake audits of financial institutions to ensure compliance with requirements of AMLA and AMLO regulations. Until the RTG provides a viable mechanism for all of its financial institutions to be examined for compliance with the AMLA, Thailand's anti-money laundering regime will not comport with international standards.

The RTG should develop and implement anti-money laundering regulations for exchange businesses and should take additional measures to address the vulnerabilities presented by its alternative

remittance systems. The RTG can further strengthen its anti-money laundering regime by promulgating cross border currency control regulations that are currently pending in the Office of Secretary of the Cabinet. Thailand should ratify the UN Convention against Transnational Organized Crime and the UN Convention Against Corruption. Thailand should also immediately rescind its rewards program for AMLO investigators who seize assets under the anti-money laundering laws, and for agents of other law enforcement agencies that engage in similar reward schemes, as it gives the appearance of impropriety, can imperil successful prosecutions, and will eventually impede international cooperation and undermine public support for Thailand's forfeiture regime and its credibility. The current "interim" government has declared that it will limit itself to a term of around one year (i.e. until September 2007) and focus on drafting a new constitution. Its willingness and ability to pass new anti-money laundering laws and regulations are, therefore, extremely constrained.

## Turkey

Turkey is an important regional financial center, particularly for Central Asia and the Caucasus, as well as for the Middle East and Eastern Europe. It continues to be a major transit route for Southwest Asian opiates moving to Europe. However, local narcotics trafficking organizations are reportedly responsible for only a small portion of the total funds laundered in Turkey.

Money laundering takes place in banks, nonbank financial institutions, and the underground economy. Money laundering methods in Turkey include: the cross-border smuggling of currency; bank transfers into and out of the country; trade fraud, and the purchase of high value items such as real estate, gold, and luxury automobiles. It is believed that Turkish-based traffickers transfer money and sometimes gold via couriers, the underground banking system, and bank transfers to pay narcotics suppliers in Pakistan or Afghanistan. Funds are often transferred to accounts in the United Arab Emirates, Pakistan, and other Middle Eastern countries. A substantial percentage of money laundering that takes place in Turkey involves fraud and tax evasion. Informed observers estimate that as much as 50 percent of the economy is unregistered. In 2005, the Government of Turkey (GOT) passed a tax administration reform law, with the goal of improving tax collection.

Turkey first criminalized money laundering in 1996. Under the law whoever commits a money laundering offense faces a sentence of two to five years in prison, and is subject to a fine of double the amount of the money laundered and asset forfeiture provisions. The Council of Ministers subsequently passed a set of regulations that require the filing of suspicious transaction reports (STRs), customer identification, and the maintenance of transaction records for five years.

In 2004, the GOT enacted additional anti-money laundering legislation, a new criminal law, and a new criminal procedures law. The new Criminal Law, which took effect in June 2005, broadly defines money laundering to include all predicate offenses punishable by one year's imprisonment. Previously, Turkey's anti-money laundering law comprised a list of specific predicate offenses. A new Criminal Procedures Law also came into effect in June 2005.

Under a Ministry of Finance banking regulation circular all banks, including the Central Bank, securities companies, post office banks, and Islamic financial houses are required to record tax identity information for all customers opening new accounts, applying for checkbooks, or cashing checks. The circular also requires exchange offices to sign contracts with their clients. The Ministry of Finance also mandates that a tax identity number be used in all financial transactions. The requirements are intended to increase the GOT's ability to track suspicious financial transactions. Turkey does not have bank secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement officials. According to anti-money laundering law Article 5, public institutions, individuals, and corporate bodies must submit information and documents as well as adequate supporting information upon the request of Turkey's Financial Crimes investigation Board (MASAK) or other authorities specified in Article 3 of the law. Individuals and corporate bodies from whom

information and documents are requested may not withhold the requested items by claiming the protection provided by privacy provisions in order to avoid submitting the requested items.

A new Banking Law was enacted in 2005 to strengthen bank supervision. The Banking Regulatory and Supervisory Agency (BRSA) conducts periodic anti-money laundering and compliance reviews under the authority delegated by MASAK. The number of STRs currently being filed is quite low, even taking into consideration the fact that many commercial transactions are conducted in cash. In 2005, 352 STRs were filed, up from 288 in 2004 and 177 in 2003. The 2006 statistics are not available.

Turkey does not have foreign exchange restrictions. With limited exceptions, banks and special finance institutions must inform authorities within 30 days, about transfers abroad exceeding $50,000 (approximately 71,300 Turkish new liras) or its equivalent in foreign currency notes (including transfers from foreign exchange deposits). Travelers may take up to $5,000 (approximately 7,130 Turkish new liras) or its equivalent in foreign currency notes out of the country. Turkey does have cross-border currency reporting requirements. Article 16 of the recently-enacted MASAK law (see below) gives customs officials the authority to sequester valuables of travelers who make false or misleading declarations and imposes fines for such declarations.

MASAK was established by the 1996 anti-money laundering law as part of the Ministry of Finance. MASAK became operational in 1997, and it serves as Turkey's Financial Intelligence Unit (FIU), receiving, analyzing, and referring STRs for investigation. MASAK has three functions: regulatory, financial intelligence, and investigative. MASAK plays a pivotal role between the financial community and Turkish law enforcement, investigators, and judiciary.

In October 2006, Parliament enacted a new law reorganizing MASAK along functional lines, explicitly criminalizing the financing of terrorism, and providing safe harbor protection to the filers of STRs. The law also expands the range of entities subject to reporting requirements, to include art dealers, insurance companies, lotteries, vehicle sales outlets, antique dealers, pension funds, exchange houses, jewelry stores, notaries, sports clubs, and real estate companies. It also specifies sanctions for failure to comply. The law gives MASAK the authority to instruct a number of different inspection bodies (such as the bank examiners, the financial inspectors or the tax inspectors) to initiate an investigation if MASAK has reason to suspect financial crimes. Likewise, MASAK can refer suspicious cases to the Public Prosecutor and the Public Prosecutor can ask MASAK to conduct a preliminary investigation prior to referring a case to the police for criminal investigation.

However, neither the current draft of the legislation, nor a June 2006 set of amendments to Turkey's antiterrorism laws, expanded upon Turkey's narrow definition of terrorism applicable only in terms of attacks on Turkish nationals or the Turkish state.

According to MASAK statistics, as of December 31, 2005 it had pursued 2,231 money laundering investigations since its 1996 inception, but fewer than ten cases resulted in convictions. Moreover, all of the convictions are reportedly under appeal. Most of the cases involve nonnarcotics criminal actions or tax evasion; as of December 31, 2005 41 percent of the cases referred to prosecutors were narcotics-related.

The GOT enforces existing drug-related asset seizures and forfeiture laws. MASAK, the Turkish National Police, and the courts are the government entities responsible for tracing, seizing and freezing assets. According to Article 9 of the anti-money laundering law, the Court of Peace—a minor arbitration court for petty offenses—has the authority to issue an order to freeze funds held in banks and nonbank financial institutions as well as other assets, and to hold the assets in custody during the preliminary investigation. During the trial phase, the presiding court has freezing authority. Public Prosecutors may freeze assets in cases where it is necessary to avoid delay. The Public Prosecutors' Office notifies the Court of Peace about the decision within 24 hours. The Court of Peace has 24 hours

to decide whether to approve the action. There is no time limit on freezes. There is no provision in Turkish law for the sharing of seized assets with other countries.

MASAK's General Communiqué No. 3, requires that a special type of STR be filed by financial institutions in cases of suspected terrorist financing. However, until the amendments to the criminal code were enacted in June 2006, terrorist financing was not explicitly defined as a criminal offense under Turkish law. Various existing laws with provisions that can be used to punish the financing of terrorism include articles 220, 314 and 315 of the Turkish penal code, which prohibit assistance in any form to a criminal organization or to any organization that acts to influence public services, media, proceedings of bids, concessions, and licenses, or to gain votes, by using or threatening violence. To commit crimes by implicitly or explicitly intimidating people is illegal under the provisions of the Law No. 4422 on the Prevention of Benefit-Oriented Criminal Organizations. The GOT distributes to GOT agencies and financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee consolidated list, as well as U.S.-designated names.

Another area of vulnerability in the area of terrorist financing is the GOT's supervision of nonprofit organizations. The General Director of Foundations (GDF) issues licenses for charitable foundations and oversees them. The Ministry of Interior regulates charitable nongovernmental associations (NGOs). Both the GDF and the Ministry of Interior keep central registries of the charitable organizations they regulate and they require charities to verify and prove their funding sources and to have bylaws. Charitable foundations are audited by the GDF and are subject to being shut down if they act outside the bylaws. Charitable organizations are required to submit periodic financial reports to the regulators. The regulators and the police closely monitor monies received from outside Turkey. The police also monitor NGO's for links to terrorist groups.

Alternative remittance systems are illegal in Turkey, and in theory only banks and authorized money transfer companies are permitted to transfer funds. Trade-based money laundering, fraud, and underground value transfer systems are also used to avoid taxes and government scrutiny. There are 21 free trade zones operating in Turkey. The GOT closely controls access to the free trade zones. Turkey is not an offshore financial center.

According to MASAK statistics, no assets linked to terrorist organizations or terrorist activities were frozen in 2005. Turkey has a system for identifying, tracing, freezing, and seizing assets that are not related to terrorism, although the law allows only for their criminal forfeiture and not their administrative forfeiture. Article 7 of the anti-money laundering law provides for the confiscation of all property and assets (including derived income or returns) that are the proceeds of a money laundering predicate offense (soon to be expanded to crimes punishable by one year imprisonment), once the defendant is convicted. The law allows for the confiscation of the equivalent value of direct proceeds that could not be seized. Instrumentalities of money laundering can be confiscated under the law. In addition to the anti-money laundering law, Articles 54 and 55 of the Criminal Code provide for post-conviction seizure and confiscation of the proceeds of crimes. The defendant, however, must own the property subject to forfeiture. Legitimate businesses can be seized if used to launder drug money or support terrorist activity, or are related to other criminal proceeds. Property or its value that is confiscated is transferred to the Treasury.

The Council of Ministers promulgated a decree (2482/2001) to freeze all the funds and financial assets of individuals and organizations included on the UNSCR 1267 Sanctions Committee's consolidated list. However, the tools currently available under Turkish law for locating, freezing, seizing and confiscating terrorist assets are cumbersome, limited and not particularly effective. For example, there is no legal mechanism to freeze the assets of terrorists not on the UN consolidated list. Even for names on the list, Turkey's decree-based system of freezing 1267-listed names was challenged in court. In July 2006, a chamber of the Council of State (administrative court) ruled that the GOT lacked the

authority to freeze assets by decree since property rights are protected under the Turkish constitution. The assets of the 1267-listed individual continue to be frozen and this ruling is under appeal.

The GOT cooperates closely with the United States and with its neighbors in the Southeast Europe Cooperation Initiative (SECI). Turkey and the United States have a Mutual Legal Assistance Treaty (MLAT) and cooperate closely on narcotics and money laundering investigations. Turkey is a member of the Financial Action Task Force (FATF). MASAK is a member of the Egmont Group. Turkey is a party to the 1988 UN Drug Convention, the UN International Convention for Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Turkey has signed and ratified the COE Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime, which came into force on February 1, 2005. In 2006, Turkey became a party to the UN Convention against Corruption.

With the passage of several new pieces of legislation, the Government of Turkey took steps in 2005 and 2006 to strengthen its anti-money laundering and counterterrorist financing regime. It now faces the challenge of aggressively implementing these laws. Turkey should improve its coordination among the various entities charged with responsibility in its anti-money laundering and counterterrorist financing regime, including the various courts with responsibilities for these issues, in order to increase the number of successful investigations and prosecutions. Turkey should also regulate and investigate alternative remittance networks to thwart their potential misuse by terrorist organizations or their supporters. Turkey should consider expanding its narrow legal definition of terrorism. Turkey should continue tax reform that will help minimize the underground economy. It should also strengthen its oversight of charities.

## Turks and Caicos

The Turks and Caicos Islands (TCI) is a Caribbean overseas territory of the United Kingdom (UK). The TCI is comprised of two island groups and forms the southeastern end of the Bahamas archipelago. The U.S. dollar is the currency in use. The TCI has a significant offshore center, particularly with regard to insurance and international business companies (IBCs). Its location has made it a transshipment point for narcotics traffickers. The TCI is vulnerable to money laundering because of its large offshore financial services sector, as well as its bank and corporate secrecy laws and internet gaming activities. As of 2006, the TCI's offshore sector has eight banks, four of which also offer offshore banking; approximately 2,500 insurance companies; 20 trusts; and 17,000 "exempt companies" that are IBCs.

The Financial Services Commission (FSC) licenses and supervises banks, trusts, insurance companies, and company managers. It also licenses IBCs and acts as the Company Registry for the TCI. These institutions are subject to on-site examination to determine compliance with TCI laws and regulations. In 2006, the Financial Services Commission employed a staff of 21, including four regulators. The FSC became a statutory body under the Financial Services Commission Ordinance 2001 and became operational in March 2002. It now reports directly to the Governor, as well as the Minister of Finance. The FSC is in the process of adopting a risk-based examination approach to better assess, identify, measure, monitor and control threats associated with potential money laundering and terrorist financing.

The offshore sector offers "shelf company" IBCs, and all IBCs are permitted to issue bearer shares. However, the Companies (Amendment) Ordinance 2001 requires that bearer shares be immobilized by depositing them, along with information on the share owners, with a defined licensed custodian. This applies to all shares issued after enactment and allows for a phase-in period for existing bearer shares of two years. Trust legislation allows establishment of asset protection trusts inoculating assets from civil adjudication by foreign governments; however, the Superintendent of Trustees has investigative

powers and may assist overseas regulators. Currently, the FSC is rewriting the trust legislation with assistance from the UK Government.

The 1998 Proceeds of Crime Ordinance (PCO) criminalizes money laundering related to all crimes and provides "safe harbor" protection for good faith compliance with reporting requirements. The PCO allows for the criminal forfeiture of assets related to money laundering and other offenses, although civil forfeiture is not permitted. The PCO also establishes a Money Laundering Reporting Authority (MLRA), chaired by the Attorney General, to receive, analyze and disseminate financial disclosures such as suspicious activity reports (SARs). Its members also include the following individuals or their designees: Collector of Customs, the Managing Director of the FSC and the Head of its Financial Crimes Unit (FSU), the Superintendent of the FSC, the Commissioner of Police, and the Superintendent of the Criminal Investigation Department. The MLRA is authorized to disclose information it receives to domestic law enforcement and foreign governments.

The Proceeds of Crime (Money Laundering) Regulations came into force January 14, 2000. The Money Laundering Regulations place additional requirements on the financial sector such as identification of customers, retention of records for a minimum of ten years, training staff on money laundering prevention and detection, and development of internal procedures in order to ensure proper reporting of suspicious transactions. The Money Laundering Regulations apply to banks, insurance companies, trusts, mutual funds, money remitters, investment dealers and issuers of credit cards. However, money remitters and investment dealers have no supervisory or regulatory authority to oversee compliance with the regulations. Other sectors, such as gambling, jewelers, real estate companies and currency exchange companies, are not subject to the Money Laundering Regulations. Although the customer identification requirements only apply to accounts opened after the Regulations came into force, TCI officials have indicated that banks would be required to conduct due diligence on previously existing accounts by December 2005.

In 1999, the FSC, acting as the secretary for the MLRA, issued nonstatutory Guidance Notes to the financial sector, in order to help educate the industry regarding money laundering and the TCI's anti-money laundering requirements. Additionally, it provided practical guidance on recognizing suspicious transactions. The Guidance Notes instruct institutions to send SARs to either the Royal Turks & Caicos Police Force or the FSC. Officials forward all SARs to the Financial Crimes Unit (FCU) of the Royal Turks and Caicos Islands Police Force, which analyzes and investigates financial disclosures. The FCU also acts as the TCI's financial intelligence unit (FIU).

As with the other United Kingdom Caribbean overseas territories, the Turks and Caicos underwent an evaluation of its financial regulations in 2000, co-sponsored by the local and British governments. The report noted several deficiencies and the government has moved to address most of them. The report noted the need for improved supervision, which the government acknowledged. An Amendment to the Banking Ordinance was introduced in February 2002 to remedy deficiencies outlined in the report relating to notification of the changes of beneficial owners, and increased access of bank records to the FSC. However, legislation has not been introduced to remedy the deficiencies noted in the report with respect to the Superintendent's lack of access to the client files of Company Service and Trust providers, nor is there legislation that clarifies how the internet gaming sector is to be supervised with respect to anti-money laundering compliance.

As a UK territory, the TCI is subject to the United Kingdom Terrorism (United Nations Measure) (Overseas Territories) Order 2001. However, the Government of the TCI has not yet implemented domestic orders that would criminalize the financing of terrorism. The UK's ratification of the International Convention for the Suppression of the Financing of Terrorism has not been extended to the TCI.

The TCI cooperates with foreign governments—in particular, the United States and Canada—on law enforcement issues, including narcotics trafficking and money laundering. The FCU also shares

information with other law enforcement and regulatory authorities inside and outside of the TCI. The Overseas Regulatory Authority (Assistance) Ordinance 2001, allows the TCI to further assist foreign regulatory agencies. This assistance includes search and seizure powers and the power to compel the production of documents.

The TCI is a member of the Caribbean Financial Action Task Force, and is subject to the 1988 UN Drug Convention. The Mutual Legal Assistance Treaty between the United States and the United Kingdom concerning the Cayman Islands was extended to the TCI in November 1990.

The Government of the Turks and Caicos Islands has put in place a comprehensive system to combat money laundering with the relevant legislative framework. The FSC has made steady progress in developing its regulatory capability and has some experienced senior staff. Notwithstanding, the current regulatory structure is not fully in accordance with international standards. The Turks and Caicos Islands should extend existing regulations to all sectors, bring all obligated entities under the supervision of a regulatory body, and enhance its on-site supervision program. The Turks and Caicos Islands should take the necessary steps to ensure that its FIU is eligible for membership in the Egmont Group of financial intelligence units. The Government of the TCI should criminalize the financing of terrorists and terrorism. Turks and Caicos Islands should expand efforts to cooperate with foreign law enforcement and administrative authorities. Turks and Caicos Islands should also provide adequate resources and authorities to provide supervisory oversight of its offshore sector in order to further ensure criminal or terrorist organizations do not abuse the Turks and Caicos Islands' financial sector.

## Ukraine

Corruption, organized crime, prostitution, smuggling, tax evasion, trafficking in persons, drugs and arms, and other organized criminal activity continue to be sources of laundered funds in Ukraine. As of June 30, 2006, Ukraine has approximately 160 active banks, two of which are state-owned. There are no offshore financial centers or facilities under Ukraine's jurisdiction.

In January 2001, the Government of Ukraine (GOU) enacted the "Act on Banks and Banking Activities," which imposes some anti-money laundering (AML) requirements upon banking institutions. The Act prohibits banks from opening accounts for anonymous persons, requires the reporting of large transactions and suspicious transactions to state authorities, and provides for the lifting of bank secrecy pursuant to an order of a court, prosecutor, or specific state body. In August 2001, the President signed the "Law on Financial Services and State Regulation of the Market of Financial Services." This law establishes regulatory control over nonbank financial institutions that manage insurance, pension accounts, financial loans, or "any other financial services involving savings and money from individuals." The law defines financial "institutions" and "services," imposes record keeping requirements on obligated entities, and identifies the responsibilities of regulatory agencies. The law established the State Commission on Regulation of Financial Services Markets, which, along with the National Bank of Ukraine (NBU) and the State Commission on Securities and the Stock Exchange, has responsibility for regulating financial services markets.

When the Financial Action Task Force (FATF), placed Ukraine on the list of noncooperative countries and territories (NCCT) in September 2001, it noted that Ukraine lacked (1) a complete set of anti-money laundering (AML) laws, (2) an efficient mandatory system for reporting suspicious transactions to a Financial Intelligence Unit (FIU), (3) adequate customer identification requirements, and (4) adequate resources at present to combat money laundering. Following the FATF action, the U.S. Treasury Department issued an advisory to all U.S. financial institutions instructing them to "give enhanced scrutiny" to all transactions involving Ukraine.

On November 28, 2002, President Kuchma signed into law Ukrainian Law No. 249-IV, an anti-money laundering package entitled "On Prevention and Counteraction of the Legalization (Laundering) of the

Proceeds from Crime" (the Basic AML Law). The Basic AML Law establishes a two-tiered system of financial monitoring consisting of initial financial monitoring (i.e. obligated entities that carry out financial transactions) and state financial monitoring (i.e. government agencies charged with regulation and supervision of the financial institutions). Overall regulatory authority is vested in the State Committee for Financial Monitoring (SCFM), in accordance with Article 4 of the AML law.

In December 2002, the FATF determined that Ukraine's AML statute did not meet international standards and recommended that FATF members impose countermeasures on Ukraine. Under Section 311 of the USA PATRIOT Act, the United States designated Ukraine as a jurisdiction of primary money laundering concern. In December 2002 and February 2003, in response to the imminent threat of countermeasures, Ukraine passed further legislative amendments in accordance with FATF recommendations.

Legislation enacted in February 2003 requires banks and other financial service providers to implement AML compliance programs, conduct due diligence to identify beneficial account owners prior to allowing the opening an account or conducting certain transactions, report suspicious transactions to the SCFM and maintain records on suspicious transactions and the people carrying them out for a period of five years. The legislation includes a "safe harbor" provision that protects reporting institutions from liability for cooperating with law enforcement agencies. Immediately upon passage of the February amendments, the FATF withdrew its call for members to invoke countermeasures and the United States followed suit on April 17, 2003, by revoking Ukraine's designation under Section 311 of the USA PATRIOT Act as a jurisdiction of primary money laundering concern. In August 2003, the State Commission established the State Register of financial institutions, and by October 2006, the State Register contained information on 1375 nonbank financial institutions.

By passing comprehensive anti-money laundering legislation, Ukraine initiated the process of NCCT de-listing. At the FATF plenary in September 2003, Ukraine was invited to submit an implementation plan, and an on-site visit to assess Ukraine's progress in developing its AML regime was conducted on January 19-23, 2004. The positive results of the on-site visit by the FATF evaluation team were reported to the European Review Group (ERG), and Ukraine was removed from the NCCT list at the FATF plenary on February 25, 2004. As a condition of de-listing, Ukraine continued to undergo monitoring by the FATF on implementation of its AML regime. Since November 2004, the GOU has made several efforts to pass a set of amendments to the AML law in order to bring Ukraine's regime into compliance with FATF's revised Forty plus Nine recommendations. The Rada, or Parliament, twice rejected the government's draft in 2005. The government has redrafted the law, narrowing its scope to the FATF recommendations, and omitting provisions introducing new SCFM authority and other bureaucratic changes that had drawn opposition in the Parliament. Among other provisions, the new legislation would expand the sectors subject to primary monitoring to include retail traders, lawyers, accountants, and traders of precious metals. The law, entitled "On Amending Some Legislative Acts of Ukraine on Prevention to Legalization (Laundering) of the Proceeds from Crime and Terrorist Financing", was registered in the Verkhovna Rada on December 28, 2006. The bill was also referred to a special expert committee called the Main Scientific Expertise Department, which provided commentary, along with the recommendation that the Rada address some problems mainly regarding terminology, and then approve the bill on its first reading.

In 2004, authorities reduced the monetary threshold beyond which transactions and operations are subject to compulsory financial monitoring from Ukrainian Hryvnias (UAH) 300,000 (approximately $59,650) for cashless payments and UAH 100,000 (approximately $19,900) for cash payments, to UAH 80,000 (approximately $15,900) for payments using either method. The compulsory reporting threshold exists only if the transaction also meets one or more suspicious activity indicators as set forth in the law. Any transaction suspected of being connected to terrorist activity must be reported to the appropriate authorities immediately.

Beginning in August 2005, as a result of amendments to the "Resolution on the Adoption of Instructions Regarding Movement of Currency, Precious Metals, Payment Documents, and Other Banking Documents over the Customs Border of Ukraine," the law mandates that travelers declare cross-border transportation of cash sums exceeding $3,000. Cash smuggling is substantial in Ukraine, although it is reportedly related more to unauthorized capital flight rather than to criminal proceeds or terrorist funding.

In 2005, the GOU sought to combat smuggling and corruption by reducing import duties, introducing new procedures for the Customs Service, and implementing transparent procedures for the privatization of state enterprises. Ukraine's 2005 budget eliminated the tax and customs duty privileges available in eleven Free Economic Zones and nine Priority Development Territories that operated within Ukraine. However, in August 2006, the government announced its intention to restore tax and customs privileges for businesses operating in the SEZs beginning in 2007. Although legislation implementing this policy decision had not yet passed the Parliament by the end of 2006, the GOU asserts that the SEZs will avoid the problems of the past.

Ukraine enacted Law 3163-IV in January 2006; this law amended the initial AML laws. Under the new Law, the entities obligated to conduct initial financial monitoring must be able to provide proof that they are fulfilling all Know Your Customer (KYC) identification requirements. Ukraine also granted state agencies enhanced authority to exchange information internationally, improved rules on bank organization, and implemented a screening requirement at the level of financial institutions. On September 14, 2006, Ukraine enacted amendments to the "Law on Banks and Banking" that require all banks to be formed as open joint-stock companies or as cooperatives. This measure strengthens disclosure requirements on the identity of the beneficial owners of banks. These amendments apply to all newly formed banks and provide a three-year period for existing banks to comply. As a result of these and other improvements to its legal framework, in February 2006, the FATF suspended its direct monitoring of Ukraine, which had been in place since December 2002.

The Criminal Code of Ukraine has separate provisions criminalizing drug-related and nondrug-related money laundering. Amendments to the Code adopted in January 2003 included willful blindness provisions and expanded the scope of predicate crimes for money laundering to include any action punishable under the Criminal Code with imprisonment of three years or more, excluding certain specified actions.

The SCFM is Ukraine's financial intelligence unit (FIU). The December 10, 2001 Presidential Decree "Concerning the Establishment of a Financial Monitoring Department" mandated the establishment of the SCFM as Ukraine's FIU. The SCFM became operational on June 12, 2003. At that time, the SCFM was an independent authority administratively subordinate to the Ministry of Finance and the sole agency authorized to receive and analyze financial information from financial institutions. On March 18, 2004, Ukraine's Rada granted the SCFM the status of a central executive agency, subordinate to the Cabinet of Ministers rather than to the Ministry of Finance. This change became effective on January 1, 2005. As of October 1, 2006, the SCFM had established 21 local branches in Ukraine's regions.

The SCFM is an administrative agency with no investigative or arrest authority. It is authorized to collect suspicious transaction reports and analyze suspicious transactions, including those related to terrorist financing, and to transfer financial intelligence information to competent law enforcement authorities for investigation. The SCFM also has the authority to conclude interagency agreements and exchange intelligence on financial transactions involving money laundering or terrorist financing with other FIUs. As of October 2006, the SCFM had concluded memoranda of understanding (MOUs) with the FIUs of thirty countries, and was working on fourteen additional MOUs.

The SCFM has processed, analyzed, and developed cases reportedly to the point of establishing the equivalent of probable cause prior to referral to law enforcement. It has become a regional leader with

regard to the volume of case information exchanged with counterpart FIUs. The SCFM acknowledges the existence and use of alternative remittance systems in Ukraine, and its personnel have attended seminars and exchanged information about such systems. The SCFM and security agencies monitor charitable organizations and other nonprofit entities that might be used to finance terrorism.

In 2005, the SCFM received 786,251 transaction reports, which include STRs and automatic threshold reports. The majority of these were submitted by banks. The SCFM designated approximately 11 percent of these for "active research" and sent 321 separate cases to law enforcement agencies. From January to November 2006, the SCFM received a total of 692,280 transaction reports. Over that same period, the SCFM referred 31 cases to the Prosecutor General's Office, 115 cases to the State Tax Administration, 127 cases to the Ministry for Internal Affairs, and 154 cases to the State Security Service of Ukraine. As a result of subsequent investigation of these 427 cases, law enforcement agencies initiated 161 criminal cases. Of these, prosecutors brought 8 cases to trial, with one conviction.

Although the reporting system is effective and the SCFM has generated a substantial number of cases, law enforcement authorities and prosecutors did not succeed in obtaining a large number of convictions. Observers reportedly believe the key problem to be local prosecutors who close money laundering investigations and cases prematurely or arbitrarily, possibly because of corruption and possibly because of a weak understanding of money laundering crimes on the part of authorities—for example, authorities are inclined to include tax crimes as money laundering. Ukraine has been working with the European Commission and Council of Europe to increase its capacity to fight money laundering and terrorism financing. The first such undertaking took place from 2003-2005 and was called "Project Against Money Laundering in Ukraine," or MOLA-UA. Those involved decided it was so successful that in September 2006, a follow-up "Project Against Money Laundering and Terrorist Financing in Ukraine" (MOLA-UA2) was established, with a focus on education, training and cooperation. MOLA-UA2 will run through April 2009 and focus on three areas: getting Ukraine's legislative framework up to international standards; enhancing the human capacities of key institutions and agencies; and developing the organizational and technical infrastructure of the system.

Ukraine has an asset forfeiture regime. Article 59 of the Ukrainian Criminal Code provides for the forceful seizure of all or a part of the property of a person convicted for grave and especially grave offenses as set forth in the relevant part of the code. With respect to money laundering, Article 209 allows for the forfeiture of criminally obtained money and other property.

On December 10, 2003, the Cabinet of Ministers issued Decree No. 1896, establishing a Unified State Information System of Prevention and Counteraction of Money Laundering and Terrorism Financing. Through this system, fourteen ministries and agencies share information by providing each other with monthly database updates. The Government is planning to automate this information sharing in 2007 by establishing a secure electronic network linking these agencies.

Law 3163-IV, which entered into force on January 1, 2006, enhanced Ukraine's ability to exchange information internationally and placed greater obligations on banks to combat terrorist financing. This Law requires banks to adopt procedures to screen parties to all transactions using a SCFM-issued list of beneficiaries of, or parties to, terrorist financing. Banks must freeze assets for two days and immediately inform the FIU and law enforcement bodies whenever a party to a transaction appears on the list. The FIU can extend the freeze to five days. During the first half of the year, banks developed their screening capabilities. On October 25, 2006, the Cabinet of Ministers approved the SCFM's list, drawn from three sources: the United Nations 1267 Sanctions Committee's consolidated list, information from the Ukrainian Security Service on individuals and entities suspected of violating article 258 of the Ukrainian Criminal Code concerning terrorism, and the lists compiled by those countries that have bilateral agreements with Ukraine on mutual recognition of terrorist designations. On September 21, 2006, the Rada enacted revisions to Article 258 of the Criminal Code, adding

Article 258-4 which explicitly criminalizes terrorist financing. The revised text mandates imprisonment from three to eight years for financing, material provision, or provision of arms with the aim of supporting terrorism. The revisions also amend the criminal procedure code to empower the State Security Service (SBU) with primary responsibility for investigation of terrorist financing.

The GOU has cooperated with U.S. efforts to track and freeze the financial assets of terrorists and terrorist organizations. The NBU, the State Commission for the Regulation of Financial Services, the Securities Exchange Commission, the State Tax Administration, the SBU, and the Ministries of Finance, Internal Affairs, and Foreign Affairs are informed about the U.S.-designation of suspected terrorists and terrorist organizations under E.O. 13224 and other U.S. authorities. Through their regulatory agencies, banks and nonbank financial services also receive these U.S.-designations, and are instructed to report any transactions involving designated individuals or entities.

The U.S.-Ukraine Treaty on Mutual Legal Assistance in Criminal Matters was signed in 1998 and entered into force in February 2001. A bilateral Convention for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with Respect to Taxes on Income and Capital, which provides for the exchange of information in administrative, civil, and criminal matters, is also in force.

Ukraine is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Ukraine is a signatory to the UN Convention against Corruption. Ukraine is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), a FATF-style regional body (FSRB). It is also an observer and technical assistance donor to the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG), another FSRB. The SCFM is a member of the Egmont Group.

Ukraine has strengthened and clarified its newly adopted laws. With the SCFM, the NBU, and other actors in the financial and legal sectors, Ukraine has established a comprehensive AML regime. To date, however, Ukraine's ability to implement this regime through consistent successful criminal prosecutions has yet to be proven. The Prosecutor General's office should address the deficiencies of that office, such as limited professional experience with money laundering among staff, which can result in prosecutors' limited commitment to criminal prosecution. The GOU should take action to establish oversight capabilities of local investigators, prosecutors, and judges to insure that cases are vigorously pursued and prosecuted. Law enforcement agencies should give higher priority to investigating money laundering cases. Both law enforcement officers and the judiciary need a better understanding of the theoretical and practical aspects of investigating and prosecuting money laundering cases. Ukraine should become a party to the UN Convention against Corruption and prosecute and convict corrupt public officials.

## United Arab Emirates

The United Arab Emirates (UAE) is an important financial center in the Persian Gulf region. Although the financial sector is modern and progressive, the UAE remains a largely cash-based society. Dubai, in particular is a major international banking center. The country also has a growing offshore sector. The UAE's robust economic development, political stability, and liberal business environment have attracted a massive influx of people, goods, and capital. The UAE is particularly susceptible to money laundering due to its geographic location as the primary transportation and trading hub for the Gulf States, East Africa, and South Asia; and its expanding trade ties with the countries of the former Soviet Union and lack of transparency in its corporate environment. The potential for money laundering is exacerbated by the large number of resident expatriates (roughly 80 percent of total population) from the aforementioned regions to the UAE who send remittances to their homelands. Given the country's proximity to Afghanistan, where most of the world's opium is produced, narcotics traffickers are increasingly reported to be attracted to the UAE's financial and trade centers. Other

sources of money laundering in the UAE include hawala, trade fraud, the real estate boom, the misuse of the international gold trade, conflict diamonds and smuggling.

Following the September 11, 2001 terrorist attacks in the United States, and amid revelations that terrorists had moved funds through the UAE, the Emirates' authorities acted swiftly to address potential vulnerabilities. In close concert with the United States, the UAE imposed a freeze on the funds of groups with terrorist links, including the Al-Barakat organization, which was headquartered in Dubai. Both national and emirate-level officials have gone on record as recognizing the threat money laundering activities in the UAE pose to the nation's reputation and security. Since 2001, the UAE Government (UAEG) has taken steps to better monitor cash flows through the UAE financial system and to cooperate with international efforts to combat terrorist financing. The UAE has enacted the Anti-Money Laundering Law No. 4/2002, and the Anti-Terrorism Law No. 1/2004. Both pieces of legislation, in addition to the Cyber Crimes Law No. 2/2006, serve as the foundation for the country's anti-money laundering and counterterrorist financing efforts.

Law No. 4 of 2002 criminalizes all forms of money laundering activities. The law calls for stringent reporting requirements for wire transfers exceeding 2000 dirhams (approximately $545) and currency imports above 40,000 dirhams (approximately $10,900).The law imposes stiff criminal penalties for money laundering that includes up to seven years in prison plus a fine of up to 300,000 dirhams (approximately $81,700), as well as a seizure of assets upon conviction. The law also provides safe harbor provisions for reporting officers.

Prior to the passage of the Anti-Money Laundering Law, the National Anti-Money Laundering Committee (NAMLC) was established in July 2000 to coordinate the UAE's anti-money laundering policy. The NAMLC was later codified as a legal entity by Law No. 4/2002, and is chaired by the Governor of the Central Bank. Members of the NAMLC include representatives from the Ministries of Interior, Justice, Finance, and Economy, the National Customs Board, Secretary General of the Municipalities, Federation of the Chambers of Commerce, and five major banks and money exchange houses (as observers).

Administrative Regulation No. 24/2000 provides guidelines to financial institutions for monitoring money laundering activity. This regulation requires banks, money exchange houses, finance companies, and any other financial institutions operating in the UAE to follow strict know your customer guidelines. Financial institutions must verify the customer's identity and maintain transaction details (i.e., name and address of originator and beneficiary) for all exchange house transactions over $545 and for all non-account holder bank transactions over $10,900. The regulation delineates the procedures to be followed for the identification of natural and juridical persons, the types of documents to be presented, and rules on what customer records must be maintained on file at the institution. Other provisions of Regulation 24/2000 call for customer records to be maintained for a minimum of five years and further require that they be periodically updated as long as the account is open.

In July, 2004, the UAE government strengthened its legal authority to combat terrorism and terrorist financing by passing Federal Law Number No. 1/2004. The Law specifically criminalizes the funding of terrorist activities and terrorist organizations. It sets stiff penalties for the crimes covered, including life imprisonment and the death penalty. It also provides for asset seizure or forfeiture. Under the law, founders of terrorist organizations face up to life imprisonment. The law also penalizes the illegal manufacture, import, or transport of "nonconventional weapons" and their components that are intended for use in a terrorist activity.

Article 12 provides that raising or transferring money with the "aim or with the knowledge" that some or all of this money will be used to fund terrorist acts is punishable by "life or temporary imprisonment," regardless if these acts occur. Law No. 1/2004 grants the Attorney General (or his deputies) the authority to order the review of information related to the accounts, assets, deposits,

transfer, or property movements on which the Attorney General has "sufficient evidence to believe" are related to the funding or committing of a terror activity stated in the law.

The law also provides for asset seizure and confiscation. Article 31 gives the Attorney General the authority to seize or freeze assets until the investigation is completed. Article 32 confirms the Central Bank's authority to freeze accounts for up to seven days if it suspects that the funds will be used to fund or commit any of the crimes listed in the law. The law also allows the right of appeal to "the competent court" of any asset freeze under the law. The court will rule on the complaint within 14 days of receiving the complaint. Through 2005, there were no reported criminal convictions for money laundering or terrorist financing under either the 2002 or the 2004 laws.

Law No. 1/2004 also established the "National Anti-Terror Committee" (NATC) to serve as the government's interagency liaison with respect to implementing the United Nations Security Council Resolutions on terrorism, and sharing information with its foreign counterparts as well as with the United Nations. Representatives from Ministries of Foreign Affairs, Interior, Justice, and Defense; Central Bank; State Security Department; and Federal Customs Authority comprise the NATC

The Anti-Money Laundering and Suspicious Case Unit (AMLSCU) was established in 2002 as the UAE's financial intelligence unit (FIU), and was housed within the Central Bank. In addition to receiving Suspicious Transaction Reports, the AMLSCU is authorized to send and receive information requests from foreign regulatory authorities in order to conduct its preliminary investigations based on suspicious transaction report data. The AMLSCU joined the Egmont Group in June 2002, and has regularly exchanged information with foreign FIUs on a reciprocal basis. It has also provided information by request to foreign FIUs (including the United States) regarding investigations being conducted in other countries. As of October 2006, the AMLSCU has received and investigated a total of 3954 suspicious transactions reports (STRs), 829 of which were received between December 2005 and October 2006. Based on AMLSCU and law enforcement investigations from these STRs, a total of 27 freeze orders were issued by the Central Bank between December 2000 (prior to the establishment of the FIU) and October 2006, one of which was issued in 2006. Of these 27 cases of freeze orders, 9 cases are currently in the process of prosecution for money laundering and confiscation of criminal proceeds. The Central Bank also ensures that it circulates an updated UNSCR 1267 Sanctions Committee's consolidated list of suspected terrorists and terrorist organizations to all the financial institutions under its supervision. Since 2000, the Central Bank has frozen a total of $1,348,381 from 17 separate bank accounts based on the names contained in the UNSCR 1267 list.

Several amendments were made to the Central Bank Regulations 24/2000 in July 2006. First, the regulations added the term "terrorism financing" to any references made to the term "money laundering." Second, the Regulations required financial institutions to freeze transactions that they believe may be destined for funding terrorism, terrorist organizations, or for terrorist purposes. The Regulations also require financial institutions to notify the financial intelligence unit (FIU) in writing of such transactions "in case of any doubt". Finally, the enhanced due diligence requirements for charities were made requiring banks to obtain a certificate from the Minister of Social Affairs before opening or maintaining any charitable organization-type account.

In 2006, the UAE enacted Law No. 2/2006 of the Cyber Crimes. Article 19 of the law criminalized the electronic transfer of money or property through the internet in which the true sources of such assets are either concealed or linked to criminal proceeds. Violations are punishable by up to seven years imprisonment and fines ranging from approximately $8,170 to $54,500. Article 21 of the law outlaws the use of the internet to finance terrorist activities, promote terrorist ideology, disseminate information on explosives, or to facilitate contact with terrorist leaders. Any violation of Article 21 is punishable by up to 5 years imprisonment.

The Central Bank is responsible for supervising the UAE financial sectors, which include banks, exchange houses, and investment companies. It is authorized to issue licenses and impose

administrative sanctions for compliance violations. The Central Bank also has the authority to issue instructions and recommendations to financial institutions as it deems appropriate, and to take any measures as necessary to ensure the integrity of the UAE's financial system

Some money laundering in the UAE is known to occur through the numerous money exchange houses. However, hawala is where money laundering activity is likely more prevalent due to the largely undocumented nature of this informal remittance system. Dubai is a regional hawala center. Hawala is an attractive mechanism for terrorist and criminal exploitation due to the nontransparent and highly resilient nature of the system to law enforcement and regulators. In 2002, the Central Bank issued new regulations to help improve the oversight of hawala. The new regulations required hawala brokers (hawaladars) to register with the Central Bank, submit the names and addresses of all originators and beneficiaries of funds, and to file suspicious transaction reports on a monthly or quarterly basis. However, since the inception of the program, there reportedly have not been any suspicious reports filed by hawaladars.

As of November 30, 2006, the Central Bank issued 201 licenses to hawaladars, with an additional 38 applicants currently working to complete their licensing requirements. Once issued a formal license, the Central Bank conducts one-on-one training sessions with each registered hawaladar to ensure that dealers understand the record-keeping and reporting obligations. The registered hawaladars are also required to use an account they open at the Central Bank to process their transactions. Currently, there is no accurate estimate of the total number of UAE-based hawala brokers, and there is no penalty for failure of hawaladars to register with the Central Bank. The UAE has hosted three international Conferences on hawala, and plans to host a fourth in March 2007.

The UAE has not set any limits on the amount of cash that can be imported into or exported from the country. No reporting requirements exist for cash exports. However, the Central Bank requires that any cash imports over $10,900 must be declared to Customs; otherwise undeclared cash may be seized upon attempted entry into the country. Upon seizing any undeclared cash, UAE authorities have the jurisdiction to conduct an investigation into the source of these funds. All cash forfeiture cases are handled at the judicial level because there are no administrative procedures to handle forfeited cash. Since the UAE is a cash-based economy, it is not unusual for people to carry significant sums of cash in general. As a result, customs officials, police, and judicial authorities tend to not regard large cash imports as potentially suspicious or criminal type activities.

The UAE authorities have admitted the need to better regulate "near-cash" items such as gold, jewelry, and gemstones, especially in the burgeoning markets located in Dubai. The UAE has participated in the Kimberley Process Certification Scheme for Rough Diamonds (KPCS) since November 2002, and began certifying rough diamonds exported from the UAE on January 1, 2003. In 2004, the UAE was the first KPCS participant country to volunteer for a "peer review visit" on internal control mechanisms. The Dubai Metals and Commodities Center (DMCC) is a quasi-governmental organization charged with issuing Kimberly Process (KP) certificates in the UAE, and employs four full-time individuals to administer the KP program. Prior to January 1, 2003, the DMCC circulated a sample UAE certificate to all KP member states and embarked on a public relations campaign to educate the estimated 50 diamond traders operating in Dubai with the new KP requirements. Under the new KP regulations, UAE customs officials are authorized to delay or even confiscate those diamonds entering the UAE from another KP member country that does not have the proper certificates.

In 2006, Russian customs officials reportedly apprehended an air passenger from Dubai after he tried to smuggle 2.5 kilos of diamonds into the country. There are also reports that diamonds are increasingly being used as medium to provide countervaluation in hawala transfers, particularly between Dubai and Mumbai. Also in December 2006 a UN report noted that UAE authorities released a suspicious shipment of diamonds after a scientific examination proved that the origin of the

diamonds had been falsified. The UN group felt there were reasonable grounds to pursue a judicial investigation rather than releasing the diamonds to the importer.

The Securities and Commodities Authority (SCA) supervises the country's two stock markets. In February 2004, the SCA issued anti-money laundering guidelines to all brokers that included identity verification instructions for new customer accounts, a reporting requirement for cash transactions above $10,900, and a minimum five-year record keeping requirement for all customer account information. The SCA also instructed brokers to file suspicious transaction reports with the SCA for initial analysis before they are forwarded to the AMLSCU for further action.

Dubai's real estate market continued to show significant growth during 2006, making this sector another area that is susceptible to money laundering abuse. In 2002, Dubai began to allow three real estate companies to sell "freehold" properties to noncitizens. Since then, several other emirates have followed suit. For instance, Abu Dhabi has passed a property law, which provides for a type of leasehold ownership for noncitizens. In addition, citizens of GCC countries have the right to purchase and trade land within designated investment areas, while other expatriates are permitted to invest in real estate properties for a 99-year leasehold basis. Due to the intense interest in and reported cash purchases of such properties, the potential for money laundering has become of increased concern to the UAE Government. As a result, developers have stopped accepting cash purchases for these properties.

Since the September 11, 2001 terrorist attacks, the UAE Government has been more sensitive to regulating charitable organizations and accounting for funds transfers abroad. In 2002, the UAEG mandated that all licensed charities interested in transferring funds overseas must do so via one of three umbrella organizations: the Red Crescent Authority, the Zayed Charitable Foundation, or the Muhammad Bin Rashid Charitable Trust. These three quasi-governmental bodies are in a position to ensure that overseas financial transfers go to legitimate parties. As an additional step, the UAEG has contacted the governments in numerous aid receiving countries to compile a list of recognized acceptable recipients for UAE charitable assistance.

Charities in Abu Dhabi and the Northern Emirates are regulated by the UAE Ministry of Social Affairs, which is responsible for licensing and monitoring registered charities in these emirates. The Ministry also requires these charities to keep records of all donations and beneficiaries, and to submit financial reports annually. Charities in Dubai are licensed and monitored by the Dubai Department of Islamic Affairs and Charitable Activities. Some charities however, particularly those located in the Northern Emirates, are only registered with their local emirate authority and not the federal Ministry. In July 2006, Regulation 24/2000 was amended, requiring charities from all emirates to obtain a certificate from the Minister of Social Affairs before being permitted to open or maintain bank accounts in the UAE. This amendment effectively required that all charities must be registered federally and no longer at just the emirate level. In November 2006, the UAE hosted a United Kingdom/Gulf Cooperation Council conference on charities, and made a proposal to hold biannual meetings going forward with the UK and GCC on charities oversight.

The UAE has both free trade zones (FTZs) and financial free zones (FFZs). The number of free trade zones (FTZs) is growing, with 26 operating in Dubai and six more in the other emirates. Every emirate except Abu Dhabi has at least one functioning FTZ. The free trade zones are monitored by the local emirate rather than federal authorities.

There are over 5,000 multinational companies located in the FTZs, and thousands more individual trading companies. The FTZs permit 100 percent foreign ownership, no import duties, full repatriation of capital and profits, no taxation, and easily obtainable licenses. Companies located in the free trade zones are considered offshore or foreign entities for legal purposes. However, UAE law prohibits the establishments of shell companies and trusts, and does not permit nonresidents to open bank accounts in the UAE. The larger FTZs in Dubai (such as Jebel Ali free zone) are well-regulated. Although some

trade-based money laundering undoubtedly occurs in the large FTZs, a higher potential for financial crime and exists in some of the smaller FTZs located in the northern emirates.

In March 2004, the UAEG passed Federal Law No. 8, regarding the Financial Free Zones (FFZs) (Law No. 8/2004). Although the new law exempts FFZs and their activities from UAE federal, civil, and commercial laws, FFZs and their operations are still subject to federal criminal laws including the Anti-Money Laundering Law (Law No. 4/2002) and the Anti-Terror Law (Law No. 1/2004). As a result of Law 8/2004 and a subsequent federal decree, the UAE's first financial free zone (FFZ), known as the Dubai International Financial Center (DIFC), was established in September 2004. By September 2005, the DIFC had opened its securities market or the Dubai International Financial Exchange (DIFX).

Law No. 8/2004 limits the issuance of licenses for banking activities in the FFZs to branches of companies, joint companies, and wholly owned subsidiaries provided that they "enjoy a strong financial position and systems and controls, and are managed by persons with expertise and knowledge of such activity." The law prohibits companies licensed in the FFZ from dealing in UAE currency (i.e., dirham), or taking "deposits from the state's markets." Further, the law stipulates that the licensing standards of companies "shall not be less than those applicable in the state." The law empowers the Emirates Stocks and Commodities Authority to approve the listing of any company listed on any UAE stock market in the financial free zone, as well as the licensing of any UAE stock broker. Insurance activities conducted in the FFZ are limited by law to reinsurance contracts only. The law further gives competent authorities in the Federal Government the power to inspect financial free zones and submit their findings to the UAE cabinet.

DIFC regulations provide for an independent regulatory body, namely the Dubai Financial Services Authority (DFSA), to report its findings directly to the office of the Dubai Crown Prince and an independent Commercial Court. According to DFSA regulators, the DFSA due diligence process is a risk-based assessment that examines a firm's competence, financial soundness, and integrity. Prior to the inauguration of the DIFC in 2004, several observers called into question the independence of the DFSA as a result of the high profile firings of the chief regulator and the head of the regulatory council (i.e., the supervisory authority). Subsequent to the firings, Dubai passed laws that gave the DFSA more regulatory independence from the DIFC, although these laws have not yet been tested. The DFSA, who modeled its regulatory regime after the United Kingdom, is the sole authority responsible for issuing licenses to those firms providing financial services in the DIFC.

The DFSA has licensed 94 financial institutions to operate within the DIFC. The DFSA prohibits offshore casinos or internet gaming sites in the UAE, and requires firms to send suspicious transaction reports to the AMLSCU (along with a copy to the DFSA). To date, there have been 9 suspicious transaction reports issued from firms operating in the DIFC (8 in 2006). Although firms operating in the DIFC are subject to Law No. 4/2002, the DFSA has issued its own anti-money laundering regulations and supervisory regime, which has caused some ambiguity about the Central Bank's and the AMLSCU's respective authorities within the DIFC. Ongoing discussions continue between the DFSA and the UAE Central Bank to create a formal bilateral arrangement. The DFSA has undertaken a campaign to reach out to other international regulatory authorities to facilitate information sharing. As of December 2006, the DFSA has MOUs with 16 other regulatory bodies, including the UK's Financial Services Authority (FSA), the Emirates Securities and Commodities Authority, and the U.S. Commodity Futures Trading Commission (CFTC).

The UAE is a party to the 1988 UN Drug Convention and to all twelve UN conventions and protocols relating to the prevention and suppression of international terrorism. It has signed and ratified the UN Convention against Corruption. The UAE has signed, but has not yet ratified the UN Convention against Transnational Organized Crime. The UAE supported the creation of the Middle East and North

Africa Financial Action Task Force (MENAFATF), and, in November 2004, was one of its original charter signatories.

The Government of the UAE has demonstrated progress in constructing a far-reaching anti-money laundering and counterterrorist finance program. Information sharing between the AMLSCU and foreign FIUs has substantially improved. However, several areas requiring further action by the UAEG remain. The most troublesome is the lack of prosecutions and convictions. Law enforcement and customs officials also need to proactively recognize money laundering activity and develop cases based on investigations, rather than wait for case referrals from the AMLSCU that are based on SARs. Additionally, law enforcement and customs officials should conduct more thorough inquiries into large and undeclared cash imports into the country, as well as require—and enforce—outbound declarations of cash and gold. All forms of trade-based money laundering must be given greater scrutiny by UAE customs and law enforcement officials, including customs fraud, the trade in gold and other commodities related to hawala transactions, and the misuse of trade to launder narcotics proceeds. The UAE should increase the resources it devotes to investigation of AML/CFT both at the federal level at the AMLSCU and at the emirate level law enforcement. The UAE's initiatives in the registration of hawaladars should be coupled with investigations. The cooperation between the Central Bank and the DFSA needs improvement, and lines of authority need to be clarified. The UAE should conduct more follow-up with financial institutions and the MSA regarding the recent tightening of regulations on charities to ensure their registration at the federal level. The UAE should also continue its regional efforts to promote sound charitable oversight, and engage in a public campaign to ensure all local charities are aware of registration requirements. The UAE should ratify the UN Convention against Transnational Organized Crime.

## United Kingdom

The United Kingdom (UK) plays a leading role in European and world finance and remains attractive to money launderers because of the size, sophistication, and reputation of its financial markets. Although narcotics are still a major source of illegal proceeds for money laundering, the proceeds of other offenses, such as financial fraud and the smuggling of people and goods, have become increasingly important. The past few years have witnessed the movement of cash placement away from High Street banks and mainstream financial institutions. The use of bureaux de change, cash smugglers (into and out of the UK), and gatekeepers (including solicitors and accountants), the purchase of high-value assets as disguises for illegally obtained money, and credit/debit card fraud has been on the increase since 2002.

The UK has implemented many of the provisions of the European Union's (EU) two Directives on the prevention of the use of the financial system for the purpose of money laundering, and the Financial Action Task Force (FATF) Forty Plus Nine Recommendations. Narcotics-related money laundering has been a criminal offense in the UK since 1986. The laundering of proceeds from other serious crimes has been criminalized by subsequent legislation. Banks and nonbank financial institutions in the UK must report suspicious transactions.

In 2001, money laundering regulations were extended to money service bureaus (e.g., bureaux de change, money transmission companies), and in September 2006, the Government published a review into the regulation and performance of money service businesses in preventing money laundering and terrorist financing. Since 2004, more business sectors are subject to formal suspicious activity reporting (SAR) requirements, including attorneys, solicitors, accountants, real estate agents, and dealers in high-value goods such as cars and jewelry. Sectors of the betting and gaming industry that are not currently regulated are being encouraged to establish their own codes of practice, including a requirement to disclose suspicious transactions.

The Proceeds of Crime Act 2002 (POCA), enacted in February 2003, creates a new criminal offense of failing to disclose suspicious transactions in respect to all crimes, not just "serious," narcotics- or terrorism-related crimes, as was the case previously. This is applicable to all regulated sectors. Along with the Act came an expansion of investigative powers relative to large movements of cash in the UK. Sections 327 to 340 of the Act address possession, acquisition, transfer, removal, use, conversion, concealment or disguise of criminal or terrorist property, inclusive of but not limited to money. The POCA also criminalizes tipping off. In 2003, the Financial Secretary to the treasury laid down the "Money Laundering Regulations 2003," along with amending orders for the POCA and the Terrorism Act. The Regulations impose requirements on various entities, including attorneys, and introduce a client identification requirement, requirements on record keeping, internal reporting procedures and training. These regulations came into force on March 1, 2004. In June 2006, a solicitor was sentenced to fifteen months' imprisonment when he was found to have "closed his eyes to the obvious" and been willfully blind to the money laundering offenses committed by his client.

The UK's banking sector provides accounts to residents and nonresidents, who can open accounts through private banking activities and various intermediaries that often advertise on the Internet and also offer various offshore services. Private banking constitutes a significant portion of the British banking industry. Both resident and nonresident accounts are subject to the same reporting and record keeping requirements. Individuals typically open nonresident accounts for tax advantages or for investment purposes.

Bank supervision falls under the Financial Services Authority (FSA). The FSA's primary responsibilities relate to the safety and soundness of the institutions under its jurisdiction. The FSA also plays an important role in the fight against money laundering through its continued involvement in the authorization of banks, and investigations of money laundering activities involving banks. The FSA regulates some 29,000 firms, which include European Economic Area (EEA) firms passporting into the UK (firms doing business on a cross-border basis), ranging from global investment banks to very small businesses, and around 165,000 individuals. From October of 2003, the FSA increased its regulatory role to include mortgage and general insurance agencies, totaling over 30,000 institutions. The FSA administers a civil-fines regime and has prosecutorial powers. The FSA has the power to make regulatory rules with respect to money laundering, and to enforce those rules with a range of disciplinary measures (including fines) if the institutions fail to comply. In October 2006, the financial services sector adopted National Occupational Standards of Competence in the fields of compliance and in anti-money laundering.

Effective July 1, 2005, the Serious Organized Crime and Police Act of 2005 (SOCAP) made changes to the money laundering provisions in the POCA. One of these changes was the creation of the Serious Organized Crime Agency (SOCA), which became the UK's financial intelligence unit (FIU). On April 1, 2006, SOCA took over all FIU functions from the National Criminal Intelligence Service (NCIS). In light of that change SARs are now filed with SOCA. In the context of the SARs regime, SOCAP gives SOCA all the FIU powers and functions that were inherited from NCIS. SOCA has three functions: the prevention and detection of serious organized crime; the mitigation of the consequences of such crime; and the function of receiving, storing, analyzing and disseminating information. Under the law, SOCA's functions are not restricted to serious or organized crime but potentially bear on all crimes, and those functions are to include assistance to others in the discharge of their enforcement responsibilities. In 2005, SOCA's precursor agency NCIS received just under 200,000 SARs and has seen a steady increase each year since 2001. The new law also affected reporting requirements: requirements were relaxed slightly to allow banks to proceed with low value transactions (not exceeding 250 pounds) involving suspected criminal property without requiring specific consent to operate the account. However, the reporting of every such transaction is still required, and other obligated entities were not granted these relaxed standards. Another change that the SOCAP made was that acts would no longer be considered to be money laundering if the act and the property gained took

place in a foreign jurisdiction where the conduct in question was not contrary to the law of the foreign jurisdiction.

The Third Money Laundering Directive was adopted under the UK's presidency of the EU in October 2005. It represents Europe's commitment to fighting the international problems of money laundering and terrorist financing by implementing the global standards produced by the Financial Action Task Force in 2003. The UK Government must implement the Directive into UK law by December 2007. In July 2006, Her Majesty's Treasury released a consultative document discussing how the government seeks to implement the directive. It identifies the areas in which changes need to be made to the Money Laundering Regulations and areas where the Government has flexibility over implementation, and discusses the options available.

The Proceeds of Crime Act 2002 has enhanced the efficiency of the forfeiture process and increased the recovered amount of illegally obtained assets. The Act consolidates existing laws on forfeiture and money laundering into a single piece of legislation, and, perhaps most importantly, creates a civil asset forfeiture system for the proceeds of unlawful conduct. It also creates the Assets Recovery Agency (ARA), to enhance financial investigators' power to request information from any bank about whether it holds an account for a particular person. The Act provides for confiscation orders and for restraint orders to prohibit dealing with property. It also allows for the recovery of property that is, or represents, property obtained through unlawful conduct, or that is intended to be used in unlawful conduct. Furthermore, the Act shifts the burden of proof to the holder of the assets to prove that the assets were acquired through lawful means. In the absence of such proof, assets may be forfeited, even without a criminal conviction. The Act gives standing to overseas requests and orders concerning property believed to be the proceeds of criminal conduct. The Act also provides the ARA with a national standard for training investigators, and gives greater powers of seizure at a lower standard of proof. In light of this, Her Majesty's Revenue and Customs (HMRC) has increased its national priorities to include investigating the movement of cash through money exchange houses and identifying unlicensed money remitters. The total value of assets recovered by all agencies under the Act (and earlier legislation) in England, Wales, and Northern Ireland was approximately $96.6 million in 2004 and approximately $149.6 million in 2005. The Assets Recovery Unit had announced additional seizures worth approximately $30 million in 2006 with an additional $200 million under restraint pending the outcome of court cases.

The Terrorism (United Nations Measures) Order 2001 makes it an offense for any individual to make any funds for financial or related services available, directly or indirectly, to or for the benefit of a person who commits, attempts to commit, facilitates, or participates in the commission of acts of terrorism. The Order also makes it an offense for a bank or building society to fail to disclose to the Treasury a suspicion that a customer or entity with whom the institution has had dealings since October 10, 2001, is attempting to participate in acts of terrorism. The Anti-Terrorism, Crime, and Security Act 2001 provides for the freezing of assets. In March 2006, the Terrorism Act received Royal Assent. This Act aims to impede the encouragement of others to commit terrorist acts, and amends existing legislation. Changes include: the introduction of warrants to enable police to search any property owned or controlled by a terrorist suspect, the extension of terrorism stop and search powers to cover bays and estuaries, with improved search powers at ports, the extension of police powers to detain suspects after arrest for 28 days (although intervals exceeding two days must be approved by a judicial authority), and the increased flexibility of the proscription regime, including the power to proscribe groups that glorify terrorism. As of October 2006, the UK had frozen a total of 188 accounts and approximately $966,000 in suspected terrorist funds.

As a direct result of the events of September 11, 2001, the FID established a separate National Terrorist Financing Investigative Unit (NTFIU), to maximize the effect of reports from the regulated sector. The NTFIU chairs a law enforcement group to provide outreach to the financial industry concerning requirements and typologies. The NTFIU is now under the remit of SOCA. The

operational unit that responds to the work and intelligence development of the NTFIU has seen a threefold increase in staffing levels directly due to the increase in the workload. The Metropolitan Police responded to the growing emphasis on terrorist financing by expanding the focus and strength of its specialist financial unit dedicated to this area of investigations.

Charitable organizations and foundations are subject to supervision by the UK Charities Commission. Such entities must be licensed and are subject to reporting and record keeping requirements. The Commission has investigative and administrative sanctioning authority, up to and including the authority to remove management, appoint trustees and place organizations into receivership. The Government intends to revise its reporting requirements in 2007 to develop a risk-based approach to monitoring with a new serious incident reporting function for charities.

The UK cooperates with foreign law enforcement agencies investigating narcotics-related financial crimes. The UK is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. In February 2006, the UK ratified both the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. The UK is a member of the FATF. SOCA is an active member of the Egmont Group and has information sharing arrangements in place with the FIUs of the United States, Belgium, France, and Australia. The Mutual Legal Assistance Treaty (MLAT) between the UK and the United States has been in force since 1996 (the United States and UK signed a reciprocal asset sharing agreement in March 2003). The UK also has an MLAT with the Bahamas. Additionally, there is a memorandum of understanding in force between the U.S. Immigration and Customs Enforcement and HM Revenue and Customs.

The United Kingdom should develop legislation and implementing regulations to ensure that the gaming and betting industries are completely covered in the same manner as the financial and designated nonfinancial businesses and professions. This should include a legal requirement to disclose suspicious transactions rather than relying on the industries' own codes of practice. In addition, authorities should track and examine the effects of the SOCAP change regarding acts and assets in or from foreign jurisdictions, and revisit this legislation to determine whether it has been effective, or whether it has enabled exploitation.

## Uruguay

In the past, Uruguay's strict bank secrecy laws, liberal currency exchange, capital mobility regulations and overall economic stability made it a regional financial center vulnerable to money laundering, though the extent and the nature of suspicious financial transactions have been unclear. In 2002, banking scandals and mismanagement, along with massive withdrawals of Argentine deposits, led to a near collapse of the Uruguayan banking system, significantly weakening Uruguay's role as a regional financial center. This crisis may have diminished the attractiveness of Uruguayan financial institutions for money launderers in the medium term. However, Uruguay's status as an offshore financial center and partially dollarized economy may increase the risk of money laundering and terrorist financing activity.

Fiduciary (offshore) companies called "SAFIs" are thought to be a convenient conduit for illegal money transactions. As of January 1, 2006, all SAFIs are required to provide the names of their directors to the Finance Ministry. In addition, the GOU has decided to completely eliminate SAFIs as part of a comprehensive tax reform law that will be presented to the legislature this year. The draft legislation will also implement a personal income tax for the first time in Uruguay.

Offshore banks are subject to the same laws and regulations as local banks, with the Government of Uruguay (GOU) requiring them to be licensed through a formal process that includes a background investigation. There are six offshore banks and 21 representative offices of foreign banks. Offshore trusts are not allowed. Bearer shares may not be used in banks and institutions under the authority of

the Central Bank, and any share transactions must be authorized by the Central Bank. There are eight free trade zones in Uruguay, all but two being little more than warehouses for regional distribution. The other two house software development firms, back-office operations, call centers, and some light manufacturing and assembly. Some of the warehouse-style free trade zones have been used as transit points for containers of counterfeit goods bound for Brazil and Paraguay. Recent U.S. law enforcement investigations have also revealed suspected funds from the Triborder Area between Argentina, Brazil and Paraguay moving through money remittance companies located in Uruguay.

Over the past five years, the GOU has instituted several legislative and regulatory reforms in its anti-money laundering regime. The May 2001 Law 17,343 extends the predicate offenses beyond narcotics trafficking and corruption to include terrorism; smuggling (value over $20,000); illegal trafficking in weapons, explosives and ammunition; trafficking in human organs, tissues and medications; trafficking in human beings; extortion; kidnapping; bribery; trafficking in nuclear and toxic substances; and illegal trafficking in animals or antiques. Money laundering is considered a crime separate from underlying offenses.

The courts have the power to seize and confiscate property, products or financial instruments linked to money laundering activities. The Central Bank also has the authority to freeze assets for 72 hours, pending a judicial decision. The banking community generally cooperates well with enforcement efforts. There is no specific system for sharing assets with foreign counterparts, but in theory it would be allowed under the provisions of treaties and agreements signed by Uruguay. There is, however, close cooperation with the United States in the sharing of intelligence related to investigations and proceedings. A recent case involving the largest cocaine seizure in Uruguay's history was aided by an unprecedented level of cooperation with U.S. and other foreign law enforcement authorities.

In September 2004, the Uruguayan Congress approved Law 17,835, which significantly strengthens the GOU's money laundering regime. It also includes specific provisions related to the financing of terrorism and to the freezing of assets linked to terrorist organizations, as well as to undercover operations and controlled deliveries. The first arrest and prosecution for money laundering under the new legislation occurred in October 2005, and the case is still pending. A more recent high profile case, involving money laundering linked to Uruguay's largest cocaine seizure, is at the initial stage. Indications are that this case has invigorated the GOU's efforts to fight money laundering and to push for increased reporting of suspicious activities.

Law 17,835 of 2004 expands the realm of entities required to file suspicious activities reports (SARs) and makes reporting of such activities a legal obligation. It specifically confers to Uruguay's financial intelligence unit (FIU), the Financial Information and Analysis Unit (UIAF) of the Central Bank, the role of receiving and analyzing SARs, and disseminating those reports that warrant further investigation to judicial authorities, such as the National Police or the Ministry of the Public Prosecutor. The UIAF also has the authority to request additional related information from obligated reporting entities. Central Bank Circular 1722 of 2000, which created the UIAF, provides the authority to respond to requests for international cooperation. The UIAF is also empowered to issue instructions to the institutions supervised by the Central Bank for them to bar, for a period of up to 72 hours, all transactions involving individuals or legal entities under reasonable suspicion of being linked to the crimes of money laundering and related offenses. The decision must be communicated immediately to the competent criminal court, which will determine, if needed, the freezing of the assets of the parties involved.

In November 2004, Resolution 2002-2072 of the Central Bank Board of Directors raised the UIAF to the level of a directorate reporting directly to the Board. Central Bank regulations require all banks, currency exchange houses, stockbrokers and insurance companies to implement anti-money laundering policies. These policies include thoroughly identifying customers, recording transactions over $10,000 in internal databases, and reporting suspicious transactions to the UIAF. Law 17,835

makes the implementation of these policies a legal obligation extended to all financial intermediaries, including casinos, dealers in art and precious stones and metals, and real estate and fiduciary companies. The law also extends legal protection to reporting institutions for filing SARs. Additionally, Law 17,835 extends the reporting requirement to all persons entering or exiting Uruguay with over $10,000 in cash or in monetary instruments. Regulations for Law 17,835 have been issued by the Central Bank for all entities it supervises, and are being issued by the Ministry of Economy and Finance for all other reporting entities, such as casinos, real estate brokers and art dealers. Although now deemed obligated entities by law, many sectors—including insurance companies, securities firms, money remitters, casinos and most designated nonfinancial businesses—do not yet report suspicious transactions to the UIAF.

The UIAF received 62 SARs in the first 9 months of 2006, almost double the amount received over the same period in 2005. Over the first 9 months of 2006, the UIAF also received 9 action requests from the courts and 15 information requests from foreign FIUs. While the level of staffing at the UIAF is not considered to be adequate, the Central Bank has hired additional staff and established a timeline to reach full staffing. The recent high profile narcotics money laundering case is expected to provide a boost to the Central Bank's efforts.

Three government bodies are responsible for coordinating GOU efforts to combat money laundering: the UIAF, the National Drug Council and the Center for Training on Money Laundering (CECPLA). The President's Deputy Chief of Staff heads the National Drug Council, which is the senior authority for anti-money laundering policy. The Director of CECPLA serves as coordinator for all government entities involved in anti-money laundering efforts, and sets general policy guidelines. The Director defines and implements GOU policies, in coordination with the Finance Ministry and the UIAF. The Ministry of Economy and Finance, the Ministry of the Interior (via the police force), and the Ministry of Defense (via the Naval Prefecture) also participate in anti-money laundering efforts. The financial private sector, most of which is foreign-owned, has developed self-regulatory measures against money laundering such as the Codes of Conduct approved by the Association of Banks and the Chamber of Financial Entities (1997), the Association of Exchange Houses (2001), and the Securities Market (2002).

Despite the power of the courts to confiscate property linked to money laundering, real estate ownership is not publicly registered in the name of the titleholder, complicating efforts to track money laundering in this sector, especially in the partially foreign-owned tourist industry. The UIAF and other government agencies must obtain a judicial order to have access to the name of titleholders. The GOU is in the process of implementing a national computerized registry that will facilitate the UIAF's access to titleholders' names.

Uruguay is a founding member of the Financial Action Task Force for South America (GAFISUD), created in December 2000 and based in Buenos Aires. Since early 2005, the ex-director of the Center for Training on Money Laundering Issues (CECPLA) has served as the GAFISUD Executive Secretary. In 2005, the International Monetary Fund (IMF), in conjunction with GAFISUD, concluded the second mutual evaluation of Uruguay's anti-money laundering and counterterrorist financing regime. Their report was presented at the GAFISUD plenary meeting in July 2006. The evaluation recognized Uruguay's advances with its new legislation but pointed out that some regulations still needed to be drafted in order to fully implement the legislative reforms. The evaluation team did not consider the UIAF to be fully operational due to understaffing and limited resources.

The GOU has taken steps to bring Uruguay into compliance with the Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing. Some of these recommendations, such as the criminalization of terrorism financing and provisions for the freezing of terrorist assets, were partially met by Law 17,835. Law 17,835 establishes a prison term of three to 18 years for terrorist financing, requires financial institutions inform the UIAF of funds that may be connected to persons

on the United Nations 1267 Sanctions Committee list and individual country lists, and allows for the freezing of terrorist funds. However, as noted by the IMF and GAFISUD mutual evaluation team, terrorist financing is a crime only to the extent that funds are collected or solicited for terrorist acts. The provision of funds to terrorists or terrorist groups, for purposes other than planned or committed acts of terrorism, is not specifically criminalized. Although terrorism is considered a predicate offense for money laundering, terrorism is not criminalized under Uruguayan law; Law 17,835, however, does establish criteria for determining the "terrorist nature" of an offense. Nonprofit organizations are not assessed for terrorist financing risk, and oversight of these institutions was deemed by the IMF/GAFISUD evaluation team to be insufficient.

The GOU states that safeguarding the financial sector from money laundering is a priority, and Uruguay remains active in international anti-money laundering efforts. Uruguay is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. It has signed, but not yet ratified, the UN Convention against Corruption and the Inter-American Convention against Terrorism. The GOU is a member of GAFISUD and the OAS Inter-American Drug Abuse Control Commission (CICAD) Experts Group to Control Money Laundering. The United States and Uruguay are parties to extradition and mutual legal assistance treaties that entered into force in 1984 and 1994, respectively.

In 2006, the Government of Uruguay continued to implement the reforms it began in 2004 and 2005 to strengthen its anti-money laundering and counterterrorist financing regime. The passage of legislation criminalizing terrorist financing, albeit limited only to the financing of terrorist acts, places Uruguay ahead of many other nations in the region. Nevertheless, the GOU should amend its legislation to make the funding of terrorists or terrorist organizations a crime. Uruguay is one of only two countries in South America that is not a member of the Egmont Group of financial intelligence units. Membership in the Egmont Group would provide the GOU with greater access to financial information that is essential to its efforts to combat money laundering and terrorist financing. The UIAF's membership in the Egmont Group, as well as the GOU's continued implementation, enhancement and enforcement of its anti-money laundering and counterterrorist financing programs, should continue to be priorities for the GOU.

## Uzbekistan

Uzbekistan is not considered an important regional financial center and does not have a well developed financial system. Legitimate business owners, ordinary citizens, and foreign residents generally attempt to avoid using the Uzbek banking system for transactions, except when absolutely required, because of the nature of the Government of Uzbekistan's (GOU) financial control system, the fear of GOU seizure of one's assets, and the lack of trust in the banking system as a whole. As a result, Uzbek citizens have functioning bank accounts only if they are required to do so by law. Citizens only deposit funds they are required to deposit and often resort to subterfuge to avoid depositing currency. The Central Bank of Uzbekistan (CB) asserts that deposits from individuals have been increasing over the past four years.

Proceeds from narcotics and black market smuggling are primary sources of money laundering. Narcotics proceeds are controlled by local and regional drug-trafficking organizations and organized crime. Foreign and domestic proceeds from criminal activity in Uzbekistan are held either in cash, high-value transferable assets, such as gold, property, or automobiles, or in foreign bank accounts.

There is a significant black market for smuggled goods in Uzbekistan. Since the GOU imposed a very restrictive trade and import regime in the summer of 2002, smuggling of consumer goods, already a considerable problem, increased dramatically. Many Uzbek citizens continue to make a living by illegally shuttle-trading goods from neighboring countries, Iran, the Middle East, India, Korea, Europe, and the U.S. The black market for smuggled goods does not appear to be significantly funded

by narcotics proceeds. It is likely, however, that drug dealers use the robust black market to clean their drug-related money.

Reportedly, the unofficial, unmonitored cash-based market creates an opportunity for small-scale terrorist or drug-related laundering of funds destined for internal operations. For the most part, the funds generated by smuggling and corruption are not directly laundered through the banking system, but through seemingly legitimate businesses such as restaurants and high-end retail stores. There appears to be virtually no money laundering through formal financial institutions in Uzbekistan because of the extremely high degree of supervision and control over all bank accounts in the country exercised by the CB, Ministry of Finance, General Prosecutor's Office (GPO), and state-owned and controlled banks. Although Uzbek financial institutions are not known to engage in illegal transactions in U.S. currency, illegal unofficial exchange houses, where the majority of cash-only money laundering takes place, deal in Uzbek soum and U.S. dollars. Moreover, drug dealers and others can transport their criminal proceeds in currency across Uzbekistan's porous borders for deposit in the banking systems of other countries, such as Kazakhstan, Russia or the United Arab Emirates.

Laundering the proceeds of drug-trafficking and other criminal activities is a criminal offense. Article 41 of the Law on Narcotic Drugs and Psychotropic Substances (1999) provides that any institution may be closed for performing a financial transaction for the purpose of legalizing (laundering) proceeds derived from illicit narcotics trafficking. Penalties for money laundering are from ten to fifteen years' imprisonment, under Article 243 of the Criminal Code. This article defines the act of money laundering to include as punishable acts the transfer, conversion, exchange, or concealment of origin, true nature, source, location, disposition, movement and rights with respect to the assets derived from criminal activity. Although the law has been in effect for more than five years, the GOU has been unable to provide sufficient information to fully assess the implementation and use of this legislation. The GOU has not adopted "banker negligence" laws that hold individual bankers responsible if their institutions launder money.

The CB, GPO, and the National Security Service (NSS) closely monitor all banking transactions to ensure that money laundering does not occur in the banking system. Banks are required to know, record, and report the identity of customers engaging in significant transactions, including the recording of large currency transactions at thresholds appropriate to Uzbekistan's economic situation. All transactions involving sums greater than $1000 in salary expenses for legal entities and $500 in salaries for individuals must be tracked and reported to the authorities. The CB unofficially "requires" commercial banks to report on private transfers to foreign banks exceeding $10,000. Depending on the type and amount of the transaction, banks are required to maintain records for time deposits for a minimum of five years. The law contains a safe harbor provision, protecting reporting individuals with respect to their cooperation with law enforcement entities.

In 2004, Uzbekistan's Parliament passed the Law on the Fight Against Legitimization of Proceeds of Crime and Combating Terrorism Financing, which went into effect on January 1, 2006. The law requires certain entities to report cash transactions above $40,000 (approximately), as well as suspicious transactions. Banks, credit unions and other lending institutions are covered entities. The law also covers some nonbanking financial institutions, such as investment funds, depositaries and other types of investment institutions; exchange houses; insurers; organizations which render leasing and other financial services; postal organizations; pawnshops; gaming houses; lotteries; and notary offices. It does not include intermediaries such as lawyers, accountants, or broker/dealers. Although casinos are illegal, GOU enforcement is generally lax, and several exist openly in Tashkent.

The Law on Banks and Bank Activity (1996), article 38, stipulates conditions under which banking information can be released to law enforcement, investigative and tax authorities, prosecutor's office and courts. Different conditions for disclosure apply to different types of clients—individuals and institutions. In September 2003, Uzbekistan enacted a bank secrecy law that prevents the disclosure of

client and ownership information for domestic and offshore financial services companies to bank supervisors and law enforcement authorities. In all cases, private bank information can be disclosed to prosecution and investigation authorities, provided there is a criminal investigation underway. The information can be provided to the courts on the basis of a written request in relation to cases currently under consideration. Protected banking information also can be disclosed to tax authorities in cases involving the taxation of a bank's client. Additionally, under a new 2006 Presidential decree and subsequent Cabinet of Ministers' resolution on the disclosure of information related to money laundering, it is mandatory for organizations involved in monetary and other transactions to report such transactions to a new Financial Intelligence Unit within the GPO (discussed below).

Existing controls on transportation of currency across borders would, in theory, facilitate detection of the international transportation of illegal source currency. When entering or exiting the country, foreigners and Uzbek citizens are required to report all currency they are carrying. Residents and nonresidents may bring the equivalent of $10,000 into the country tax-free. Amounts in excess of this limit are assessed a one-percent duty. Nonresidents may take out as much currency as they brought in. However, residents are limited to the equivalent of $2,000. Residents wishing to take out higher amounts must obtain authorization to do so; amounts over $2,000 must be approved by an authorized commercial bank, and amounts over $5,000 must be approved by the CB. International cash transfers to or from an individual person are limited to $5,000 per transaction; there is no monetary limit on international cash transfers made by legal entities, such as corporations. However, direct wire transfers to or from other Central Asian countries are not permitted; a third country must be used.

International business companies are permitted to have offices in Uzbekistan and are subject to the same regulations as domestic businesses, if not stricter. Offshore banks are not present in Uzbekistan and other forms of exempt or shell companies are not officially present.

In April 2006, the President of Uzbekistan signed a decree entitled, "On Actions to Strengthen Combating Financial, Economic and Tax Crimes and Legalization of Criminally Gained Income." This decree expands the mandate of the General Prosecutor's Office for Combating Tax and Hard Currency Crimes to include combating money laundering, and established the Department on Combating Tax, Currency Crimes and Legalizations of Criminal Proceeds under the GPO. This Department, which will serve as Uzbekistan's Financial Intelligence Unit (FIU), will conduct operational, analytical and investigative work in the areas of tax and hard currency crimes, money laundering and terrorism financing. The FIU is charged with monitoring and preventing money laundering and terrorist financing. It will analyze information received from banks and financial institutions, create and keep electronic databases of financial crimes, and, when warranted, pass information to the CB, tax and law enforcement authorities, or other parts of the GPO for investigation and prosecution of criminal activity. Authorities envisage a staff of 22 people in the FIU. The Department of Investigation of Economic Crimes within the Ministry of Internal Affairs (MVD) and a specialized structure within the NSS also are authorized to conduct investigations of money laundering offenses.

In the coming year, the new FIU analysts and investigators, as well as authorities in related ministries and agencies, will require training and capacity building for the FIU. Uzbekistan has entered into agreements with supervisors to facilitate the exchange of supervisory information including on-site examinations of banks and trust companies operating in the country. Since September 2006, the Uzbek financial supervisory authorities, along with law enforcement officers, have been attending World Bank-sponsored workshops to acquaint them with the AML/CFT law. These workshops will continue into May 2007.

In July 2006, the Uzbek Cabinet of Ministers adopted a resolution on the submission of data to the FIU related to money laundering and terrorism financing.

Unofficial information from numerous law enforcement officials indicates that there have been few, if any, prosecutions for money laundering under article 243 of the Criminal Code since its enactment in 2001. MVD officials claim to have opened nine money laundering-related cases in 2005 and six cases in the first six months of 2006. No information was provided on the ultimate disposition of these cases. In March 2006, an opposition activist was convicted for money laundering and other economic crimes, but the defendant was freed in May and the sentence was suspended, reportedly due to human rights questions surrounding the case. Overall, the GOU appears to lack a sufficient number of experienced and knowledgeable agents to investigate money laundering.

Article 155 of Uzbekistan's Criminal Code and the law "On Fighting Terrorism" criminalize terrorist financing. The latter law names the NSS, the MVD, the Committee on the Protection of State Borders, the State Customs Committee, the Ministry of Defense, and the Ministry for Emergency Situations as responsible for implementing the counterterrorist legislation. The law names the NSS as the coordinator for government agencies fighting terrorism. The GOU has the authority to identify, freeze, and seize terrorist assets. Uzbekistan has circulated to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the names of individuals and entities included on the UN 1267 consolidated list. In addition, the GOU has circulated the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 to the CB, which has, in turn, forwarded these lists to banks operating in Uzbekistan. According to the CB, no assets have been frozen.

Other than a plan to step up enforcement of currency regulations, the GOU has taken no steps to regulate or deter alternative remittance systems such as hawala, black market exchanges, trade-based money laundering, or the misuse of gold, precious metals and gems, nor are any legislative initiatives addressing alternative remittance under consideration. Although officially there is complete currency convertibility, in reality convertibility requests can be significantly delayed or refused. The GOU took additional steps in the second half of 2005 to further restrict convertibility, leading to a slightly higher black market exchange rate for the soum.

The GOU closely monitors the activities of charitable and nonprofit entities, such as NGOs, that can be used for the financing of terrorism. In February 2004, the Cabinet of Ministers issued Decree 56 to allow the government to vet grants to local NGOs from foreign sources, ostensibly to fight money laundering and terrorist financing. Given the degree of supervision of charities and other nonprofits, and the level of threat Uzbekistan perceives from the Islamic Movement of Uzbekistan (IMU) and other extremist organizations, it is extremely unlikely that the NSS would knowingly allow any funds to be funneled to terrorists through Uzbekistan-based charitable organizations or NGOS.

Uzbekistan has established systems for identifying, tracing, freezing, seizing, and forfeiting proceeds of both narcotics-related and money laundering-related crimes. Current laws include the ability to seize items used in the commission of crimes such as conveyances used to transport narcotics, farm facilities (except land) where illicit crops are grown or which are used to support terrorist activity, legitimate businesses if related to criminal proceeds and bank accounts. The banking community, which is entirely state-controlled and, with few exceptions, state-owned, cooperates with efforts to trace funds and seize bank accounts. Uzbek law does not allow for civil asset forfeiture, but the Criminal Procedure Code provides for "civil" proceedings within the criminal case to decide forfeiture issues. As a practical matter, these proceedings are conducted as part of the criminal case. There appears to be no new legislation or changes to current law under active consideration by the GOU regarding seizure or forfeiture of assets. The obstacles to enacting such laws are largely rooted in the widespread corruption that exists within the country.

In 2000, Uzbekistan set up a fund to direct confiscated assets to law enforcement activities. In accordance with the regulation, the assets derived from the sale of confiscated proceeds and instruments of drug-related offenses were transferred to this fund to support entities of the NSS, the

MVD, the State Customs Committee, and the Border Guard Committee, all of which are directly involved in combating illicit drug trafficking. According to the GOU, a total of 115 million soum (approximately $97,000) was deposited into this fund, roughly $80,000 of which was turned over to Uzbek law enforcement agencies. In 2004, however, the Cabinet of Ministers issued an order to close the Special Fund as of November 1, 2004. Under the new procedures, each agency manages the assets it seizes. There is also a specialized fund within the MVD to reward those officers who directly participate in or contribute to law enforcement efforts leading to the confiscation of property. This fund has generated 20 percent of its assets from the sale of property confiscated from persons who have committed offenses such as the organization of criminal associations, bribery and racketeering. The GOU enthusiastically enforces existing drug-related asset seizure and forfeiture laws. The GOU has not been forthcoming with information regarding the total dollar value of assets seized from crimes. Reportedly, existing legislation does not permit sharing of seized narcotics assets with other governments.

The GOU realizes the importance of international cooperation in the fight against drugs and transnational organized crime and has made efforts to integrate the country in the system of international cooperation. Uzbekistan has entered into bilateral agreements for cooperation or exchange of information on drug related issues with the United States, Germany, Italy, Latvia, Bulgaria, Poland, China, Iran, Pakistan, the CIS, and all the countries in Central Asia. It has multilateral agreements within the framework of the CIS and under the Shanghai Cooperation Organization (SCO). An "Agreement on Narcotics Control and Law Enforcement Assistance" was signed with the United States on August 14, 2001, with two supplemental agreements that came into force in 2004.

Uzbekistan does not have a Mutual Legal Assistance Treaty with the United States. However, Uzbekistan and the United States have reached informal agreement on mechanisms for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing and other serious crime investigations. In the past, Uzbekistan has cooperated with appropriate USG law enforcement agencies and other governments investigating financial crimes and several important terrorist-related cases. However, cooperation in these areas has become increasingly problematic in an atmosphere of deteriorating U.S.-Uzbekistan bilateral relations.

Uzbekistan joined the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG), a FATF-style regional body, at the group's December 2005 plenary meeting. In April 2006, at the invitation of the Prosecutor General of Uzbekistan, the EAG Chairman visited Tashkent to discuss, in part, Uzbekistan's partnership in the EAG, the progress the country has made in establishing an AML/CFT regime, and technical assistance that will be required. Uzbekistan is scheduled to have an EAG mutual evaluation in 2008.

The GOU is an active party to the relevant agreements concluded under the CIS, CAEC, ECO, SCO, and the "Six Plus Two" Group. In December 2005, Uzbekistan hosted the SCO in Tashkent to discuss issues relating to and the overall prevention of money laundering. Uzbekistan is also a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime.

A lack of trained personnel, resources, and modern equipment continues to hinder Uzbekistan's efforts to fight money laundering and terrorist financing. The GOU should ensure that those with supervisory authority and those charged with investigating potential money laundering and terrorism financing have the training and resources necessary to be effective. This includes legal resources as well: the GOU should continue to refine its pertinent legislation to adhere to international standards. Uzbekistan also should expand the cross-border currency reporting rules to cover the transfer of monetary instruments, gold, gems and precious metals. Access to financial institution records should be given to appropriate regulatory and law enforcement agencies so that they can properly conduct compliance

examinations and investigations. Furthermore, while the establishment of a Financial Intelligence Unit is a positive step, its effectiveness will depend on the unit's authority as the sole repository and analytical tool for suspicious transaction reporting. The FIU's ability to effectively cooperate with other GOU law enforcement and regulatory agencies in receiving and disseminating information on suspicious transactions will be critical to the success of an AML/CFT regime. The GOU should ensure that the FIU has the appropriate resources, including the technical requirements for a database, training on analytical, legal and technical elements for the staff, and the authority and bureaucratic tools to meet international standards and accomplish its mandate.

## Vanuatu

Vanuatu's offshore sector is vulnerable to money laundering, as Vanuatu has historically maintained strict banking secrecy provisions that have the effect of preventing law enforcement agencies from identifying the beneficial owners of offshore entities registered in the sector. Due to allegations of money laundering, and in response to pressure from the Financial Action Task Force (FATF), a few United States-based banks announced in December 1999 that they would no longer process U.S. dollar transactions to or from Vanuatu. The Government of Vanuatu (GOV) responded to these concerns by introducing reforms designed to strengthen domestic and offshore financial regulation. The GOV passed amendments to four of its main legislations pieces of legislation relative to money laundering and terrorist financing during its last session of Parliament in November 2005. The four pieces of legislation affected are the Mutual Assistance in Criminal Matters Act No. 31 of 2005, the Financial Transaction Reporting Act No. 28 of 2005, the Counter-Terrorism and Transnational Organized Crime Act No. 29 of 2005, and the Proceeds of Crime Act (Amendment) Act No. 30 of 2005.

Vanuatu's financial sector includes four domestic licensed banks (that carry out domestic and offshore business); one credit union; seven international banks; five insurance providers (both life and general); and eight foreign exchange instrument dealers, money remittance dealers and bureaux de change, all of which are regulated by the Reserve Bank of Vanuatu. Since the passage of the International Banking Act of 2002, the Reserve Bank of Vanuatu regulates the offshore banking sector that includes the seven international banks and approximately 4,700 international business companies (IBCs), as well as offshore trusts and captive insurance companies. These institutions were once regulated by the Financial Services Commission. IBCs are now registered with the Vanuatu Financial Services Commission. This change was one of many recommendations of the 2002 International Monetary Fund Module II Assessment Report (IMFR) that found Vanuatu's onshore and offshore sectors to be "noncompliant" with many international standards.

Regulatory agencies in Vanuatu have instituted stricter procedures for issuance of offshore banking licenses under the International Banking Act No. 4 of 2002, and continue to review the status of previously issued licenses. All financial institutions, both domestic and offshore, are required to report suspicious transactions and to maintain records of all transactions for six years, including the identities of the parties involved.

The Financial Transaction Reporting Act (FTRA) of 2000 established Vanuatu's Financial Intelligence Unit (FIU) within the State Law Office. The FIU receives suspicious transaction reports (STRs) filed by banks and distributes them to the Public Prosecutor's Office, the Reserve Bank of Vanuatu, the Vanuatu Police Force, the Vanuatu Financial Services Commission, and law enforcement agencies or supervisory bodies outside Vanuatu. The FIU also issues guidelines to, and provides training programs for, financial institutions regarding record keeping for transactions and reporting obligations. The Act also regulates how such information can be shared with law enforcement agencies investigating financial crimes. Financial institutions within Vanuatu must establish and maintain internal procedures to combat financial crime. Every financial institution is required to keep records of all transactions. Five key pieces of information are required to be kept for every financial

transaction: the nature of the transaction, the amount of the transaction, the currency in which it was denominated, the date the transaction was conducted, and the parties to the transaction.

Although the amendments have been withdrawn from Parliament twice, FTRA amendments were finally passed in November 2005 and enacted in late February 2006. The amendments include mandatory customer identification requirements; broaden the range of covered institutions required to file STRs to include auditors, trust companies, and company service providers; and provide safe harbor for both individuals and institutions required to file STRs. In addition to STR filings, financial institutions will now be required to file currency transaction reports (CTRs), which involves any single transaction in excess of VT 1 million (approximately $9,100) or its equivalent in a foreign currency, and wire transfers into and out of Vanuatu in excess of VT 1 million. The amendments also require financial institutions to maintain internal procedures to implement reporting requirements, appoint compliance officers, establish an audit function to test their anti-money laundering and terrorist financing procedures and systems, as well as provide the FIU a copy of their internal procedures. Failure to do so will result in a fine or imprisonment for an individual, or a fine in the case of a corporate entity. The amendments supersede any inconsistent banking or other secrecy provisions and clarify the FIU's investigative powers.

The amended FTRA defines financial institutions to include casinos licensed under the Casino Control Act No.6 of 1993, lawyers, notaries, accountants and trust and company service providers. The scope of the legislation is so broad that entities such as car dealers and various financial services that currently do not exist in Vanuatu (and are unlikely to in the future) are covered. Applications by foreigners to open casinos are subject to clearance by the Vanuatu Investment Promotion Authority (VIPA) which reviews applications and conducts a form of due diligence on the applicant before issuing a certification of the department of Customs and Revenue to issue an appropriate license. The Department of Customs and Inland Revenue receives applications from local applicants directly.

The Vanuatu Police Department and the FIU are the primary agencies responsible for ensuring money laundering and terrorist financing offences are properly investigated in Vanuatu. The Public Prosecutions Office (PPO) is responsible for the prosecution of money laundering and terrorist financing offences. The Vanuatu Police Department has established a Transnational Crime Unit (TCU), and is responsible for investigations involving money laundering and terrorist financing offences, the identification and seizure of criminal proceeds, as well as conducting investigations in cooperation with foreign jurisdictions.

Supervision of the financial services sector is divided between three main agencies: the Reserve Bank of Vanuatu (RBV), the Vanuatu Financial Services Commission (VFSC) and the Customs and Revenue Branch of the Ministry of Finance. The RBV is responsible for supervising and regulating domestic and off-shore banks. The VFSC supervises insurance providers, credit unions, charities and trust and company service providers, but is unable to issue comprehensive guidelines or to regulate the financial sectors it has responsibility for.

The Serious Offenses (Confiscation of Proceeds) Act 1989 criminalized the laundering of proceeds from all serious crimes and provided for seizure of criminal assets and confiscation after a conviction. The Proceeds of Crime Act (2002) retained the criminalization of the laundering of proceeds from all serious crimes, criminalized the financing of terrorism, and included full asset forfeiture, restraining, monitoring, and production powers regarding assets. A new development to the Proceeds of Crime Act No. 30 of 2005 was an insertion of Section 74A, which now cover the cross-border movement of currency. After the passing of the bill in Parliament in November 2005, all incoming and outgoing passengers to and from Vanuatu will be legally obligated to declare to the Department of Customs cash exceeding one million Vatu in possession (approximately $9,100).

Vanuatu passed the Mutual Assistance in Criminal Matters Act in December 2002 for the purpose of facilitating the provision of international assistance in criminal matters for the taking of evidence,

search and seizure proceedings, forfeiture or confiscation of property, and restraints on dealings in property that may be subject to forfeiture or seizure. The Attorney General possesses the authority to grant requests for assistance, and may require government agencies to assist in the collection of information pursuant to the request. The Extradition Act of 2002 includes money laundering within the scope of extraditable offenses.

The amended International Banking Act has now placed Vanuatu's international and offshore banks under the supervision of the Reserve Bank of Vanuatu. Section 5(5) of the Act states that if existing licensees wish to carry on international banking business after December 31, 2003, the licensee should have submitted an application to the Reserve Bank of Vanuatu under Section 6 of the Act for a license to carry on international banking business. If an unregistered licensee continued to conduct international banking business after December 31, 2003, in violation of Section 4 of the Act, the licensee is subject to a fine or imprisonment. Under Section 19 of the Act, the Reserve Bank can conduct investigations where it suspects that an unlicensed person or entity is carrying on international banking business. Since this time, three international banking businesses have had their licenses revoked.

One of the most significant requirements of the amended legislation is the banning of shell banks. As of January 1, 2004, all offshore banks registered in Vanuatu must have a physical presence in Vanuatu, and management, directors, and employees must be in residence. At the September 2003 plenary session of the Asia/Pacific Group on Money Laundering (APG), Vanuatu noted its intention to draft new legislation regarding trust companies and company service providers, which it is now in the final stages of completing. The new legislation will cover disclosure of information with other regulatory authorities, capital and solvency requirements, and "fit and proper" requirements. In 2005, Vanuatu enacted Insurance Act No. 54, drafted in compliance with standards set by the International Association of Insurance Supervisors.

International Business Companies (IBC) may be registered using bearer shares, shielding the identity and assets of beneficial owners of these entities. Secrecy provisions protect all information regarding IBCs and provide penal sanctions for unauthorized disclosure of information. These secrecy provisions, along with the ease and low cost of incorporation, make IBCs ideal mechanisms for money laundering and other financial crimes. Section 125 of the International Companies Act No. 31 of 1992 (ICA), provides a strict secrecy provision for information disclosure related to shareholders, beneficial ownership, and the management and affairs of IBCs registered in Vanuatu. This provision, in the past, has been used by the industry to decline requests made by the FIU for information. However, section 17(3) of the new amended FTRA clearly states that the new secrecy-overriding provision in the FTRA overrides section 125 of the ICA.

In November 2005, Vanuatu passed the Counter-Terrorism and Transnational Organized Crime Act (CTTOCA) No. 29 of 2005. The CTTOCA was brought into force on 24 February 2006. The aim of the Act is to implement UN Security Council Resolutions and Conventions dealing with terrorism and transnational organized crime, to prevent terrorists from operating in Vanuatu or receiving assistance through financial resources available to support the activities of terrorist organizations, and to criminalize human trafficking and smuggling. Terrorist financing is criminalized under section 6 of the CTTOCA. Section 7 of the CTTOCA makes it an offence to "directly or indirectly, knowingly make available property or financial or other related services to, or for the benefit of, a terrorist group." The penalty upon conviction is a term of imprisonment of not more than 25 years or a fine of not more than VT 125 million ($1 million), or both. Section 8 criminalizes dealing with terrorist property. The penalty upon conviction is a term of imprisonment of not more than 20 years or a fine of not more than VT100 million ($USD 876,500), or both. There were no terrorist financing or terrorism-related prosecutions or investigations in 2006.

In addition to its membership the Asia Pacific Group on Money Laundering, Vanuatu is a member of the Offshore Group of Banking Supervisors, the Commonwealth Secretariat, and the Pacific Island Forum. Its Financial Intelligence Unit became a member of the Egmont Group in June 2002. The GOV acceded to the UN International Convention for the Suppression of the Financing of Terrorism in October 2005, and acceded to both the UN Convention against Transnational Organized Crime and the 1988 UN Drug Convention on January 4, 2006. The FIU has a memorandum of understanding with Australia.

In March 2006, the APG conducted a mutual evaluation of Vanuatu, the results of which were reported at the APG plenary meeting in November 2006. The APG evaluation team found that Vanuatu had improved its anti-money laundering and counterterrorist financing regime since its first evaluation in 2000 by criminalizing terrorist financing, requiring a wider range of entities to report to the FIU and enhancing supervisory oversight of obligated entities. However, some deficiencies remain: the GOV has not taken a risk-based approach to combating money laundering and terrorist financing; a person who commits a predicate offense for money laundering cannot also be charged with money laundering; and current law does not require the names and addresses of directors and shareholders to be provided upon registration of an IBC.

The Government of Vanuatu should immobilize bearer shares and require complete identification of the beneficial ownership of international business companies (IBCs). It should implement all the provisions of its Proceeds of Crime Act and enact all additional legislation that is necessary to bring both its onshore and offshore financial sectors into compliance with international standards.

## Venezuela

Venezuela is one of the principal drug-transit countries in the Western Hemisphere, with an estimated 250-300 metric tons of cocaine passing through the nation during 2006. Venezuela's proximity to drug producing countries, weaknesses in its anti-money laundering regime, refusal to cooperate with the United States on counternarcotics activities, and rampant corruption throughout the law enforcement, judicial, banking, and banking regulatory sectors continue to make Venezuela vulnerable to money laundering. The main source of money laundering is believed to be from proceeds generated by cocaine and heroin trafficking organizations. Trade-based money laundering, such as the Black Market Peso Exchange, through which money launderers furnish narcotics-generated dollars in the United States to commercial smugglers, travel agents, investors, and others in exchange for Colombian pesos, remains a prominent method for laundering narcotics proceeds. It is reported that many of these black market traders ship their wares through Venezuela's Margarita Island free trade zone. Reportedly, some money is also laundered through the real estate market in Margarita Island.

Venezuela is not a regional financial center, nor does it have an offshore financial sector. The relatively small but modern banking sector, which consists of 55 banks, primarily serves the domestic market. The majority of these banks, about 90 percent, belong to the Venezuelan Association of Banks. Membership is voluntary and meetings are held monthly.

Money laundering in Venezuela is criminalized under the 2005 Organic Law against Organized Crime, the passage of which broadened the legal mechanisms provided by the 1993 Organic Drug Law. Under the Organic Law against Organized Crime, money laundering is an autonomous offense, punishable by a sentence of eight to twelve years in prison. Those who cannot establish the legitimacy of possessed or transferred funds, or are aware of the illegitimate origins of those funds, can be charged with money laundering, without any connection to drug-trafficking. In addition to establishing money laundering as an autonomous predicate offense, the Organic Law against Organized Crime broadens asset forfeiture and sharing provisions, adds conspiracy as a criminal offense, strengthens due diligence requirements, and provides law enforcement with stronger investigative powers by authorizing the use of modern investigative techniques, such as the use of undercover agents. This law,

coupled with the new Law Against the Trafficking and Consumption of Narcotics and Psychotropic Substances, effectively brings Venezuela's Penal Code in line with the 1988 UN Drug Convention.

In spite of the advances made with the passage of the Organic Law against Organized Crime in 2005, three major gaps remain. First, the financing of terrorism has yet to be specifically criminalized and there is still no independent financial investigative unit. One year after promulgation, there are no money laundering cases being tried under the new law. Many, if not most, judicial and law enforcement officials remain ignorant of the Law against Organized Crime and its specific provisions. Second, widespread corruption within the judicial and law enforcement sectors undermines the effectiveness of the law as a tool to combat the growing problem of money laundering. Finally, there is little evidence that the Government of Venezuela (GOV) has the will to effectively enforce the legislation it has promulgated.

Under the Organic Law against Organized Crime and Resolution 333-97 of the Superintendent of Banks and Other Financial Institutions (SBIF), anti-money laundering controls have been implemented requiring strict customer identification requirements and the reporting of both currency transactions over a designated threshold and suspicious transactions. These controls apply to all banks (commercial, investment, mortgage, and private), insurance and reinsurance companies, savings and loan institutions, financial rental agencies, currency exchange houses, money remitters, money market funds, capitalization companies, frontier foreign currency dealers, casinos, real estate agents, construction companies, car dealerships, hotels and the tourism industry, travel agents, and dealers in precious metals and stones. These entities are required to file suspicious and cash transaction reports with Venezuela's financial intelligence unit (FIU), the Unidad Nacional de Inteligencia Financiera (UNIF. Financial institutions are required to maintain records for a period of five years.

The UNIF was created under the SBIF in July 1997 and began operating in June 1998. Under the original draft of the Organic Law against Organized Crime, the UNIF would have become an autonomous entity with investigative powers, independent of the SBIF, but the relevant clauses were removed just prior to the law's passage. The UNIF has a staff of approximately 55 and has undergone multiple bureaucratic changes, with five different directors presiding over the UNIF since 2004. The SBIF and the UNIF have little credibility within the financial sector, with credible reports indicating that both are used by the government to investigate political opponents.

The UNIF receives suspicious transaction reports (STRs) and reports of currency transactions (CTRs) exceeding approximately $2,100 from institutions regulated by the SBIF, the Office of the Insurance Examiner, the National Securities and Exchange Commission, the Bureau of Registration and Notaries, the Central Bank of Venezuela, and the Bank Deposits and Protection Guarantee Fund, as well as the other entities now included under the Organic Law against Organized Crime. The Venezuelan Association of Currency Exchange Houses (AVCC), which counts all but one of the country's money exchange companies among its membership, voluntarily complies with the same reporting standards as those required of banks. Some institutions regulated by the SBIF, such as tax collection entities and public service payroll agencies, are exempt from the reporting requirement. The SBIF also allows certain customers of financial institutions-those who demonstrate "habitual behavior" in the types and amounts of transactions they conduct-to be excluded from currency transaction reports filed with the UNIF. SBIF Circular 3759 of 2003 requires financial institutions that fall under the supervision of the SBIF to report suspicious activities related to terrorist financing; however, terrorist financing is not a crime in Venezuela.

In addition to STRs and CTRs, the UNIF also receives reports on the domestic transfer of foreign currency exceeding $10,000, the sale and purchase of foreign currency exceeding $10,000, and summaries of cash transactions that exceed approximately $2,100. The UNIF does not, however, receive reports on the transportation of currency or monetary instruments into or out of Venezuela. A system has been developed for electronic receipt of CTRs, but STRs must be filed in paper format.

Obligated entities are forbidden to reveal reports filed with the UNIF or suspend accounts during an investigation without official approval, and are also subject to sanctions for failure to file reports with the UNIF.

The UNIF analyzes STRs and other reports, and refers those deemed appropriate for further investigation to the Public Ministry (the Office of the Attorney General). According to the UNIF, it forwards approximately 30 percent of the STRs it receives to the Attorney General's Office. The Attorney General's office subsequently opens and oversees the criminal investigation. The Venezuelan constitution guarantees the right to bank privacy and confidentiality, but in cases under investigation by the UNIF, the SBIF, the Attorney General's office, a judge can waive these rights, making Venezuela one of least restrictive countries in Latin America from an investigatory standpoint.

Prior to the passage of the 2005 Organic Law against Organized Crime, there was no special prosecutorial unit for the prosecution of money laundering cases under the Attorney General's office, which is the only entity legally capable of initiating money laundering investigations. As a result of the limited resources and expertise of the drug prosecutors who previously handled money laundering investigations, there have only been three money laundering convictions in Venezuela since 1993, and all of them were narcotics-related. Under the Organic Law against Organized Crime, a new unit is supposed to be established, the General Commission against Organized Crime, with specialized technical expertise in the analysis and investigation of money laundering and other financial crimes. This commission has not been established to date. The Organic Law against Organized Crime also expanded Venezuela's mechanisms for freezing assets tied to illicit activities. A prosecutor may now solicit judicial permission to freeze or block accounts in the investigation of any crime included under the law. However, to date there have been no significant seizures of assets or successful money laundering prosecutions as a result of the law's passage.

The 2005 Organic Law against Organized Crime counts terrorism as a crime against public order and defines some terrorist activities. The law also establishes punishments for terrorism of up to 20 years in prison. However, the Organic Law against Organized Crime does not establish terrorist financing as a separate crime, nor does it provide adequate mechanisms for freezing terrorist assets.

The UNIF has been a member of the Egmont Group since 1999 and has signed bilateral information exchange agreements with counterparts worldwide. Venezuela participates in the Organization of American States Inter-American Commission on Drug Abuse Control (OAS/CICAD) Money Laundering Experts Working Group and is a member of the Caribbean Financial Action Task Force (CFATF). The GOV is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the OAS Inter-American Convention Against Terrorism, and has signed, but not yet ratified, the UN Convention against Corruption. The GOV continues to share money laundering information with U.S. law enforcement authorities under the 1990 Agreement Regarding Cooperation in the Prevention and Control of Money Laundering Arising from Illicit Trafficking in Narcotics Drugs and Psychotropic Substances, which entered into force on January 1, 1991. Venezuela also has a Mutual Legal Assistance Treaty (MLAT) with the United States, which entered into force in March 2004.

The Government of Venezuela took several steps to expand its anti-money laundering regime in 2006 with the implementation of the 2005 Organic Law against Organized Crime. The enactment of this bill has provided law enforcement and judicial authorities the much-needed tools for the effective investigation and prosecution of money laundering derived from all serious crimes, broadened asset forfeiture and sharing provisions, strengthened due diligence requirements, strengthened the capabilities of the Public Ministry to successfully investigate and prosecute crimes related to money laundering, and expanded the mandate of UNIF. However, the deletion of those portions of the proposed law that would have made the UNIF autonomous undercut the credibility and effectiveness

of the unit. Venezuela should also create and enact legislation to criminalize the financing of terrorism, as well as institute measures to expedite the freezing of terrorist assets. Although the passage of the Organic Law against Organized Crime indicates an increased willingness to strengthen the GOV's abilities to fight money laundering, legislation criminalizing the financing of terrorism and allowing for the freezing of terrorist assets is necessary to bring Venezuela into compliance with international standards for combating financial crimes. However, without the political will to implement its anti-money laundering regime, "paper" enhancements to its regime will be ineffective.

## Vietnam

Vietnam is not an important regional financial center. Vietnam remains a largely cash-based economy and both U.S. dollars and gold are widely used as a store of value and means of exchange. Real estate prices are commonly quited in gold. Remittances are a large source of foreign exchange, exceeding annual disbursements of development assistance and rivaling foreign direct investment in size. Remittances from the proceeds of narcotics in Canada and the United States are also a source of money laundering as are proceeds attributed to Vietnam's role as a transit country for narcotics.

The Vietnamese banking sector is in the opening phase a transition from a state-owned to a partially privatized industry. At present, approximately 80 percent of the assets of the banking system are held by state-owned commercial banks which allocate much of the available credit to state-owned enterprises. Almost all trade and investment receipts and expenditures are processed by the banking system, but neither trade nor investment transactions are monitored effectively. As a result, the banking system could be used for money laundering either through over or under invoicing exports or imports or through phony investment transactions. Official inward remittances in the first six months of 2006 were estimated to be approximately $2 billion. These amounts are generally transmitted by wire services and while officially recorded, there is no reliable information on either the source or the recipients of these funds. Financial industry experts believe that actual remittances may be double the official figures. There is evidence that large amounts of cash are hand carried into Vietnam, which is legal as long as the funds are declared. The GVN does not require any explanation of the source or intended use of funds brought into the country in this way.

The U.S. Drug Enforcement Agency (DEA) is engaged in a number of investigations targeting significant ecstasy and marijuana trafficking organizations, composed primarily of Vietnamese legal permanent residents in the United States and Vietnamese landed immigrants in Canada as well as naturalized U.S. and Canadian citizens. These drug trafficking networks are capable of laundering tens of millions of dollars per month back to Vietnam, exploiting U.S. financial institutions to wire or transfer money to Vietnamese bank and remittance accounts, as well as engaging in the smuggling of bulk amounts of U.S. currency and gold into Vietnam. The drug investigations have also identified multiple United States-based money remittances businesses that have remitted over $100 million annually to Vietnam. It is suspected that the vast amount of that money is derived from criminal activity. Law enforcement agencies in Australia and the United Kingdom have also tracked large transfers of drug profits back to Vietnam.

Article 251 of the Amended Penal Code criminalizes money laundering. The Counter-Narcotics Law, which took effect June 1, 2001, makes two narrow references to money laundering in relation to drug offenses: it prohibits the "legalizing" (i.e., laundering) of monies and/or property acquired by committing drug offenses (article 3.5); and, it gives the Ministry of Public Security's specialized counter narcotics agency the authority to require disclosure of financial and banking records when there is a suspected violation of the law. The Penal Code governs money laundering related offenses.

In June 2005, GVN issued Decree 74/2005/ND-CP on Prevention and Combating of Money Laundering. The Decree covers acts committed by individuals or organizations to legitimize money or property acquired from criminal activities. The Decree applies to banks and nonbanking financial

institutions. The State Bank of Vietnam (SBV) and the Ministry of Public Security (MPS) take primary responsibility for preventing and combating money laundering. The decree does not cover counterterrorist finance.

SBV supervises and examines financial institutions for compliance with anti-money laundering/counter terrorist financing regulations. Financial institutions are responsible for knowing and recording the identity of their customers. They are required to report cash transactions conducted in one day with aggregate value of VND 200 million (approximately $13,000) or more, or equivalent amount in foreign currency or gold. The threshold for savings transactions is VND 500 million (approximately $31,000). Furthermore, financial institutions are required to report all suspicious transactions. Banks are also required to maintain records for seven years or more. Banks are responsible for keeping information on their customers' secret, but they are required to provide necessary information to law enforcement agencies for investigation purposes.

Foreign currency (including notes, coins and traveler's checks) in excess of $7,000 and gold of more than 300 grams must be declared at customs upon arrival and departure. There is no limitation on either the export or import of U.S. dollars or other foreign currency provided that all currency in excess of $7,000 (or its equivalent in other foreign currencies) is declared upon arrival and departure, and supported by appropriate documentation. If excess cash is not declared, it is confiscated at the port of entry/exit and the passenger may be fined.

The 2005 Decree on Prevention and Combating of Money Laundering provides for provisional measures to be applied to prevent and combat money laundering. Those measures include 1) suspending transactions; 2) blocking accounts; 3) sealing or seizing property; 4) seizing violators of the law; and, 5) taking other preventive measures allowed under the law.

The 2005 Decree also provides for the establishment of an Anti-Money Laundering Information Center under the State Bank of Vietnam (SBV). Similar to a Financial Intelligence Unit (FIU), the Center will function as the sole body to receive and process information. It will have the right to request concerned agencies to provide information and records for suspected transactions. This center was formally established and began operations since February 2006. The Director of the center is appointed by the Governor of the SBV and reports directly to the Governor on anti-money laundering issues. SBV acts as the sole agency responsible for negotiating, concluding and implementing international treaties and agreements on exchange of information on transactions related to money laundering.

The Anti-Money Laundering Information Center will have a separate office with equipment and computers funded by a loan from French Development Assistance. The Center has five full time staff members. Since the Center became operational, it has not detected any suspicious activity.

The MPS is responsible for investigating money laundering related offences. There is no information on investigations, arrests, and prosecutions for money laundering or terrorist financing. MPS is responsible for negotiating and concluding international treaties on judicial assistance, cooperation and extradition in the prevention and combat of money laundering related offenses.

Vietnam is a party to the 1999 International Convention for the Suppression of the Financing of Terrorism. Reportedly, Vietnam plans to draft separate legislation governing counter terrorist financing, though it will not set a specific time frame for this drafting. Currently SBV circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list. No related assets have been identified.

Vietnam is a party to the 1988 UN Drug Convention. Under existing Vietnamese legislation, there are provisions for seizing assets linked to drug trafficking. In the course of its drug investigations, MPS has seized vehicles, property and cash, though the seizures are usually directly linked to drug crimes.

Final confiscation requires a court finding. Reportedly, MPS can notify a bank that an account is "seized" and that is sufficient to have the account frozen.

Vietnam has signed but not ratified the UN Convention against Corruption and is ranked 111 out of 163 countries in Transparency International's 2006 Corruption Perception Index. The Government of Vietnam should promulgate all necessary regulations to fully implement the 2005 decree on the Prevention and Combating of Money Laundering. Vietnam should also pass legislation governing the prevention and suppression of terrorism financing. Vietnam should ratify the UN Conventions against Transnational Organized Crime and Corruption. Vietnamese law enforcement authorities should investigate money laundering, trade fraud, alternative remittance systems, and other financial crimes in Vietnam's shadow economy. Vietnam should become a member of the Asia/Pacific Group on Money Laundering and take additional steps to establish an anti-money laundering/counterterrorist financing regime that comports with international standards.

## Yemen

The Yemeni financial system is not yet well developed and the extent of money laundering is not known. Although financial institutions are technically subject to limited monitoring by the Central Bank of Yemen (CBY), alternative remittance systems, such as hawala, in practice, are not subject to scrutiny and are vulnerable to money laundering. The banking sector is relatively small with 17 commercial banks, including four Islamic banks. The CBY supervises the banks. Local banks account for approximately 62 percent of the total banking activities, while foreign banks cover the other 38 percent.

Yemen's parliament passed a comprehensive anti-money laundering legislation (Law 35) in April 2003. The legislation criminalizes money laundering for a wide range of crimes, including narcotics offenses, kidnapping, embezzlement, bribery, fraud, tax evasion, illegal arms trading, and monetary theft, and imposes penalties of three to five years of imprisonment. Yemen has no specific legislation relating to terrorist financing, although terrorism is covered in various pieces of legislation that treat terrorism and terrorist financing as serious crimes.

Law 35 requires banks, financial institutions, and precious commodity dealers to verify the identity of individuals and entities that open accounts (or in the case of the dealers for those who execute a commercial transaction), to keep records of transactions for up to ten years, and to report suspicious transactions. In addition, the law requires that reports be submitted to the Anti-Money Laundering Information Unit (AMLIU), an information-gathering unit within the CBY. This unit acts as the financial intelligence unit (FIU), which in turn reports to the Anti-Money Laundering Committee (AMLC) within the CBY.

The AMLIU is understaffed with a total of three employees at the main office. The 18 field inspectors for banking supervision also serve as investigators for the AMLIU. The AMLIU has no database and is not networked internally or to the rest of the CBY. The CBY provides training to other members of the government to assist in elements of anti-money laundering enforcement, but the lack of capacity hampers any attempts by the AMLIU to control illicit activity in the formal financial sector.

The AMLC is composed of representatives from the Ministries of Finance, Foreign Affairs, Justice, Interior, and Industry and Trade, the Central Accounting Office, the General Union of Chambers of Commerce and Industry, the CBY, and the Association of Banks. The AMLC is authorized to issue regulations and guidelines and provide training workshops related to combating money laundering efforts.

Law 35 also grants the AMLC the right to exchange information with foreign entities that have a signed a letter of understanding with Yemen. The head of the AMLC is empowered by law to ask local judicial authorities to enforce foreign court verdicts based on reciprocity. Also, the law permits

the extradition of non-Yemeni criminals in accordance with international treaties or bilateral agreements.

Prior to passage of the anti-money laundering law, the CBY issued Circular 22008 in April 2002, instructing banks and financial institutions that they must verify the legality of all proceeds deposited in or passing through the Yemeni banking system. The circular stipulates that financial institutions must positively identify the place of residence of all persons and businesses that establish relationships with them. The circular also requires that banks verify the identity of persons or entities that wish to transfer more than $10,000, when they have no accounts at the banks in question. The same provision applies to beneficiaries of such transfers. The circular also prohibits the transfer of more than $10,000 cash in or out of the country without prior permission from the CBY, although this requirement is not strictly enforced. Banks must also take every precaution when transactions appear suspicious, and report such activities to the AMLIU. The circular has been distributed to the banks along with a copy of the Basel Committee's "Customer Due Diligence for Banks," concerning "know your customer" procedures and "Core Principles for Effective Banking Supervision". The CBY issued Circular No. 4 on December 9, 2003, ordering banks to set up intelligence gathering units specializing in investigating and monitoring suspicious funds and transactions in their regulatory structures. In 2006, however, no reports of suspicious type activity were filed with the AMLIU, and there were no prosecutions.

In September 2003, the CBY responded to the UNSCR 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, and Yemen's Council of Ministers' directives, by issuing two circulars (75304 and 75305) to all banks operating in Yemen. Circulars 75304 and 75305 directed banks to freeze the accounts of 144 persons, companies, and organizations, and to report any findings to the CBY. As a result, one account was immediately frozen. Circular No. 75304 also contained a consolidated list of all persons and entities belonging to al-Qaida (182) and the Taliban (153). In 2006, the CBY began issuing a circular every three months containing an updated list of persons and entities belonging to al-Qaida and the Taliban. Since the February 2004 addition of Sheikh Abdul Majid Zindani to the UNSCR 1267 Sanctions Committee's consolidated list, the Yemeni government has made no known attempt to enforce the sanctions and freeze his assets.

A law was passed in 2001 governing charitable organizations. This law entrusts the Ministry of Labor and Social Affairs with overseeing their activities. The law also imposes penalties of fines and/or imprisonment on any society or its members convicted of carrying out activities or spending funds for other than the stated purpose for which the society in question was established. The CBY Circular No. 33989 of June 2002, and Circular No. 91737 of November 2004, ordered banks to abide by the enhanced controls regulating the opening and management of the accounts of charities. This was in addition to keeping these accounts under continuous supervision in coordination with the Ministry of Labor and Social Affairs.

During 2006, the CBY has been active in educating the public and the financial sector, including money services businesses and money laundering reporting officers, about the proper ways and means of detecting and reporting suspicious financial transactions. They have done so through public forums and workshops. In 2005, the AMLC distributed an anti-money laundering procedural directory to all public and private financial institutions. The directory explains how to monitor and report suspected money laundering cases.

Yemen is one of the original signatories of the memorandum of understanding governing the establishment of the Middle East and North Africa Financial Action Task Force (MENAFATF). Yemen is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Yemen is a party to the Arab Convention for the Suppression of Terrorism.

Yemen has a large underground economy. The smuggling of trade goods and contraband are profitable. The use of khat is common in Yemen and there have been a number of investigations over the years of khat being smuggled from Yemen and East Africa into the United States and profits laundered and repatriated via hawala networks. Yemen is rated 119 out of 163 countries in Transparency International's 2006 Corruption Perception Index.

The Government of Yemen (GOY) should continue to develop an anti-money laundering regime that adheres to international standards, including the FATF recommendations. In particular, banks and nonbank financial institutions should enhance their capacity to detect suspicious financial transactions and should report such transactions to a strengthened AMLIU for analysis and possible investigation by Yemeni law enforcement. Yemen should examine the prevalence of alternative remittance systems such as hawala and how the hawala networks are used in money laundering and value transfer. Law enforcement and customs authorities should also examine trade-based money laundering and customs fraud. As a next step, Yemen should enact specific legislation with respect to terrorist financing and forfeiture of the assets of those suspected of terrorism. Yemen should ratify the UN Convention against Transnational Organized Crime and should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism. Yemen should enforce the sanctions and freeze the assets of Sheikh Abdul Majid Zindani who was added to the UN 1267 Sanctions Committee Consolidated list in February 2004.

## Zimbabwe

Zimbabwe is not a regional financial center, but as the pace of economic contraction accelerates, it faces a serious, growing problem with official corruption and other risk factors associated with money laundering, such as a flourishing parallel exchange market; widespread evasion of exchange controls by legitimate businesses; and company ownership through nominees. Deficiencies in the Government of Zimbabwe's (GOZ) regulatory and enforcement framework contribute to Zimbabwe's potential as a money laundering destination. These deficiencies include: an increasingly understaffed bank supervisory authority; a lack of trained regulators and lack of investigators to investigate and enforce violations and financial crime; financial institutions determined to bypass the regulatory framework; limited asset seizure authority; a laissez-faire attitude toward compliance with the law on the part of elements of the business community; ready acceptance of the U.S. dollar in transactions and, significant gold exports and illegal gold trading.

In December 2003, the GOZ submitted the "Anti-Money Laundering and Proceeds of Crime Act" to Parliament, which enacted the legislation. This bill criminalized money laundering and implemented a six-year record keeping requirement. In 2004, the GOZ adopted more expansive legislation in the "Bank Use Promotion and Suppression of Money Laundering Act" ("The Act") that extended the anti-money laundering law to all serious offenses. The Act mandated a prison sentence of up to fifteen years for a conviction. It also criminalized terrorist financing and authorized the tracking and seizure of assets. The Act has reportedly raised human rights concerns due to the GOZ's history of selective use of the legal system against its opponents, but its use to date has not been associated with any reported due process abuses or provoked any serious public opposition. The Exchange Control Order, enacted in 1996, obligates banks to require individuals who deposit foreign currency into a foreign currency account to submit a written disclosure of sources of the funds.

The Reserve Bank of Zimbabwe (RBZ) is the lead agency for prosecuting money laundering offenses. In May 2006, the RBZ issued new Anti-Money Laundering Guidelines that outlined and reinforced requirements established in the Act for financial institutions and designated nonfinancial businesses and professions. These binding requirements make provisions regarding politically exposed persons and include the obligation to gather and make available to regulators more personal data on these high-profile clients. Financial institutions must now keep records of accounts and transactions for at least

ten years, and report any suspicious transactions to the financial intelligence unit (FIU). The Act also criminalizes tipping off. Failure to report suspected money laundering activities carries a possible fine of Z$5 million (approximately $20,000), and violating rules on properly maintaining customer data carries a possible fine of Z$1 million (approximately $4,000).

The 2004 Act provides for the establishment of an FIU. The Financial Intelligence Inspectorate and Evaluation Unit (FIIE) is housed within the RBZ. The FIIE receives suspicious transaction reports (STRs), issues guidelines such as those issued in May 2006, and enforces compliance with procedures and reporting standards for obligated entities.

According to the Governor of the RBZ, the GOZ has been working throughout 2006 on legislation to address problems with cybersecurity and cybercrime, including money laundering via electronic means. However, the legislation has not been passed. During the year, the RBZ sharpened limits on daily cash withdrawals for individuals and companies, ostensibly in an effort to curtail money laundering but more likely to inhibit private sector parallel foreign exchange activities. In November, the Zimbabwe dollar was trading on the parallel market at a historic premium of about 700 percent above the official exchange rate. The central bank began monitoring all payments by financial institutions of more than Z$1 million (approximately $4,000 at the official exchange rate). When requested, the local banking community has cooperated with the GOZ in the enforcement of asset tracking laws. However, increasingly burdensome GOZ regulations and the resulting hostile business climate have led to growing circumvention of the law by otherwise legitimate businesses.

The GOZ continued to arrest prominent Zimbabweans for activities that it calls “financial crimes.” Prosecutions for such crimes, however, have reportedly been selective and politically motivated. The government often targets persons who have either fallen out of favor with the ruling party, or individuals without high-level political backing. To date, the Act has not been employed in the prosecution of individuals for such offenses. The GOZ prefers to prosecute financial crimes under the Criminal Procedures and Evidence Act, rather than the Anti-Money Laundering Act, because it allows for those charged to be held in custody for up to 28 days. During the year, the authorities made two high-profile arrests of persons (both Nigerian nationals) attempting to smuggle significant sums of foreign currency out of the country.

Most of these crimes involved violations of currency restrictions that criminalize the externalization of foreign exchange. In light of the inability of the vast majority of businesses to access foreign exchange from the RBZ, most companies privately admit to externalizing their foreign exchange earnings or to accessing foreign currency on the parallel market. Moreover, the GOZ itself, through the RBZ, has been a major purchaser of foreign currency on the parallel market. Citing “nonperformance and defiant behavior by most players” in the money transfer sector, in October the RBZ canceled the licenses of all money transfer agencies (MTAs). The MTAs reportedly were exchanging foreign currency at the parallel market rate. Many observers speculated this move would fuel an even greater use of already popular alternative remittance systems.

In August, the GOZ implemented a currency re-denomination program that slashed three zeros from Zimbabwe’s currency (so that Z$100,000 became Z$100). The purpose of the campaign was to assert greater GOZ control over the financial sector and to attempt to reassure a public concerned about the 1200 percent inflation within their country. The RBZ gave all holders of the old currency 21 working days to deposit their cash holdings into the banking system, and set limits for cash deposits either without proof of the source of funds, or without depositors being interrogated on the origins of their money. Although the campaign had nothing to do with cracking down on money laundering, when the holder of cash could not prove a legitimate source of funds, the cash was deposited into zero-interest “anti-money laundering coupons,” and the case was referred to the RBZ’s Suppression of Money Laundering Unit for further investigation. To evade these requirements, those with an excess of cash, such as entrepreneurs, have purchased high-value commodities to retain their wealth. During the

changeover period, there were numerous reports of police arbitrarily seizing cash without issuing receipts or filing official documentation with the authorities. The government claimed that more than 2,000 persons were arrested for "money laundering" in this period and charged under the Exchange Control Act. The government has not provided any additional information about the status or resolution of any of these cases.

The 2001 Serious Offenses (Confiscation of Profits) Act establishes a protocol for asset forfeiture. The Attorney-General may request confiscation of illicit assets. The Attorney-General must apply to the court that has rendered the conviction within six months of the conviction date. The court can then issue a forfeiture order against any property. Despite the early date of this law compared to the money laundering legislation that followed, this law does define and incorporate money laundering among the bases for the GOZ to confiscate assets.

With the country in economic collapse and increasingly isolated, Zimbabwe's laws and regulations remained ineffective in combating money laundering. The May 2006 guidelines notwithstanding, the government's anti-money laundering efforts throughout the year appeared to be directed more at securing the government's own access to foreign currency than to ensuring compliance. Despite having the legal framework in place to combat money laundering, the sharp contraction of the economy, growing vulnerability of the population, and decline of judicial independence raise concerns about the capacity and integrity of Zimbabwean law enforcement. The banking community and the RBZ have cooperated with the United States in global efforts to identify individuals and organizations associated with terrorist financing.

Zimbabwe is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime or the African Union Anti-Corruption Convention. Zimbabwe has yet to sign the UN International Convention for the Suppression of the Financing of Terrorism. Zimbabwe joined the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) in 2003 and in August 2006, assumed the Presidency for ESAAMLG for the 2006/2007 administrative year.

Transparency International ranks the Government of Zimbabwe at 130 of 163 countries on its Corruption Perception Index. The GOZ leadership should work to develop and maintain transparency, prevent corruption, and to subscribe to practices ensuring the rule of law. The GOZ must also work toward reducing the rate of inflation, halting the financial collapse, and rebuilding the economy to restore confidence in the currency. The GOZ can illustrate its seriousness in combating money laundering and terrorism financing by using its legislation for the purposes for which it was designed, instead of using it to persecute opponents of the regime and nongovernmental organizations with which it opposes. Once these basic prerequisites are met, the GOZ should endeavor to develop and implement an anti-money laundering/counterterrorist regime that comports with international standards.