

MONEY LAUNDERING AND FINANCIAL CRIMES

The Money Laundering and Financial Crimes section of the International Narcotics Control Strategy Report is based upon the contributions of many U.S. Government agencies. The Financial Crimes Enforcement Network (FinCEN) of the Department of the Treasury, as a member of the international Egmont Group of Financial Intelligence Units, has a unique strategic and tactical perspective on international anti-money laundering developments. It is the primary contributor to the majority of the country write-ups and the SAR analyses in this section. Other agencies that have helped produce this section include (from the Department of Treasury) the U.S. Customs Service, the Internal Revenue Service, the Office of the Comptroller of the Currency, the Office of Technical Assistance, the Office of Foreign Asset Control, and the Secret Service; (from the Department of Justice) the Drug Enforcement Administration, the Federal Bureau of Investigation; the Criminal Division's Asset Forfeiture and Money Laundering Section, the Counterterrorism Section, and the Overseas Prosecutorial Development Assistance and Training Office. The Federal Deposit Insurance Corporation and the Federal Reserve Board also contributed to this section.

Introduction

Today the world is a riskier place for criminals to launder their ill-gotten gains and for terrorists to finance their operations than it was a year ago. This progress is largely the result of intensified international efforts to combat terrorist financing that followed the September 11 attacks. While money laundering and terrorist financing are not identical phenomena, the legal, regulatory and enforcement tool kit necessary to combat both are virtually the same. Yet, even without the response to the terrorist attacks, international anti-money laundering efforts were reaching a new level in 2002. The international community, seeking to respond immediately to September 11, was fortunate to have an excellent model and foundation in the form of well-established anti-money laundering standards and procedures developed over the previous twelve years by the multi-lateral Financial Action Task Force on Money Laundering (FATF), the flagship of international anti-money laundering/anti-terrorist financing efforts; the global network of FATF-styled regional bodies; and unilateral actions taken by committed countries in accordance with these norms and standards. The 31-member FATF, through its four-year old Non-Cooperative Countries and Territories (NCCT) process, directed for the first time that “counter-measures” be applied to long-identified NCCTs of Nauru and Ukraine. These counter-measures were applied to countries and territories that persisted in their failure to pass adequate anti-money laundering legislation as the necessary first step toward building and implementing a comprehensive and effective anti-money laundering regime. The exercise has had an impact, as country after country either subject to, or faced with the prospect of, counter-measures began passing the legislation necessary to avoid counter-measures and taking, in many cases, the additional steps to be removed from the NCCT list. Nigeria avoided countermeasures by passing legislation that remedied some of the deficiencies that FATF had identified. The imposition of countermeasures against the Ukraine in December 2002 had an immediate effect. In early 2003, Ukraine passed necessary amendments to its anti-money laundering legislation and FATF, at its February, 2003 Plenary called for removal of countermeasures.

Some notable 2002 accomplishments achieved through the FATF NCCT process include the following: Dominica, Hungary, Israel, Lebanon, the Marshall Islands, Niue, Russia and St. Kitts & Nevis made sufficient progress in remedying the deficiencies in their anti-money laundering regimes that they were removed from the NCCT list. Other NCCTs, notably St. Vincent and the Grenadines and Grenada, enacted significant new legislation or implementing regulations in 2002. At its February 2003 Plenary, FATF removed Grenada from the NCCT list.

While the NCCT process focused on money laundering and not terrorist financing per se, FATF, the United Nations (UN), and other international entities lost little time in 2002 moving to ensure that the international community incorporated anti-terrorist financing into its anti-money laundering regimes. FATF and the UN Counter-terrorism Committee (CTC) led the way by requesting, collecting and analyzing reports and self-assessments from nearly every jurisdiction about its ability to address terrorist financing. Against the backdrop of all of these efforts, and with the United States in the lead as the year closed, the international donor community was beginning to accelerate its efforts to provide anti-money laundering/anti-terrorist financing technical assistance to committed countries most vulnerable to terrorist financing. Much remains to be done, however, and it will require a sustained and increasingly broadened effort to accomplish the international anti-money laundering/anti-terrorist financing objectives that still lie ahead.

The United States’ international efforts to combat terrorist financing rely on a mix of multilateral and bilateral initiatives. Our strategy includes the following central elements:

- Establishing a clear set of norms, starting with key UN Security Council Resolutions and relevant international conventions concerning terrorist financing;
- Making the fight against terrorist financing a central element of every relationship the United States has with other countries and institutions;

- Convincing other countries to identify individuals and institutions involved in financing terrorism and to take appropriate action to shut down their activities, including through the freezing of their financial assets;
- Strengthening law enforcement cooperation in matters related to terrorist financing; and
- Providing training to increase the capacity of other countries to close down terrorist financing activities on their own soil, whether these activities occur in financial institutions, non-bank financial institutions, alternative remittance systems or through other means.

Additional diplomatic efforts beyond FATF are also helping to strengthen the international coalition to thwart money laundering and the funding of terrorism. This is playing out in anti-terrorist financing and enhanced anti-money laundering measures by, for instance, the Group of Eight Nations (G-8), the UN, the Asia Pacific Economic Cooperation Forum (APEC), the Organization of American States (OAS), the European Union (EU), the Organization for Security and Co-Operation in Europe (OSCE), and other multilateral and regional organizations. They have variously sponsored conferences, offered technical assistance, crafted recommendations, or adopted conventions and other instruments designed to strengthen measures and enhance cooperation. Some milestones marking this success include the following:

- The Department of the Treasury noted that the United States and 30 other nations have blocked an estimated \$125 million of terrorists' assets to date.
- As of December 31, 2002, 64 countries, including the United States, had ratified the UN International Convention for the Suppression of the Financing of Terrorism; another 75 countries had signed but not ratified the Convention. Among other provisions, this Convention obligates parties to criminalize the provision or collection of funds with the intent that they be used, or in the knowledge that they are to be used, to conduct terrorist activity.
- By year's end, 181 of the UN's 191 Member States had provided the CTC with self-assessment reports on their anti-terrorism capabilities, including their ability to combat terrorist financing, in response to requirements in UN Security Council Resolution 1373, adopted on September 28, 2001.
- On June 3, 2002, the United States, along with 29 other countries, signed the Inter-American Convention against Terrorism, which the OAS General Assembly adopted on that day. Three other countries signed the Convention before December 31, 2002, including Canada, which became the first state to ratify it. The Convention includes a provision requiring parties, to the extent they have not already done so, to "institute a legal and regulatory regime to prevent, combat, and eradicate the financing of terrorism and for effective international cooperation thereto . . ." Nearly all major regional political organizations have issued statements denouncing terrorism and have begun the process of implementing work plans designed to enable member states to eradicate terrorist financing.
- Both the International Monetary Fund and the World Bank agreed to include assessments of compliance with relevant FATF Forty Recommendations on Money Laundering and the Special Recommendations on Terrorist Financing in their Financial Sector Assessment Programs to assist in the monitoring of the progress of countries' adherence to international standards.

The United States is relying on this strong foundation of norms and international commitments to implement its most robust anti-money laundering foreign assistance program to date, focused sharply on

Money Laundering and Financial Crimes

terrorist financing. Shortly after September 11, 2001, the Department of State convened an interagency group to identify those countries most vulnerable to terrorist financing and to devise a strategy to provide them with the necessary training and technical assistance to create comprehensive, effective anti-money laundering/anti-terrorist financing regimes. Throughout 2002, State Department-led Financial Systems Assessment Teams (FSATs) of U.S. experts conducted detailed assessments of the legal, regulatory and law enforcement capabilities and vulnerabilities of the most affected countries. By the end of the year, a majority of these countries had been assessed. Training and technical assistance implementation plans had been developed on virtually all of the assessed countries, and assistance had begun being delivered according to these plans. This program remains a high priority in 2003 and will be pursued until comprehensive anti-money laundering regimes are established in all of the priority countries.

The United States, however, does not have enough experts or funds to meet all of the anti-money laundering institution-building requirements worldwide. That is why we have had to prioritize and why we have made “burden-sharing” a key element in our discussions with other donor countries and organizations. International financial institutions and America’s friends and allies are increasingly agreeing to provide technical assistance to needy countries. Indonesia—a FATF NCCT—is a unique but illustrative example. Even before the October 2002 terrorist attack in Bali, donors had been providing assistance to the government. This included a joint Australian-U.S. program to draft anti-money laundering legislation; Australian training for police investigators; a \$1.5 million grant by Japan to the Asian Development Bank to develop a comprehensive assistance plan; and consultations with Indonesia’s Central Bank and private sector financial institutions by a U.S. non-profit organization of senior bankers. These and other post-Bali generous proposals by our partners, for the development of specific aspects of an anti-money laundering regime, underscore the need to coordinate training and technical assistance so that costly programs are complementary, not duplicative, and so all assistance needs are met. The World Bank is one of several organizations grappling with this challenge. It has created a secure database, accessible to all potential donors, in which FATF-styled regional bodies may enter requests for assistance by their member countries.

The United States also began making greater use of its domestic legislation to combat the international money laundering threat. For instance, significant provisions in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) have been used to counter-terrorist financing threats.

In other noteworthy cases, two U.S. financial institutions were penalized for failing to file Suspicious Activity Reports (SARs). Banks in the United States have been required to file SARs since April 1, 1996, but no monetary penalties had been imposed for failing to comply with these regulations until last year. In September 2002, the Financial Crimes Enforcement Network (FinCEN) imposed a \$100,000 civil penalty against Great Eastern Bank of Florida for failing to file SARs for transactions that involved the structuring of cash deposits to avoid currency reporting requirements, and other similar transactions indicative of money laundering activity. In November 2002, Broadway National Bank in New York City pled guilty to three criminal charges for failing to file SARs, failing to have an adequate anti-money laundering program, and allowing the illegal structuring of currency transactions, and paid a fine of \$4 million. These penalties mark the beginning of a new chapter in the enforcement of laws and regulations involving SARs and anti-money laundering programs.

Global efforts against money laundering and the financing and support of terrorism are necessary to achieve successful deterrence of these activities. The United States is actively engaged in this process through its diplomatic efforts and through its assessment, technical assistance and training programs to support governments committed to developing comprehensive anti-money laundering/anti-terrorist financing regimes. The past year saw substantial progress in many nations. With the impetus of international cooperation and assistance, countries will continue to make their financial systems more resistant to money laundering and terrorist financing. Those jurisdictions that fail to meet international standards will be identified and isolated.

Money Laundering and Terrorist Financing—A Global Threat

International recognition and action against the threat posed by money laundering have increased over the last decade. Money laundering produces several deleterious economic, social and political effects. Money laundering undermines free enterprise by crowding out the private sector; threatens the financial stability of countries and the international free flow of capital; and poses international and national security threats through corruption of officials and legal systems. Indeed, the revenue produced by some narcotics-trafficking organizations can far exceed the funding available to the law enforcement and security services of some emerging market countries.

Since the events of September 11, 2001, there has also been a new recognition of the threat posed by money laundering's closely related corollary, terrorist financing. The amount of damage in loss of life and economic after-effects from a relatively small amount of operational funding can be staggering. While terrorist financing shares most of the fundamental attributes of money laundering, (e.g. fundraising, funds transfers, and obfuscation of origin and beneficial owner of funds), and while the legal and regulatory regimes needed to control both are essentially the same, terrorist financing does exhibit some significant differences.

Money Laundering and Terrorist Financing: Differences and Similarities

With the exception of crimes of passion, most crime is committed for financial gain. The primary motivation for terrorism, however, is not financial. While traditional narcotics-traffickers and organized crime groups primarily seek monetary gain, terrorist groups usually seek non-financial goals, such as publicity for their cause and political influence. Terrorist financing also differs from traditional forms of money laundering in other respects. Ordinarily, criminal activity produces funds and other proceeds that money launderers disguise so that the funds can be used for legitimate or criminal purposes. Funds that support terrorist activity may come from illicit activity but are also generated through legitimate means such as fundraising through legal non-profit entities. In fact, a significant portion of terrorists' funding comes from contributors, some who know the intended purpose of their contributions and some who do not. Terrorist financing therefore contrasts with the financing of, for example, a narcotics-trafficking network, which obtains virtually all of its funding from illegal activities.

Operationally, the problems of criminal money launderers and terrorist financiers differ. Traditional money launderers must take large cash deposits and enter them into the financial system without detection. Terrorist financiers need to place substantially fewer funds into the hands of terrorist cells and their members because terrorist operations require relatively little money (for example, the attacks on the World Trade Center and the Pentagon are estimated to have cost approximately \$500,000). This is a significantly easier task than seeking to disguise the large amounts of proceeds generated by organized crime and drug kingpins.

Funding Sources

While the terrorist groups require modest funding for their operations and do not pursue financial gain as a primary goal, international terrorist groups need significant amounts of money to organize, recruit new adherents, train and equip them, and otherwise support their activities. In addition to direct costs, some terrorist organizations also need to fund media campaigns, to buy political influence, and to undertake social projects aimed at maintaining membership and attracting sympathetic supporters.

Because of these larger organizational costs, terrorists often rely in part on funds gained from traditional crimes such as robbery, kidnapping for ransom, narcotics-trafficking, extortion, document forgery, currency and merchandise counterfeiting, fraud, and smuggling. In this respect al-Qaida is an anomaly as,

at least initially, it was largely self-financed by Usama Bin Ladin. In most cases, terrorists engage in criminal activity, at least to some extent, and then use some of the proceeds of these criminal activities to finance their terrorism efforts. Indeed, some Foreign Terrorist Organizations (FTOs), such as the United Self Defense Forces of Colombia (AUC) and the Revolutionary Armed Forces of Colombia, (FARC), and Sendero Luminoso in Peru, are so closely linked to the narcotics trade that they are often referred to as “narcoterrorists”.

As is frequently the case with narcotics-related money laundering, terrorist groups also utilize front companies; that is, commercial enterprises that engage in legitimate enterprise, but which are also used to commingle illicit revenues with legitimate profits from the commercial enterprise. Front companies are frequently established in offshore financial centers that provide anonymity to their beneficial owners, thereby insulating the beneficial owners from law enforcement. In addition to commingling the proceeds of crime, terrorist front companies also commingle donations from witting and unwitting sympathizers.

Terrorists tap a wide range of sources for their financial support, including the proceeds of criminal activity, otherwise legitimate commercial enterprises, social and religious organizations and State sponsors of terrorism. (The Secretary of State has designated Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria as states whose governments have repeatedly provided support for acts of international terrorism.)

Transnational organized crime groups have long relied on criminal proceeds to fund and expand their operations, and were pioneers in using corporate structures to commingle funds to disguise their origin. In particular, it is the terrorists’ use of social and religious organizations, and to a lesser extent, state sponsorship, that differentiates their funding sources from those of traditional transnational organized criminal groups.

Money Movements of Criminal and Terrorist Funds

The methods used for moving and laundering money for general criminal purposes are nearly identical to those used to move money to support terrorist activities. Indeed, in many cases, criminal organizations and terrorists employ the services of the same money professionals (currency exchangers, bankers, accountants and lawyers) to help move their funds.

Both terrorists and criminal groups have used and continue to use established mechanisms in the formal financial sector, such as banks, primarily because of their international linkages. Terrorist and criminal organizations have little trouble determining which countries and jurisdictions have poorly regulated banking systems. Both terrorist organizations and narcotics-trafficking groups have exploited these weaknesses, and their built-in impediments to international cooperation, and have made use of their financial services to originate wire transfers and establish accounts that require minimal or no identification and do not require disclosure of ownership.

In addition to the formal financial sector, terrorists and traffickers alike employ other methods as well. One common method is smuggling cash across borders either in bulk or through the use of couriers. Similarly, both traffickers and terrorists rely on currency or moneychangers. Moneychangers play a major role in transferring funds in Asia, the Americas, the Middle East, and other regions. Their presence is largest in countries where currency or exchange rate controls exist and where cash is the traditionally accepted means of settling commercial accounts. These systems are also commonly used by large numbers of expatriates to remit funds to families abroad. Traffickers and terrorists have become adept at exploiting the weaknesses and lack of supervision of these systems to move their funds.

Both terrorists and traffickers have used informal value transfer systems, such as “hawala” or Hundi, and underground banking; these systems use trusted networks to move funds and settle accounts with little or no paper records. Such systems are prevalent throughout Asia and the Middle East as well as within their expatriate communities in other regions.

Trade-based money laundering is known to be used by organized crime groups and is increasingly suspected of being used by terrorist financiers as well. This method involves the use of commodities, false invoicing, and other trade manipulation to move funds. Examples of this include the Black Market Peso Exchange in the Western Hemisphere, the use of gold in the Middle East and South Asia, and the use of conflict diamonds in Africa.

One method of money movement that seems to be used frequently by some terrorist groups is the misuse of Islamic banks to move funds. Islamic banks operate in keeping with Islamic law, which prohibits the payment of interest and certain other activities. They have proliferated throughout Africa, Asia and the Middle East since the mid-1970s. Terrorists find these to be attractive vehicles because, in some instances, these banks are not subject to a wide range of anti-money laundering regulations and controls normally imposed on secular commercial banks. Islamic banks often do not undergo the regulatory or supervisory scrutiny by bank regulators via periodic bank examinations or inspections. While these banks may voluntarily comply with banking regulations, and in particular, anti-money laundering guidelines, there is often no control mechanism to ensure such compliance or the implementation of updated anti-money laundering policies. In addition, many religious charities naturally gravitate to Islamic banks and use their services, which presents another vulnerability, as terrorists often move funds diverted from religious charities. Islamic banking is not unique to the Middle East, but is increasingly found in many regions. Some of the largest Islamic financial institutions now operate investment houses in Europe and elsewhere.

Like money laundering, terrorist financing represents a potential exploitable vulnerability. In money laundering, transnational organized crime groups deliberately distance themselves from the actual crime and the jurisdiction in which it occurs; for them the loss of drugs or products is merely seen as the cost of doing business, but they are never far away from the eventual revenue stream. In terrorist financing the operational funds are very difficult to track, but by adapting methods used to combat money laundering, such as financial analysis and investigations, use of task forces, and administrative blocking procedures, authorities can significantly disrupt the financial networks of terrorists, interdict the potential movement of terrorists' funds and build a paper trail and base of evidence that helps to identify and locate the leaders of the terrorist organizations and cells.

International Cooperation and Capacity Building

Building the capacity of our coalition partners to combat money laundering and terrorist financing through cooperative efforts, and through training and technical assistance programs is critical to our national security. As Deputy Secretary of the Treasury Kenneth Dam stated on June 8, 2002 in an address to the Council on Foreign Relations, "...international cooperation is particularly important because the financial front of the war on terrorism cannot be won without it...you can't bomb a foreign bank account. You need the cooperation of the host government to investigate and freeze that foreign account."

While there are some important differences between money laundering and terrorist financing as noted above, in terms of capacity building through training and technical assistance there is no appreciable difference. The same measures that are required to establish a comprehensive anti-money laundering regime—sound legislation and regulations, suspicious transaction reporting mechanisms, Financial Intelligence Units, on-site supervision of the financial sector, internal controls, trained financial investigators, legal authorization to utilize special investigative techniques, modern asset forfeiture and administrative blocking capability, and the ability to cooperate and share information internationally) that are used to prevent, detect, investigate and prosecute money laundering—are precisely the tools required to identify, interdict and disrupt terrorist financing.

Increasingly, international organizations and regional groups are recognizing this and are adding anti-terrorist financing to their objectives and incorporating appropriate measures into their assessment and assistant programs. With increasing frequency around the world, a new FIU is established, or a new money laundering law enacted, or a regulation passed that disrupts the efforts to launder money and finance terrorism. While significant progress is being made, additional efforts are still necessary to secure

expertise, devote resources to training and technical assistance, prioritize requirements, and then harmonize assistance efforts to continue the headway made thus far against money laundering and terrorist financing.

The United States Response

The USA PATRIOT Act

Money laundering and terrorist financing enforcement efforts are not limited to targeting charitable fronts and fundraising appeals, freezing assets, or obtaining regulatory cooperation from our foreign partners. Money laundering and terrorist financing enforcement plays a critical role by identifying and thwarting terrorist and transnational organized crime groups before they carry out their plans. The cornerstone of these efforts lies in our legislative response to terrorist financing and money laundering embodied in the USA PATRIOT Act. The USA PATRIOT Act was passed in October 2001, and revises key elements of the criminal code and Bank Secrecy Act to provide powerful new tools in the arsenal against terrorist financing and money laundering.

On the criminal side, the USA PATRIOT Act expands criminal offenses relating to terrorism, including offenses related to the support and financing of terrorism; permits more expansive sharing of information between the intelligence and law enforcement communities; and streamlines procedures concerning the use of domestic electronic intercepts of terrorist information that can be, and have been, used against those who provide, attempt to provide and/or conspire to provide material support or resources to terrorists or foreign terrorist organizations.

On the financial side, the USA PATRIOT Act expands the scope of pre-existing forfeiture laws; broadens compliance, reporting and record keeping requirements for certain types of financial institutions; encourages information sharing mechanisms between the government and the private sector; and restricts the ability of shell banks to do business in the United States. The USA PATRIOT Act also amends existing law to make it easier to pursue federal prosecutions of money remitters who fail to comply with state licensing or registration requirements. While the USA PATRIOT Act itself was passed in 2001, it was not until 2002 that many of the implementing regulations were enacted, and the new features of the USA PATRIOT Act began to be successfully employed.

Terrorist Financing and Foreign Terrorist Organizations

By strengthening several sections of the criminal code, provisions in the USA PATRIOT Act make it easier for prosecutors to bring and prove charges of providing material support or resources to terrorists, through financial or other assistance, including through personal services provided by those who voluntarily enroll in terrorist training camps. The U.S. Criminal Code was strengthened by the Act to make it a crime for persons within the United States to provide, conceal or disguise the nature, location, source, or ownership of “material support or resources” used or attempted to be used in the commission of any of the predicate, enumerated terrorist-related crimes.

The USA PATRIOT Act also expanded an existing provision of the U.S. Criminal Code, enacted in 1994, that makes it a crime to provide “material support or resources” to terrorists. The USA PATRIOT Act amendments expand the existing definition of “material support or resources” to make it a crime for anyone subject to U.S. jurisdiction to provide anything of value—including expert advice or assistance—to those involved in terrorist activity. The USA PATRIOT Act amendments also expand the scope of another provision in the U.S. Criminal Code, enacted in 1996, which makes it a crime for anyone, within the United States or subject to the jurisdiction of the United States, knowingly to provide “material support or resources” to a foreign terrorist organization.

In 2002, the United States enacted other important legislation to combat terrorist financing. The Suppression of the Financing of Terrorism Convention Implementation Act of 2002, enacted as title II of Public Law 107-197, implements the requirements of the International Convention for the Suppression of the Financing of Terrorism. Among its provisions, this statute makes it a crime, by any means, directly or indirectly, unlawfully and willfully to provide or collect funds with the intention that such funds be used, or with the knowledge that such funds are to be used to carry out an offense set forth in the Convention, or any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

Strengthening Asset Forfeiture

One of the significant provisions in the USA PATRIOT Act is a stipulation that amends the civil forfeiture statute in the United States to permit the forfeiture of funds held in U.S. correspondent accounts on behalf of foreign banks. Where the government can show that forfeitable property was deposited into an account at a foreign bank, U.S. prosecutors can now file a civil forfeiture action against the equivalent amount of money in that foreign bank's correspondent account in the United States. This new power was used for the first time in 2001 and demonstrates the increasing reach of laws to seize and freeze terrorist funds.

The USA PATRIOT Act also expands the scope of forfeiture laws to permit the forfeiture of any property involved in the commission of a terrorist act. In addition, the Act remedies a technical problem that made it more difficult to prosecute and forfeit unreported cash smuggled in bulk into, or out of, the United States.

Special Measures

The Act also contains several provisions that increase the means available to the United States to advance worldwide initiatives against money laundering and terrorist financing. Prominent among these are the special measures contained in Section 311 of the Act which can be employed to protect the U.S. financial system from abuse by money launderers operating from or through international financial crime havens.

In the past, the United States has had limited choices when it came to protecting itself from such abuse, having on the one hand informational advisories issued to domestic banks about specific jurisdictions, and on the other hand, sanctions authorized by the International Emergency Economic Powers Act that blocked transactions with designated entities in a jurisdiction. Now, under Section 311, the United States has available a graduated set of five special measures that give it much greater flexibility in responding to current and emerging international money laundering and terrorist financing threats: requiring domestic financial institutions to broadly implement enhanced reporting requirements; additional requirements to identify beneficial owners of accounts; requirements for additional due diligence for payable-through accounts; requirements for additional information and record keeping on correspondent accounts; and a prohibition on the opening or maintenance of correspondent accounts for institutions from a named jurisdiction.

The authority of Section 311 of the Act was invoked for the first time in December 2002 when the United States designated Ukraine and the Republic of Nauru as primary money laundering concerns. (Both had already been listed by the Financial Action Task Force (FATF) as a Non-Cooperating Country or Territory (NCCT), and had been singled out by FATF for countermeasures for their lack of progress in strengthening their anti-money laundering regimes.) Designation is the required first step before implementing one or more of the above special measures, and it indicates that the United States is prepared to use this new authority to help counter international money laundering and terrorist financing threats.

Financial Institution Responsibilities

The Act calls for the implementation of new suspicious activity reporting requirements for several categories of non-depository financial institutions, including securities broker/dealers, mutual funds, money service businesses, and currency exchanges. Additionally, such entities are tasked with developing and implementing anti-money laundering compliance programs.

Banks are restricted from doing business directly, or indirectly, with foreign shell banks. Any correspondent account a domestic bank holds for a foreign bank is subject to scrutiny to determine whether the foreign bank has a physical presence in another jurisdiction and to ensure that the foreign bank is not providing United States banking privileges to a shell bank through the use of a U.S. correspondent account. Any accounts found to fall within the shell bank prohibitions must be closed. Banks are also subject to enhanced due diligence requirements when doing business with foreign citizens opening large-dollar private banking accounts.

Finally, the Act makes it easier to prosecute, federally, money remitters who fail to comply with state licensing or registration requirements. Several cases were brought in 2002 to attack the problem of unlicensed money remitters. The first conviction of an unlicensed remitter occurred in November 2002.

The increased scrutiny of those conducting financial transactions through U.S. institutions is designed to limit the vulnerabilities of the U.S. financial sector and to detect money laundering and terrorist financing.

Federal Bureau of Investigation

Terrorist Financing Operations Section

The FBI's Terrorist Financing Operations Section (TFOS), formerly known as the Terrorist Financial Review Group, was formed in response to the critical need for a more comprehensive, centralized approach to investigate the financing of terrorists and terrorism. The mission of TFOS is to provide a coordinated financial investigative component to terrorism investigations and to develop predictive terrorist identification mechanisms to identify terrorists and their networks, and to disrupt and dismantle those networks and their funding mechanisms. The efforts of TFOS were initially focused on conducting and coordinating a comprehensive financial analysis of the 19 hijackers in order to link them together and to identify their financial support structure within the United States and abroad.

Terrorists, their networks and their support structures require funding in some form to exist and operate. Whether the funding and financial support is minimal or substantial, it leaves a financial trail that can be traced, tracked, and exploited for pro-active and reactive purposes. Being able to identify and track financial transactions and links after a terrorist act has occurred or terrorist activity has been identified represents only a small portion of the mission; the key lies in exploiting financial information to identify previously unknown terrorist cells, recognize potential terrorist activity/planning, and predict and prevent potential terrorist acts. The importance of the terrorist financing component of terrorism investigations is readily apparent from the fact that, through financial information, the TFOS and FBI established how the hijackers responsible for the September 11 attacks received their money, where they lived, and details concerning their flight training and associates.

TFOS provides assistance with the financial aspects of terrorism investigations to FBI Field Offices. Depending upon resource needs and expertise, assistance consisting of investigative, analytical, and document handling support, or the conduct of all aspects of the financial investigation, is also provided to Joint Terrorism Task Forces (JTTFs) operating in the FBI Field Offices, and to the 44 FBI Legal Attaché Offices located in foreign countries. TFOS also conducts independent terrorist financing investigations from FBI Headquarters.

TFOS use a relational database to organize, capture and analyze all TFOS financial documents. As information is entered into the database, link analysis and queries can be conducted to identify associations and further expand the scope of an investigation. The ultimate purpose of this process is to help investigators and analysts identify and clarify the activities of individuals, illicit charities, and corrupt financial institutions engaged as facilitators of terrorist funding. TFOS has used the database in connection with financial investigations of over 3,195 individuals and groups. Over 137,500 financial documents encompassing approximately 144,788 financial transactions have been entered into the database for link analysis. As part of its analytical efforts, TFOS also cultivates and maintains a contact database of private industry and government sources, and persons who can provide financial and other data in support of investigations.

TFOS has conducted a comprehensive national and international outreach initiative in an effort to share information regarding terrorist financing methods with the financial community and law enforcement. TFOS support of domestic and international terrorism investigations has led to TFOS-sponsored training programs on terrorism financing both domestically and with over 38 countries worldwide.

U.S. Customs Service: Operation Green Quest

The U.S. Treasury Department established Operation Green Quest in October 2001 as part of America's response to the events of September 11. Operation Green Quest is a multi-agency terrorist financing task force, headed by the U.S. Customs Service, that attempts to bring the full scope of the Treasury's financial expertise to bear upon "...identifying, disrupting, and dismantling the financial infrastructures and sources of terrorist funding."

The Green Quest Task Force includes representatives from the U.S. Customs Service; Internal Revenue Service; Secret Service; Bureau of Alcohol, Tobacco and Firearms; Office of Foreign Assets Control; Financial Crimes Enforcement Network; Federal Bureau of Investigation; Postal Inspection Service; Naval Criminal Investigative Service; and the Department of Justice. Members of the Task Force assist in coordinating U.S. investigations of terrorist financing and prioritizing resources to meet national security objectives.

Operation Green Quest has initiated a proactive, multi-faceted approach to increase communication among the private sector, financial institutions, and Green Quest. Over the years, law enforcement has found that outreach to, and dialog with, the private sector can yield enormous dividends.

Office of Foreign Assets Control

The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions against international narcotics-traffickers, targeted foreign countries, and terrorists and terrorism-sponsoring organizations, based on U.S. foreign policy and national security goals. OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

OFAC's economic sanction programs against narcotics-traffickers began in October 1995 with President's Clinton's signing of Executive Order 12978, imposing sanctions on named narcotics traffickers centered in Colombia. In 1999, the Foreign Narcotics Designation Kingpin Act (Kingpin Act) provided the authority to impose similar sanctions on a global basis. Currently, OFAC's economic sanctions programs involving foreign narcotics traffickers rely principally on the President's broad powers under the International Emergency Economic Powers Act (IEEPA) and the Kingpin Act to prohibit commercial transactions involving specific individuals and entities. The Kingpin Act "de-certifies" foreign drug lords rather than foreign governments and countries. It also is designed to deny significant foreign narcotics

traffickers and their organizations, including related businesses and operatives, access to the U.S. financial system and all trade and transactions involving U.S. companies and individuals.

OFAC implements and administers the IEEPA-based designation of terrorists, terrorist organizations, and terrorist supporters and networks as Specially Designated Global Terrorists (SDGTs) under Executive Order 13224, which President Bush issued on September 23, 2001 as part of the war on terrorist financing. Designation leads to the freezing of their assets and public exposure of their connections with terrorism or terrorist fundraising activities. Under this Executive Order, as amended, the Secretary of State, in consultation with the Secretary of the Treasury, the Attorney General, and the Secretary of Homeland Security, designates foreign persons that have committed, or pose a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy or economy of the United States. Designations of persons who act for or on behalf of, support or sponsor, or are otherwise associated with, terrorists and terrorist organizations are prepared by OFAC's International Programs and Foreign Terrorist Divisions. OFAC's Licensing, Compliance and Blocked Assets Divisions administer the programs and conduct funds interdiction activities, and its Civil Penalties and Enforcement Divisions issue civil penalties and coordinate criminal investigations relating to transactions of the sanctions prohibitions.

The office also administers an umbrella of other asset freeze and trade embargo programs involving terrorists or sponsors of terrorism, including those targeting:

- Terrorist-supporting states designated under 6(j) of the Export Administration Act of 1979, including Cuba (since 1963), Iran (since 1979), Iraq (since 1990), Libya (since 1986), North Korea (since 1950), Sudan (since 1997), and Syria (since 1979);
- Foreign Terrorist Organizations (FTOs) designated under section 219 of the Immigration and Nationality Act, as amended; and,
- Specially Designated Terrorists (SDTs) named under earlier IEEPA-based freeze orders issued in 1995 and 1998 targeting certain Middle East terrorist groups and individuals.

Money Laundering Trends and Typologies

As in previous years, money launderers have demonstrated great creativity in combining traditional money laundering techniques into complex money laundering schemes designed to thwart the ability of authorities to prevent, detect and prosecute money laundering. Below is a review of U.S. money laundering trends in 2002 are examples of the various money laundering/terrorist financing typologies.

Statistical Overview of U.S. Money Laundering Trends in 2002

The U.S. Suspicious Activity Reporting System plays a critical role in U.S. anti-money laundering efforts. Similar types of reporting throughout the world are key to global efforts to combat money laundering. The aggregate totals for U.S. Suspicious Activity Reports (SARs) help illustrate the nature of illegal proceeds and the relative scale of the problem. Depository institutions (i.e., banks, thrifts, savings and loans, and credit unions) have been required to file SARs since 1996. The USA PATRIOT Act extended the mandatory reporting requirements to brokers and dealers in securities, and the Department of the Treasury, pursuant to its rulemaking authority extended it to casinos and money services businesses, including money exchangers, sellers of traveler's checks and money transmitters (MSBs). The requirements went into effect on January 1, 2002 for MSBs, and on January 1, 2003 for brokers and

dealers in securities, and will become effective for casinos in March 2003. The regulations generally require that covered financial institutions file a SAR when they suspect transactions of law or suspicious activities involving amounts greater than between \$2,000 and \$5,000. The following statistics provide aggregate totals for SARs filed by depository institutions since implementation of the system on April 1, 1996 through October 2002. Additionally, a small part of the total volume reflects reports filed by affiliates of depository institutions or, in some cases, filed voluntarily by brokers and dealers in securities who are not affiliated with banks or gaming businesses that, as of October 2002, were not yet required under the Bank Secrecy Act (BSA) to file SARs.

Table 1: SAR Filings by Year and Month

Month	Number of Filings					
	1997	1998	1999	2000	2001	2002
January	6,123	6,832	8,621	13,399	13,767	19,424
February	5,519	7,055	9,949	13,634	14,660	17,881
March	6,850	8,938	11,492	15,154	16,084	25,037
April	7,148	8,057	9,478	11,499	15,357	19,249
May	6,754	7,409	10,400	13,674	16,335	27,313
June	6,696	8,737	10,956	13,963	14,387	16,590
July	7,175	8,757	8,518	12,611	16,823	26,600
August	6,322	8,532	10,484	14,111	19,283	22,433
September	7,561	7,577	8,471	13,321	14,283	24,571
October	7,439	8,165	9,842	13,148	20,571	25,134
November	5,960	7,848	11,243	14,437	20,444	
December	7,604	8,614	11,050	13,769	21,624	
Subtotal	81,151	96,521	120,504	162,720	203,538	224,232
Total Filings	888,666					

Table 2 provides a rank ordering of the underlying suspicious activity identified in the SAR data between April 1997 and October 2002.

Money Laundering and Financial Crimes

**Table 2: Frequency Distribution of SAR Filings by Characterization of Suspicious Activity
April 1, 1997 Through October 31, 2002**

Violation Type	1997	1998	1999	2000	2001	2002
BSA/Structuring/Money Laundering	35,625	47,223	60,983	90,606	108,925	126,971
Bribery/Gratuity	109	92	101	150	201	331
Check Fraud	13,245	13,767	16,232	19,637	26,012	26,170
Check Kiting	4,294	4,032	4,058	6,163	7,350	7,686
Commercial Loan Fraud	960	905	1,080	1,320	1,348	1,571
Computer Intrusion	0	0	0	65	419	1,293
Consumer Loan Fraud	2,048	2,183	2,548	3,432	4,143	3,644
Counterfeit Check	4,226	5,897	7,392	9,033	10,139	10,198
Counterfeit Credit/Debit Card	387	182	351	664	1,100	1,050
Counterfeit Instrument (Other)	294	263	320	474	769	659
Credit Card Fraud	5,075	4,377	4,936	6,275	8,393	12,347
Debit Card Fraud	612	565	721	1,210	1,437	975
Defalcation/Embezzlement	5,284	5,252	5,178	6,117	6,182	5,101
False Statement	2,200	1,970	2,376	3,051	3,232	2,995
Misuse of Position or Self Dealing	1,532	1,640	2,064	2,186	2,325	2,217
Mortgage Loan Fraud	1,720	2,269	2,934	3,515	4,696	4,617
Mysterious Disappearance	1,765	1,855	1,854	2,225	2,179	1,869
Wire Transfer Fraud	509	593	771	972	1,527	3,293
Other	6,675	8,583	8,739	11,148	18,318	25,346
Unknown/Blank	2,317	2,691	6,961	6,971	11,908	6,753

General Money Laundering Trends in 2002

Organized crime and narcotics-traffickers have used the following methods for decades to launder their illegal proceeds:

- Financial activity inconsistent with the stated purpose of the business;
- Financial activity not commensurate with stated occupation;
- Use of multiple accounts at a single bank for no apparent legitimate purpose;
- Importation of high dollar currency and traveler's checks not commensurate with stated occupation;
- Significant and even dollar deposits to personal accounts over a short period;

- Structuring of deposits at multiple bank branches to avoid Bank Secrecy Act requirements;
- Refusal by any party conducting transactions to provide identification;
- Apparent use of personal account for business purposes;
- Abrupt change in account activity;
- Use of multiple personal and business accounts to collect and then funnel funds to a small number of foreign beneficiaries;
- Deposits followed within a short period of time by wire transfers of funds;
- Deposits of a combination of monetary instruments atypical of legitimate business activity (business checks, payroll checks and social security checks); and
- Movement of funds through countries that are on the FATF list of NCCTs.

SARS Related to NCCT Countries

Financial institutions identifying suspicious transactions under the Bank Secrecy Act of 1970, chapter 53 of title 31, United States Code (BSA) are required to report such transactions by filing a SAR with the Financial Crimes Enforcement Network (FinCEN), in accordance with applicable regulations. SARs are not proof of illegal activity; rather they note possible wrongdoing that warrants further investigation. An actual determination of criminal activity can only be made following an investigation by law enforcement of the activity addressed in the SAR.

FinCEN did an analysis of the Suspicious Activity Reporting System to determine the volume of SARs filed that relate to jurisdictions the FATF has placed on the NCCT list since 2000.

The results of that analysis follow. Again, the results represent possible illegal activity; they are not positive determinations that criminal activity has occurred.

An asterisk (*) following the name of a jurisdiction indicates that FATF removed the jurisdiction from the NCCT list prior to December 31, 2002.

Bahamas. * An analysis by FinCEN of the Suspicious Activity Reporting System, for the period January 1, 2002 to October 31, 2002, reveals that there are 227 SARs that could be linked to transactions associated with the Bahamas. These SARs were filed by 50 U.S. banks, 11 foreign banks, 15 brokerage services firms, and one money service business with reported amounts ranging from a low of zero dollars to a high of \$81,000,000. This is a slight increase over the 214 SARs filed in the first ten months of 2001. A significant number of financial violations relate to suspicious or fraudulent wire transfer activity to or from the Bahamas. Narratives describe processing large numbers of wire transfers, often in even numbered amounts, many times for several million dollars each. Other activity reported in SARs includes suspicious deposits of money orders and Nigerian advance fee fraud letters.

Burma. An analysis by FinCEN of the Suspicious Activity Reporting System, for the period January 1, 2002 to October 31, 2002, reveals that there are eight SARs that could be linked to transactions associated with Burma. Most of the reported activity involves suspicious wire transfer activity to or from Burma or involving a citizen of Burma. SARs report wire transfers originating in Tokyo, Hong Kong, and Singapore flowing into the United States and sent by individuals using Burmese passports for identification. Banks identify the activity as suspicious due to a lack of information linking the activity to legitimate funds. Additional activity reported on the SARs includes structured cash deposits made by Burmese citizens in an apparent attempt to avoid BSA filing requirements.

Money Laundering and Financial Crimes

Cayman Islands. * An analysis by FinCEN of the Suspicious Activity Reporting System, for the period January 1, 2002 to October 31, 2002, identifies 215 SARs that could be linked to transactions associated with the Cayman Islands. These SARs were filed by 26 U.S. banks, 13 foreign banks, and eight brokerage services firms, with reported amounts ranging from a low of zero dollars to a high of \$14,250,000. This is a noticeable increase over the 187 SARs filed in the first ten months of 2001. The analysis reveals that a significant number (156 or 72.6 percent) involve suspicious or fraudulent wire transfer activity to or from the Cayman Islands. A number of the reports cite “structuring” instances in order to avoid reporting requirements, and Nigerian advance fee fraud letters. Also reported are instances of traveler’s checks, money orders, personal and cashier’s checks being deposited to personal accounts over a relatively short period of time in excessive dollar amounts, followed by issuance of personal checks or wire transfer of funds.

Cook Islands. An analysis by FinCEN of the Suspicious Activity Reporting System for transactions relating to the Cook Islands reveals that 62 SARs were filed by U.S. and foreign banks, brokerage services firms, and money service businesses from January 1, 2002 through October 31, 2002. Reports indicate that 80 percent of the activities involve suspicious or fraudulent wire transfer activity involving Cook Islands entities. The reporting financial institutions in the United States have been unable to verify a physical presence for these entities, described as banks. The banks, reportedly operating in the Cook Islands, maintain correspondent relationships with several banks located in Hong Kong, Taiwan, New Zealand, and Estonia, and have been sending and receiving wire transfers to and from various locations. Each of the correspondent banks has a relationship with United States filing institutions. Incoming wire transfers originate in Cyprus, Russia, Thailand, Azerbaijan, Hong Kong, Germany, Belize, Taiwan, Switzerland, Denmark, Slovenia, Georgia, St. Vincent and the Grenadines, and the Cook Islands itself. Outgoing wires are sent to Belize, Denmark, Cook Islands, Switzerland, Taiwan and Hong Kong.

Dominica. * An analysis by FinCEN of the Suspicious Activity Reporting System, for the period January 1, 2002 to October 31, 2002, reveals that 23 SARs have been filed which could be linked to transactions associated with Dominica. These SARs were filed by 16 U.S. banks and one brokerage services firm with reported amounts ranging from a low of zero dollars to \$4,246,936. This is an increase over 16 SARs filed in 2001, with almost 58 percent (15) of the filings citing “Bank Secrecy Act/structuring/money laundering”; 12 percent (three) citing “Other”, and another 12 percent (three) citing wire transfer fraud.

The majority of the reported activity (16 filings or 70 percent) involves suspicious wire transfers originating and/or terminating in Dominica. Often this is seen in concert with structured cash deposits to avoid BSA reporting requirements, large cash deposits, and the receipt of large checks. Dominica-based financial institutions, as well as companies in various industries including financial services, securities trading, commodities trading, and some retail establishments, are cited as being involved with suspect activity. An interesting trend is the number of SARs citing activity by companies related to Internet gaming/gambling, with several companies mentioned in multiple SARs. Another prevalent feature of wire activity is the use of correspondent banking relationships by Dominica-based financial institutions and companies.

Egypt. An analysis FinCEN of the Suspicious Activity Reporting System, for the period January 1, 2002 to October 31, 2002, reveals 481 SARs that could be linked to transactions associated with Egypt, an increase of 53 percent from the 315 SARs filed in all of 2001. The SARs report transaction amounts ranging from zero dollars to \$84 million.

Most of the reported activity involves suspicious or fraudulent wire transfers destined for Egypt or originating from Egypt. A significant number of overall filings describe transactions conducted by or involving Egyptian nationals. Twenty percent of the SARs report that the specific reason for their filing is a possible relationship to terrorist attacks. It should also be noted that filings display a dramatically increased awareness and scrutiny of all financial activities involving Egypt, although they may not be directly related to the attacks of September 11, 2001. Furthermore, some of these filings make specific

references to transactions by Islamic charitable organizations now suspected of being involved in funding terrorist activities.

Another type of possible money laundering activity noted in Egypt-related filings is the use of credit card accounts. Many SARs report large cash payments (\$9,900 to \$20,000) to credit card accounts with small or zero balances. Two SARs indicate the deposits were made in Cairo, that is, outside of the United States, with the U.S.-based cardholders requesting "Credit Balance Refund Checks" to be sent to them within days of the cash deposits being made. This activity circumvents BSA rules while allowing accessibility to funds virtually worldwide.

Grenada. * FATF removed Grenada from the NCCT list in February 2003. An analysis by FinCEN of the Suspicious Activity Reporting System, for the period of January 1, 2002 to October 31, 2002, reveals 37 SARs involving Grenada, which is lower than the 46 SARs filed in 2001. The 2002 SARs were filed by 16 U.S. banks, two brokerage or mortgage service firms, one foreign bank, and one money service business. Two SARs filed in February 2002 relate to the September 11 terrorist attacks on the United States. Both SARs, which were filed by the same U.S. bank, describe an attempt to open accounts for the benefit of the victims of the September 11 attacks. The trust funds were allegedly going to be donated by a trust organization incorporated in Belize, which has its headquarters in Grenada, and an office in Canada. Bank research indicates that the trust organization's sources of funding are suspect and the bank did not open the accounts.

Guatemala. The FinCEN conducted an analysis of the Suspicious Activity Reporting System for transactions relating to Guatemala for the period January 1, 2002 through October 31, 2002. Results of the query include identification of 184 SARs that could be linked to transactions associated with Guatemala. These SARs were filed by 50 U.S. banks, nine foreign banks, and six money service businesses, with reported transaction amounts ranging from a low of zero dollars to \$300 million.

Most of the reported activity involves suspicious or fraudulent wire transfer activity to or from Guatemala. Scenarios reported include groups of individuals sending wire transfers within minutes of each other from the same U.S. money service business location to the same locations in Guatemala, attempts to disguise originating countries in North Africa and Southwest Asia by routing wire transfers through European countries, and excessive cash and/or monetary instrument deposits followed by wire transfers that are not commensurate with the type of business. Several instances of wire transfer activity are reported in conjunction with allegations of political corruption in Guatemala. Businesses involved in the wire transfer activities reported include import/export companies, recycling companies, and money exchange services. Another ongoing trend seen during the past year involves large currency deposits, some of which contain suspicious traveler's checks and money orders, by Guatemalan financial institutions. The traveler's checks and money orders are usually consecutively numbered and payable to the same beneficiaries.

Hungary. * FinCEN conducted an analysis of the Suspicious Activity Reporting System and determined there are 67 SARs that could be linked to transactions associated with Hungary. The SARs were filed by U.S. and foreign banks and money services businesses during the period January 1, 2002 to October 31, 2002. Twenty-one SARs (36.8 percent) involve suspicious or fraudulent wire transfer activity to or from Hungary. Other activity reported includes deposits of multiple postal money orders over short periods of time, most of which were purchased four at a time, many times at different post offices. The deposits are structured in amounts under BSA reporting thresholds and are accompanied by letters instructing that the money be transferred to an offshore mutual fund account. Additional instances of "structuring" in order to avoid reporting requirements are noted. One SAR reports activity involving individuals, who are suspected of being involved in the funding of HAMAS, sending wire transfers to Lebanon. One of the wires came from a Hungarian bank.

Indonesia. FinCEN conducted an analysis of the Suspicious Activity Reporting System for the period from January 1, 2002 through October 31, 2002. Results identify 497 SARs that could be linked to transactions associated with Indonesia. These SARs were filed by 56 U.S. banks, 19 foreign banks, four brokerage services firms, and three money service businesses, with reported transaction amounts ranging

Money Laundering and Financial Crimes

from zero dollars to \$500 million. Three hundred thirty-three (66 percent) of the filings cite “Bank Secrecy Act/money laundering,” while 137 (28 percent) cite “Other” transactions. It is noteworthy that the majority of the transactions listed in the “Other” category are reported as related to terrorist activities.

Most of the reported activity (64 percent) involves suspicious or fraudulent wire transfer activity to or from Indonesia. Incoming and outgoing wire activity, routed through, originating in, and/or terminating in Indonesia involves several different geographical locations, including locations in the Middle East and Asia. The primary pattern of activity, however, involves funds moving from Indonesia to the United States.

Since September 11, 2001, there has been a large increase in filings regarding terrorist-related activities. The searched period yields 85 SARs filed by various financial institutions in response to the attacks of September 11. The following scenarios are seen: (1) financial activity is found for individuals with names similar to known terrorists documented in governmental, regulatory, or media reports; (2) suspect purchases at military supply stores, discount knife stores, aviation schools, and global positioning services; and charitable donations by individuals where the occupations do not support such expenditures; (3) multiple individuals use a single account to conduct suspect financial activity such as outlined above; and (4) automated teller machine (ATM) activity in foreign locations is not commensurate with the stated occupation of the suspects.

Israel. * FinCEN conducted an analysis of the Suspicious Activity Reporting System, for the period January 1, 2002 to October 31, 2002, and determined there are 395 SARs that could be linked to transactions associated with Israel. The SARs indicate that many of the reported financial transactions (311 or 79 percent) involve suspicious or fraudulent wire transfer activity to or from Israel. Frequently the wire transfers seem to be structured to avoid reporting requirements. A number of SARs indicate that family members, or agents claiming to be acting for a person in Israel, conducted wire transfers and other account activities. Financial institutions also filed SARs because the amounts or frequency of the activity is much higher than in the past, because the source of the funds is unknown, or because the filer suspects an agent of using the account for laundering money without the knowledge of the account holder. SARs also report suspicious deposits of sequentially numbered money orders or apparently structured purchases of money orders, and the use of traveler’s checks, often in large volumes. Many of the filing financial institutions suspect that traveler’s checks are used to move money internationally, when other available means would be safer and easier, to avoid reporting requirements.

Sixteen of the SARs report the reason for their filing is related to possible terrorism. For example, among the SARs, five detail wire transfers and other account activity of individuals who are exact or partial matches to names designated by the U.S. Government pursuant to various legal authorities, six recount wire transfers and other account activity that could possibly be pertinent to terrorist funding, and one reports wire transfers involving a charity suspected of funding terrorist activities.

Lebanon. * An analysis by FinCEN of the Suspicious Activity Reporting System related to Lebanon for the period January 1, 2002 through October 31, 2002, reveals there are 286 SARs that could be linked to transactions associated with Lebanon. It also reveals that much of the reported activity (156 or 54.5 percent) involves suspicious or fraudulent wire transfer activity between Lebanon and other countries. Many of the SAR narratives cite “structuring” instances in order to avoid reporting requirements. Other narratives describe the use of traveler’s checks in money laundering attempts and Nigerian advance fee fraud scams. Still other SARs report suspicious use of money orders. Two of the SARs report the reason for their filing is related to possible terrorism.

Liechtenstein. * FinCEN conducted an analysis of its Suspicious Activity Reporting System and found 26 SARs relating to Liechtenstein. SARs were filed by banks (U.S. and foreign) and one brokerage services firm between January 1, 2002 and October 31, 2002. Much of the reported activity (24 SARs, or 92 percent) involves suspicious or fraudulent wire transfer activity to or from Liechtenstein. The SAR narratives report sudden wire transfer activity for large amounts in accounts that had never experienced wire transfer activity. Others note funds wire transferred from unidentified individuals in Liechtenstein

that were then rerouted out of the United States. The SARs seem to indicate a pattern of high dollar value transfers, rather than structuring, which is reported in only one SAR. The reported high value transfers are often by, or to, individuals or companies for whom such activity is an anomaly, or for no discernible reason.

Marshall Islands. * FinCEN conducted an analysis of the Suspicious Activity Reporting System for transactions relating to the Marshall Islands. The SARs were filed by U.S. and foreign banks, brokerage services firms, and money service businesses from January 1, 2002 through October 31, 2002. Two SARs were filed reporting possible transaction amounts ranging from \$2,400 to \$640,000. One SAR cites “Bank Secrecy Act/structuring/money laundering,” while the other SAR cites a check fraud transaction. Activity described in the SARs includes outgoing wire activity originating in the United States and terminating in the Marshall Islands with no apparent business reason for the transaction, and an alleged embezzlement. In this instance, checks drawn on the suspect account were made payable to a U.S. bank, endorsed with two signatures, and cash was received for the amount of the checks.

Nauru. An analysis by FinCEN of the Suspicious Activity Reporting System identifies five SARs that could be linked to transactions associated with Nauru. These SARs were filed by three foreign banks and one brokerage services firm from January 1, 2002 through October 31, 2002. Reported transaction amounts range from a low of zero dollars up to \$55 million (a fraudulent bank guarantee). This is a significant decrease from the 25 SARs filed in 2001. The SARs report activity involving suspicious or fraudulent wires associated with companies or financial institutions either registered or with addresses in Nauru. SAR narratives describe Nauru banks (using only a post office box address) as receiving high dollar value wire transfers and requesting third party wire transfers and checks, deemed to be suspicious by the filing financial institution. The wire transfer activity was rejected and the accounts closed. Additional scenarios identified in SAR narratives include the attempted use of fraudulent bank guarantee documents.

Nigeria. An analysis by FinCEN of the Suspicious Activity Reporting System, for the period January 1, 2002 to October 31, 2002, reveals there are 2,399 SARs that could be linked to transactions associated with Nigeria. There are a high number of financial transactions related to wire transfer fraud, check fraud, and counterfeit checks and money orders. A typical check fraud scheme includes the deposit of counterfeit or fraudulent checks that are sent to United States account holders as payment for merchandise purchased from Nigeria, often over the Internet. A similar, less prevalent check fraud trend involves new account fraud--Nigerian organized crime groups who open new bank accounts using false or stolen information, then deposit fraudulent checks and attempt to withdraw the money before the checks are returned. SAR information also reveals suspicious transactions related to large-volume deposits of traveler’s checks usually purchased or negotiated in Nigeria. Overall, the most frequently reported activity involves advance fee fraud where financial institutions receive solicitations for participation in the fraud scheme, or institutions report on customer activities that indicate their possible involvement in a fraud scheme.

Niue. * An analysis by FinCEN of the Suspicious Activity Reporting System, for the period January 1, 2002 to October 31, 2002, reveals that one SAR has been filed that could be linked to transactions associated with Niue. This is a decrease over the two SARs filed in 2001. The SAR reports “Other” as the transaction and describes suspicious wire transfer activity. The wire was for the benefit of a company with an address in Niue. The SAR filer was unable to obtain a sufficient explanation for the purpose of the wire, did not complete the transaction, and was in the process of closing the account when the SAR was filed.

Panama. * An analysis by FinCEN of the Suspicious Activity Reporting System identifies 304 SARs that could be linked to transactions associated with Panama. These SARs were filed by U.S. and foreign banks, brokerage services firms, and money service businesses from January 1, 2002 through October 31, 2002. The amounts of the transactions range from zero dollars to a high of \$300,000,000. Eighty-two percent of the SARs report “Bank Secrecy Act/money laundering” as the type of transaction, many of which are

“structuring” instances designed to avoid reporting requirements. Much of the reported activity (64 percent) involves suspicious or fraudulent wire transfer activity to or from Panama. In many instances, the individuals deposit cash and then immediately wire out the same amount, or a slightly lesser amount, to beneficiaries in Panama or other countries. A few SARs report “related to terrorism” as the reason for filing the report, because they involve wire transfers by individuals whose names are partial matches to names designated by the U.S. Government pursuant to various legal authorities. These SARs list wire transfers between Panama and Spain, Canada, and Pakistan. One SAR lists dozens of international money transfers by an individual whose name resembles two names on the Specially Designated Nationals list of the USG Treasury Office of Foreign Assets Control (OFAC).

Philippines. FinCEN conducted an analysis of the Suspicious Activity Reporting System for transactions relating to the Philippines. The 407 related SARs were filed by U.S. and foreign banks, brokerage services firms, and money service businesses from January 1, 2002 through October 31, 2002. Incoming and outgoing wire transfer activity, routed through, originating in, and/or terminating in the Philippines represents the majority of the SAR reporting. Most of the SAR narratives report large cash deposits followed by wire transfers to the Philippines. Additional activities reported in SAR narratives include issuance of numerous consecutively numbered checks by a global payment service; involvement in a pyramid scheme operating in Malaysia, Hong Kong, Thailand, Singapore, and Indonesia; and structured cash deposits to avoid reporting requirements.

Russia. * FinCEN conducted a review of the Suspicious Activity Reporting System, for the period January 1, 2002 to October 31, 2002, and identified 664 SARs that could be linked to transactions relating to Russia. The SARs were filed by U.S. and foreign banks, brokerage services firms, and money services businesses. The majority of filings (65 percent) involve wire transfers either to Russia from U.S. accounts, or vice versa. Many of the wires are in large and/or even dollar amounts totaling hundreds of thousands, or even millions of dollars, over periods of months to a year. In many instances funds are wired to an account at a Russian bank with no beneficiary identified. The majority of activity that involves Russian banks cites correspondent-banking relationships with U.S. banks. A behavior noted frequently in SARs citing suspicious wire transfers is the use of ATMs to withdraw funds via locations in the United States as well as in Russia and other European nations.

Approximately 15 percent of SAR filings report that the reason for their filing is related to the terrorist attacks of September 11, 2001, and awareness or scrutiny of all transactions involving customers and businesses associated with Russia, a country on FATF’s NCCT list. A small but significant number of filings mention Russian companies or banks involved in financial fraud schemes. Some of these firms were found to be associated with well-known Russian organized crime groups operating worldwide, while other businesses were identified by local or regional law enforcement from previous incidents in a specific area. Some of the filings cite examples of Nigerian Advanced Fee Fraud, or 419 fraud (referring to the relevant provision in the Nigerian criminal code), indicating that the funds to be moved are allegedly a result of a “pay-back contract” between a Nigerian and a Russian firm operating in Nigeria.

St. Kitts and Nevis. * FinCEN conducted an analysis of the Suspicious Activity Reporting System for transactions relating to St. Kitts and Nevis for the period January 1, 2002 through October 31, 2002. The 53 SARs that could be linked to transactions associated with St. Kitts and Nevis were filed by 19 U.S. banks, three foreign banks, six brokerage services firms, and one money service business, with reported transaction amounts ranging from a low of zero dollars to a high of \$100,000,000. This is a significant decrease over 137 SARs filed in the first ten months of 2001.

The FinCEN analysis reveals significant activity (36 or 64 percent) involving suspicious or fraudulent wire transfer activity to or from Saint Kitts and Nevis. Other SAR narratives describe what appears to be computer intrusion and identity theft, and refer to an apparent fraud that netted over \$200,000. Almost all of the money comes from a bank in Nevis. Other narratives describe alleged real estate investments involving bank guarantees in the \$100 million range, of which the filing institutions were suspicious, and therefore, the reporting institutions decided to close the business accounts involved.

St. Vincent and the Grenadines. FinCEN conducted an analysis of the Suspicious Activity Reporting System for transactions involving St. Vincent and the Grenadines (SVG) for the period January 1, 2002 through October 31, 2002. U.S. banks, money service businesses, and brokerage service companies filed 37 SARs. Overall, SAR narratives report activity involving suspicious wire transfers, most frequently wires sent to SVG. Other SAR narratives (36.4 percent of the total number of SARs), all filed by the same U.S. bank, report suspicious activity carried out by a bank registered in St. Vincent, believed to be operating as a shell bank, since no physical presence could be confirmed. The SAR describes large volumes of suspicious wire transfers into what appear to be three different business accounts at the St. Vincent bank. Additional activities reported include possible securities fraud, structured cash deposits, suspicious account applications, and check fraud activity.

Ukraine. An analysis by FinCEN of the Suspicious Activity Reporting System reveals that the majority of the 130 SARs relating to Ukraine, filed by U.S. and foreign banks, money services businesses, and brokerage service firms from January 1, 2002 to October 31, 2002, report suspicious wire transfer activity. Some of this wire transfer activity is possibly related to charitable organizations with alleged links to terrorism. Narratives describe businesses allegedly operating as shell banks (registration and address information could not be verified) that continue to send and receive wire transfers, as well as fraudulent or suspicious letters of credit, bonds, checks, and certificates of deposit.

SARS Relating to Terrorist Financing

As part of its support to law enforcement, FinCEN routinely prepares proactive referral packages developed from SARs and other BSA information. In 2002, FinCEN conducted a search of the SAR database to determine the extent of SAR filings related to terrorism.

Between September 12, 2001 and March 31, 2002, more than 1,600 SARs were filed that contained references to terrorism or terrorist groups:

September 2001	27
October 2001	446
November 2001	324
December 2001	215
January 2002	292
February 2002	112
March 2002	241

The review indicates that the increase in filings was attributed to the issuance of various government lists of known or suspected terrorists, against which financial institutions researched their files/databases for possible matches. Eighty-five percent of the SARs (1,369) indicate the SAR was filed as the result of apparent matches to the names of individuals or entities provided to institutions by government agencies.

- The SARs were filed by 255 financial institutions.
- The suspicious activity reported in the SARs occurred in 43 states, the District of Columbia, Puerto Rico and Guam.
- Foreign branches of U.S. banks located in Saudi Arabia, Sri Lanka, the United Kingdom and Costa Rica filed SARs relating to terrorist activity.

Money Laundering and Financial Crimes

- Transaction amounts ranged from \$0 to \$300 million.
- There were 1,016 SARs that were filed for reasons other than an attempt to complete a transaction.

The three main activities described in the SARs filed as a result of apparent name matches are:

- Wire transfers;
- Use of ATMs; and
- Large cash transactions.

The suspicious wire transfers occurred predominantly to or from Middle-Eastern countries. Other countries identified in connection with suspicious wire transfer activity included Pakistan, Malaysia, Indonesia, the Philippines, Liberia, Tanzania, Switzerland, the United States and Canada.

The ATM activity was described as suspicious because of the frequency of use and the geographic location of usage. The countries cited in SARs that reported suspicious use of ATMs included Lebanon, Morocco, Saudi Arabia, Jordan and the United States.

The suspicious cash transactions described in SAR narratives were conducted to establish new accounts, pay off credit card debts, effect wire transfers, and purchase money orders and/or travelers checks.

FinCEN further reviewed the SARs to evaluate whether any of them could possibly involve mechanisms to fund terrorist activities. The review reveals that traditional methods of money laundering were used, and at least one of the following additional indicators was involved:

- Movement of funds through state sponsors of terrorism and countries listed as having highly active anti-American terrorist activities;
- Use of unfamiliar charity/relief organization as a link in transactions;
- Wire transfer activities to and from multiple relief and/or charitable organizations, domestic and foreign; and/or
- The individual or entity involved is identified on one of the lists of suspected terrorists, terrorist organizations, or associated individuals or entities.

While these indicators alone may or may not denote terrorist funding, when combined with the common indicators of financial crime and money laundering, such transactions or patterns could be associated with terrorist financing activity. Additionally, when one or more of the potentially suspicious factors exist in regard to a specific financial transaction, increased scrutiny is warranted. Moreover, when the individual or entity appears on one of the lists of terrorist organizations or associated individuals or entities, the transaction may be subject to blocking or forfeiture.

The five synopses below were developed from SARs and other BSA information. They are provided here as illustrations of behavior that could indicate terrorist fundraising activities.

SARS and Terrorist Financing Leads/Cases

Relief/Charitable Organizations in the United States

A bank filed three SARs reporting the activities of a relief organization operating in the United States, whose stated primary purpose is the collection of donations and funds for worthwhile causes in Middle Eastern countries. Over an approximate 15-month period, the relief organization initiated wire transfers from its U.S. bank account totaling \$685,560, through its primary account in a former Soviet Republic, to its accounts in other former Soviet Republic countries. The relief organization's U.S. bank account also

received wire transfers totaling \$724,694 from unknown senders at a European bank, and wired a total of \$65,740 to a U.S. charitable organization. The filing institution deemed this activity inconsistent with the stated purpose of the account.

FinCEN identified two other SARs filed by two banks regarding financial activity of the U.S. charitable organization. The SARs identify \$445,325 wired to the U.S. charitable organization's account in the Middle East through the filing banks' U.S. correspondent bank. The organization also wired \$18,000 to a media services business in the Middle East in 2001. Four different accounts were used. SARs also describe structured cash deposits totaling \$53,800, and check deposits totaling \$121,705. FinCEN identified three additional accounts at three other banks through currency transaction reports (CTRs). Those CTRs report cash deposits totaling \$227,519.

Relief Organization in the Middle East

FinCEN identified 649 SARs filed by seven depository institutions, reporting transactions totaling \$9 million involving structured cash deposits and deposits of business, payroll and Social Security benefit checks. These SARs were filed during a 3-1/2 year period. Deposited funds were subsequently wire transferred within one or two days to a company located in the Middle East. The deposit and wire transfer activity involved 37 individuals conducting transactions through 44 accounts on behalf of four businesses. Two of the businesses were wire remittance companies; one was described as a relief organization at the same location as one of the wire remittance businesses; the fourth undescribed business, located in the Middle East, was the beneficiary of the wire transfer activity. The majority of the wire transfers were sent to two accounts in the Middle East. Other wire transfers were made to accounts at three different banks in foreign locations. The majority of the transactions (83 percent) were structured. Amounts of the deposits ranged from \$350 to \$636,790; most deposits fell between \$2,000 and \$8,000.

Owner of Pharmaceutical Company

A SAR was filed reporting two same-day deposits (\$3,500 and \$9,900), made three hours apart to a savings account by a bank customer. The bank initiated a review of the customer's accounts. The review identified additional suspicious activity in four of his personal accounts, including the original savings account. From December 1999 through April 2001, 38 cash/non-cash deposits and one wire transfer deposit totaled \$2,202,384. During the same time period, one withdrawal, two redemptions of negotiable instruments, three wire transfers and two other debit transactions totaled \$2,256,223. Of this total, \$2,040,370 flowed into the original suspect's savings account and \$2,097,323 flowed out of the account. Cash and non-cash deposits were described as even dollar amounts ranging from \$1,000 to \$100,000. Wire transfer activity included a \$25,000 wire transfer received from an individual and three transfers totaling \$100,000 sent to two different individuals. The SAR, and related CTRs, describe the individual as the owner/president of a pharmaceutical company and the owner/CEO of a biochemical laboratory.

In July 1996, this individual transported \$11,200 into the United States from a Caribbean country, and in December 2000, he transported \$11,500 from the United States to Europe. In both instances, he claimed citizenship in a country subject to a travel warning for anti-American terrorist activity and provided a non-U.S. passport as identification. He is also cited as entering the United States a total of 32 times from March 1996 through August 2001. Identification provided, as cited in the entry records, was an alien registration number.

Law Enforcement Cases Relating to Terrorism

In 2002, law enforcement agencies continued to use both the financial transparency "paper trail" and investigative techniques such as informants and undercover investigations to penetrate suspect criminal organizations. Generally, law enforcement uses a combination of resources and techniques to put a case together. The following case examples highlight successful law enforcement investigations and techniques:

Operation Smoke Screen

In a far-reaching case involving the prosecution of individuals involved in the financing of terrorism, two men in Charlotte, North Carolina were convicted in May 2002 (seven defendants previously pled guilty) of providing, and conspiring to provide, material support to Hizballah, a designated Foreign Terrorist Organization. The criminal group perpetrated an interstate cigarette tax evasion scheme whereby inexpensive cigarettes from North Carolina were transported to and then sold in Michigan to avoid the latter state's higher taxes. Profits from the operation were forwarded to Hizballah. Law enforcement authorities around the world have recognized that cigarette smuggling networks can generate enormous profits. Moreover, trafficking in cigarettes often is the precursor to other types of contraband smuggling such as weapons and narcotics.

The case was initiated when a deputy sheriff working part-time at a large tobacco wholesaler in North Carolina noticed the same individuals purchasing large quantities of cigarettes. The suspects drove vehicles with out-of-state license plates. A joint investigation among federal, state, and local authorities ensued. Surveillance of the suspects revealed a large-scale cigarette smuggling ring involving the use of tobacco storefront operations in North Carolina to justify the large purchases and bulk sale of cigarettes. Based on the surveillance, search warrants were obtained for the businesses and residences of the subjects. As a result of the warrants, law enforcement personnel seized photos of the subjects counting large volumes of cash, a Hizballah banner, a Hizballah propaganda video of suicide bombers, and materials evidencing the involvement of some of the suspects with military training and/or operations. A receipt from a Hizballah leader for money received from the smuggling ring was located during the searches. Numerous false identification documents for the subjects were also found. Further evidence recovered showed that the criminal group intended to purchase a variety of items for Hizballah including night vision devices, radios and receivers, and metal detection devices. Ultimately, 25 individuals were charged with various transactions, including material support to a terrorist organization, money laundering, conspiracy, bank fraud, credit card fraud, and visa entry fraud. The Bureau of Alcohol, Tobacco, and Firearms played a large role during the initial stages of the investigation and the Federal Bureau of Investigation contributed during the later stages by helping to develop the link to a terrorist organization.

HAMAS Leader Indicted

In Dallas, Texas, an indictment was returned against a senior leader of HAMAS (a designated Foreign Terrorist organization) for conspiring to violate United States laws that prohibit dealings in terrorist funds. The HAMAS leader and a Texas-based company, INFOCOM Corporation, allegedly conspired to hide his continuing financial interests with the computer company. The indictment asserts that INFOCOM continued to engage in financial transactions with the HAMAS leader after his designation as a terrorist, in violation of the International Emergency Economic Powers Act.

Terrorist Organization Donor Indicted

In another case, the director of an Islamic charity in suburban Chicago was charged with funneling money to a terror network and other violent groups through his Benevolence International Foundation. The indictment describes a multi-national criminal enterprise that over many years fraudulently used charitable contributions from innocent Americans—Muslim, non-Muslim and corporations alike—to support al-Qaida, the Chechen mujahedin, and armed violence in Bosnia. The charges include providing material support to terrorists, mail and wire fraud, and transactions of the Racketeer Influenced and Corrupt Organizations (RICO) statute.

Narcoterrorism

Indictments were issued against terrorist groups that directly combine narcotics-trafficking with their terrorism activities. Leaders of the United Self-Defense Forces of Colombia (AUC), a Colombian right-

wing paramilitary group listed on the State Department's Foreign Terrorist Organization list since 2001, were charged with various narcotics-trafficking offenses. The indictment alleges that, since January 1997, they caused the maritime shipment of approximately 17 tons of cocaine to the United States and Europe. The United States has requested that the Colombian government extradite all defendants to the United States for trial. A second case against members of AUC commenced in Houston, Texas. This case also involved a massive cocaine-for-arms scheme. Through three separate indictments, the United States has charged several members of a second Colombian terrorist group, the Revolutionary Armed Forces of Colombia, or FARC, with murder, kidnapping of U.S. citizens, and trading illegal drugs for weapons. The United States has long considered FARC a terrorist organization. Finally, in October 2002, an indictment was issued in San Diego that charged three individuals with a drug conspiracy and with conspiring to provide material support or resources to al-Qaida. This case started as an undercover sting operation, in which an FBI agent posing as a prospective drug buyer approached a person in the United States who claimed to have contacts in Pakistan with narcotics available for sale. The scheme evolved into discussions about an exchange of drugs for Stinger missiles, which the Pakistani defendants claimed were needed for persons fighting in Afghanistan (i.e., the Taliban or al-Qaida).

Charity Maze

In December 2001, Operation Green Quest developed information that a group of individuals were allegedly funneling funds to designated terrorist organizations through a maze of interrelated charities. The initial analysis reflected that these organizations were conducting transactions in excess of \$1 billion. In 2002, Operation Green Quest coordinated the execution of approximately 20 search warrants on businesses and residences associated with this organization. Ten warrants were also executed on identified Internet servers. The ongoing investigation includes the review of seized documents, electronic files, and financial transactions in order to identify the suspect terrorist connections.

Bulk Currency Smuggling

In the United States, "bulk currency smuggling" is a money laundering and/or terrorism financing technique that is designed to bypass financial transparency reporting requirements and the U.S. Customs Service Currency and Monetary Instrument Report (CMIR), which obligates the filer to declare if he or she is transporting across the border \$10,000 or more of cash or monetary instruments. Often the currency is smuggled into or out of the United States concealed in personal effects, secreted in shipping containers, or transported in bulk across the border via vehicle, vessel or aircraft. In 2002, an Operation Green Quest investigation was initiated in response to two seizures by U.S. Customs of approximately \$300,000 concealed within the lining of clothing being shipped to Lebanon. Search warrants executed on the address associated with the violator resulted in the seizure of approximately \$2.2 million. The investigation is progressing as a joint effort between U.S. Customs and other federal law enforcement agencies.

Outreach and Unlicensed Remitter

In 2002, U.S. Customs initiated an investigation of a company suspected of providing financial support to terrorism. The investigation was based on a referral from a financial institution. Customs agents identified \$28 million that the targeted company wired overseas from the United States. As the investigation progressed, agents determined the target was operating as an unlicensed remitter, and a significant amount of the funds were illegally being transferred to an embargoed country. A search warrant executed on the business subsequently led to approximately 29 search warrants throughout the United States. The investigation culminated with the indictment and arrest of the primary target and five of his representatives. Charges include money laundering, with transactions of the International Emergency Economic Powers Act as the predicate crime. In an effort to trace the flow of funds and merchandise internationally, agents are working with their foreign counterparts to determine the end users and prosecute the intermediaries who were involved in the transactions.

Trade-Based Money Laundering

The misuse of international trade has long been employed to avoid taxes, tariffs, and customs duties. It is believed that with the increasing transparency governing financial transactions around the world, criminal elements may also increasingly use traditional and widespread fraudulent trading practices to launder funds. For example, the under-invoicing of a shipment of trade goods from country A to country B is a simple and effective way of avoiding or lowering customs duties or tariffs. Trade is also used to launder the proceeds of criminal activity. Over-invoicing a shipment of goods can provide criminal organizations the paper rationale to send payment abroad and/or launder money. For example, if a container of electronics is worth \$50,000 dollars but is over-invoiced for \$100,000, the subsequent payment of \$100,000 will pay both for the legitimate cost of the merchandise (\$50,000) and also allow an extra \$50,000 to be remitted or laundered abroad. The cover of the business transaction and related documentation wash the money clean. There are a multitude of other types of invoice fraud and trade manipulation. For example, export incentives often encourage fraud. There have been numerous examples of governments paying a company cash incentives to export products at the same time the company is using the same export to launder money. In some countries, traders report to exchange control authorities that imports cost more or exports less than the actual cost. The excess foreign exchange generated can be used to purchase additional foreign trade items. And in some areas of the world, trade goods (including narcotics) are simply bartered for other commodities of value.

The simple examples above are made complex when the misuse of trade also involves traditional and entrenched ethnic trading networks, indigenous business practices, smuggling, corruption, narcotics-trafficking, the need for foreign exchange, capital flight, terrorist financing, and tax avoidance. Frequently, many of these elements are commingled and intertwined, making it extremely difficult for criminal investigators to follow the trail.

Trade-based money laundering can also be viewed as a component of other types of alternative remittance systems, such as hawala, the Black Market Peso Exchange, and the use of precious metals and gems. Alternative remittance systems, sometimes also known as informal value transfer systems (IVTS), parallel banking or underground banking, move money or transfer value without necessarily using the regulated financial industry. In all of these alternative systems, trade is most often the vehicle that provides “counter-valuation” or a method of “balancing the books”.

Because of the increased worldwide focus on counter-terrorist financing, increased attention is also being given to these non-traditional methodologies that are frequently found in regions of concern. It is difficult for law enforcement and customs to interdict suspect transactions in this underworld of trade. But at times, these systems may intersect with banks and other traditional financial institutions in order to obtain currency needed to make disbursements, or as links in the clearing process involving wire transfers. It is at these intersections with financial institutions that the brokers or their representatives may become known, and their transactions reviewed for indications of unusual activity in countries that require suspicious transaction reports. Customs and law enforcement officials must play a much more aggressive role in recognizing and investigating how trade can be used in money laundering and in the financing of terrorism.

Gold, Gems, Diamonds and Trade

The trade in gold, diamonds other precious metals and gems has long been associated with money laundering. Terrorist organizations around the world have also used gold and the trade of precious commodities to launder money or transfer value. Since there has been increasing worldwide success in implementing financial transparency, the underworld of gold and other precious metals and gems may increasingly be used as an alternative method of laundering funds.

There are many reasons for gold’s popularity with money launderers. For example, gold has been a haven for wealth since antiquity; it is a readily acceptable medium of exchange around the world; its value is

relatively constant; it offers easy anonymity; it is portable; the form of gold can be readily altered; the trade is easily manipulated; there are often cultural reasons that ensure a constant demand for gold; depending on the form of gold, it can act as either a commodity or a de facto bearer instrument. Gold is used in all stages of money laundering, i.e. placement, layering, and integration. Gold is an alternative remittance system by itself. It is also an integral part of other alternative remittance systems such as hawala and the Black Market Peso Exchange. Although almost any trade item can be used to launder money, gold is particularly attractive to money launderers because it is less bulky than many other commodities and has a relatively constant high dollar value.

Because of gold's unique properties, it has also long been used as a vehicle to help finance terrorist operations. For example, the right-wing Posse Comitatus in the United States, the Aum Shinri Kyo cult in Japan, and Colombian narcotics traffickers have used gold. Most recently, there are reports that al-Qaida has used gold as an instrument of finance.

Gems such as emeralds and tanzanite are also linked to money laundering and terrorist financing. For example, much of the trade in emerald gemstones identified as originating in Pakistan actually originates in Afghanistan. The gems are often traded through Mumbai and Jaipur, India, and the resulting sale revenue goes directly to Dubai, where it is traded for gold bullion, which goes back to India. Gemstone auctions in Burma are used to launder narcotics monies. There are reports that tanzanite, mined only in northeastern Tanzania, is smuggled through ports in East Africa to bazaars in the Middle East. The black market trade in these gems is susceptible to manipulation by money launderers and those that help finance terrorism.

The extra-legal trade in diamonds in Africa often involves money laundering for criminal and political purposes, and loss of revenue via tax evasion. It also provides the means to purchase arms and influence the political arena. "Blood diamonds" is the term used to describe the diamond trade that has helped finance African civil wars in Angola, Sierra Leone, Liberia, and other countries. There are also allegations that the diamond trade intersects terrorist financing operations. The diamond trade in Africa is susceptible at many levels to exploitation, including cross-border trade using established diamond trade routes, secondary level traders and agents, and suspect buyers. Diamond traders in Africa are often non-African. Operating from secured compounds, expatriate buyers often purchase rough diamonds via local currency. (Although purchases occur in local currency, the diamond trade uses U.S. dollars at all levels of commerce including the payment to buyers.) Subsequent exports by the diamond buyers to the major diamond trading centers are often under-valued. Diamonds are also used to provide counter-valuation in hawala transactions. Many of the diamond buyers involved with illicit diamond dealing in West and Central Africa pay protection money to groups identified as terrorist organizations.

Trade and Terrorist Financing

A south Asian trader based in southern Africa has a legitimate business involving the importation of electronics from a supplier based in Dubai. He also has a side business that launders money for numerous businessmen who are also based in southern Africa and are of the same ethnic group as the trader. Most of the laundered money originates from the black trade in precious gems. During the course of his import business, he asks the Dubai supplier, a member of his same extended family, to over invoice the electronics by 100 per cent. For example, a legitimate invoice for \$100,000 would be invoiced as \$200,000. The electronics are then shipped from Dubai to the trader in southern Africa where they are sold for profit.

The trader then sends a wire transfer for payment of the \$200,000 from his bank in southern Africa to the bank of the Dubai supplier. The difference between the \$100,000 actual price of the electronics and the fictitious price of \$200,000 represents \$100,000 laundered from his colleague's criminal activity involving the trade in precious gems. Some of the money in Dubai is then transferred to a third country as legitimate business profits via normal banking procedures. The participants in the money laundering network share the same political ideology. Thus, twenty percent of the profits from the laundering operation are transferred to terrorist affiliated organizations.

Trade and Hawala

In Somalia, there currently is an absence of regulated commercial banks. As a result, remittance companies are the primary conduits for moving funds into and out of Somalia. Although the overwhelming majority of these funds are used for legitimate purposes, a small percentage of transactions—sometimes labeled “black hawala”—mask the transfer of value for criminal purposes. The following is an example of how trade is used to provide counter-valuation for hawala¹: A Somali trader buys commodities from Dubai for resale in Somalia. In order to finance the trade, the Somali trader contacts a local agent of a remittance company in Mogadishu. The trader gives cash to the local remittance agent. (Most transactions are dollar-based but other currencies are used as well.) A commission is charged for the exchange. The trader asks that the funds be transferred to his foreign bank account located in Dubai.

The local agent of the remittance company contacts a hawala clearinghouse that is also located in Dubai and asks that funds be transferred to the Dubai-based bank account identified by the Somali trader. The Dubai bank issues a letter of credit so that goods can be purchased. The desired goods are purchased in Dubai and the vendors have no idea—nor do they care—that the origin of the funds is actually the result of a hawala exchange. The trade goods are then shipped to Somalia and sold by the trader. A percentage of the profit is kept and the balance is used to pay suppliers, and the cycle is repeated. Although this example focuses on Somalia, reports have indicated that the same hawala/trade networks are also used in other countries in Eastern Africa.

Black Market Peso Exchange—Trade and the Underground Economy

One of the most prevalent methods of laundering money through trade in the Western Hemisphere is via the Colombian Black Market Peso Exchange or BMPE. This money laundering technique is used to evade detection through the U.S. Bank Secrecy Act reporting requirements. In simple terms, Colombian cartels sell drug-related, U.S. dollars to black market peso exchangers in Colombia. Once this currency exchange has occurred, the trafficking organization has effectively laundered its money and is out of the BMPE process. The peso broker, on the other hand, must then launder the accumulated U.S. dollars in the United States. The peso broker uses a variety of methods to place the U.S. narcotics proceeds into financial institutions. (For U.S. law enforcement, the “placement” stage in money laundering represents the best opportunity to identify and interdict money laundering.) The peso broker, operating in Colombia, thus has a pool of narcotics-derived funds in the United States to “sell” or “exchange” to legitimate Colombian importers. The funds are used to purchase trade goods such as cigarettes, electronics, and gold.

The U.S. Department of Treasury’s Internal Revenue Service Criminal Investigation Division (CID) has an Illegal Source Financial Crimes Program that recognizes that money gained through illegal sources is part of the untaxed underground economy. The underground economy is a threat to the U.S. voluntary tax compliance system and undermines the overall public confidence in the tax system. The Internal Revenue Code generally states that all income is taxable, from whatever source it is derived. The IRS Narcotics Related Financial Crimes Program seeks to reduce the profits and financial gains of narcotics-trafficking and money laundering organizations that comprise a significant portion of the untaxed underground economy. In the case of BMPE investigations, the IRS and other law enforcement agencies, such as the U.S. Customs Service and the Drug Enforcement Administration, seek to disrupt a trade-based money laundering methodology that aims to legitimize the proceeds of narcotics-trafficking by exchanging funds for trade items often found in the untaxed underground economy.

¹ Abdusakem Omer, “A Report on Supporting Systems and Procedures for the Effective Regulation and Monitoring of Somali Remittance Companies (Hawala)” prepared for the United Nations Development Program, Mogadishu , 2002, pp 12-13.

Bank Secrecy Act CTR Filings: BMPE Structuring Case

On April 22, 2002 in Miami Florida, Lourdes Garcia-Rodriguez and Nancy Torguet-Cavantes were found guilty of conspiracy to launder drug money and conspiracy to structure bank deposits in amounts under the \$10,000 IRS reporting threshold. The subjects laundered approximately \$5 million in drug proceeds through the Colombian BMPE. The subjects used their Miami-based freight company to export over \$5 million worth of household appliances to customers in Colombia. Those customers paid for the appliances with bulk amounts of drug cash delivered to the offices of the Miami freight company. The subjects accepted the cash without completing the IRS forms required to document the receipt of cash over \$10,000. They then deposited the drug dollars into a series of bank accounts in structured deposits of less than \$10,000 each; this enabled them to avoid the financial reporting laws that require banks to report all cash transactions over \$10,000. As a result of this IRS investigation, in January 2003, the subjects were sentenced to a total of 70 months imprisonment.

BMPE—Undercover Operation and International Cooperation

Operation Wire Cutter is another example of targeting a BMPE exchange that attempted to launder millions of drug dollars. Operation Wire Cutter used undercover operations as a successful law enforcement technique to interdict and thwart the BMPE methodology. Operation Wire Cutter began in September 1999 when U.S. Customs Service agents of the multi-agency “El Dorado” Task Force in New York developed information about suspected money brokers using the BMPE. The primary suspects were eight senior money brokers, located in Bogotá, believed to have over 50 years combined experience laundering drug money for Colombian cartels. Each of the money brokers headed distinct organizations that provided money laundering services to several organizations on a contract basis.

Undercover U.S. Customs agents in New York, posing as money launderers, entered into agreements with the Colombian brokers. Acting on instructions from the Colombian brokers, the undercover Customs agents “picked-up” drug currency in various U. S. cities and wired it to accounts specified by the brokers. At the same time, the Colombian Departamento Administrativo de Seguridad (DAS) working with Customs and the U.S. Drug Enforcement Administration (DEA) conducted a parallel investigation of the BMPE money brokers and their associates in Colombia. This was the first time that U.S. authorities were able to combine undercover pick-ups of drug proceeds in the U.S. with investigative efforts by Colombian authorities to target BMPE money brokers. By coordinating investigative resources, authorities in both countries were able to monitor the money laundering process “full-circle”—watching drug funds enter the system in the United States and exit the system in Colombia.

Operation Wire Cutter resulted in the arrest of 37 individuals, 29 in the United States and eight in Colombia. United States authorities also seized more than \$8 million dollars as well as 400 kilos of cocaine, 100 kilos of marijuana and 6.5 kilos of heroin.

Bilateral Activities

Training and Technical Assistance

During 2002, a number of U.S. law enforcement and regulatory agencies provided training and technical assistance on money laundering countermeasures and financial investigations to their law enforcement, financial regulatory, and prosecutorial 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, 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

Through the Department of State's Bureau for International Narcotics and Law Enforcement Affairs (INL) in close coordination with the Department's Office of the Coordinator for Counter-Terrorism on terrorist financing issues, \$3.27 million was expended in fiscal year 2002 to provide law enforcement, prosecutorial and central bank training to countries around the globe. A prime focus of the training program was a multi-agency approach to develop or enhance financial crime and anti-money laundering regimes capable of combating not only money laundering activities but terrorist financing in selected jurisdictions. Supported by and in coordination with the State Department, the Department of Justice, Treasury Department component agencies, the Board of Governors of the Federal Reserve, the Federal Deposit Insurance Corporation, and non-government organizations offered law enforcement, regulatory and criminal justice programs worldwide.

During 2002, 37 INL-funded programs were delivered in 31 countries to combat international financial crimes, money laundering and terrorist financing. Nearly every federal law enforcement agency assisted in this effort by providing basic and advanced training courses in all aspects of financial criminal activity. In addition, INL made funds available for intermittent posting of 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 worldwide to combat money laundering.

INL along with the European Union and the Government of the United Kingdom continues to fund the Caribbean Anti-Money Laundering Programme (CALP). INL contributed \$600,000 to the CALP in 2002. The objectives of CALP are to reduce the laundering of the proceeds of all serious crime by facilitating the prevention, investigation, and prosecution of money laundering. CALP also seeks to develop a sustainable institutional capacity in the Caribbean region to address the issues related to anti-money laundering efforts at a local, regional and international level.

In 2002, INL contributed \$1.5 million to the United Nations Global Program 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 year-long basis to specific countries or regions. In 2001, GPML mentors in the Caribbean assisted the Bahamas and Barbados in constructing viable Financial Intelligence Units. A GPML mentor provided advice on money laundering and asset forfeiture legislation to Antigua and Barbuda as well. Another GPML mentor provided assistance to the Secretariat of the East and South Africa Anti-Money Laundering Group (ESAAMLG). INL continues to provide significant financial support for many of the anti-money laundering bodies around the globe. During 2002, INL support was furnished to the Financial Action Task Force on Money Laundering (FATF), the international standard setting organization, and to FATF-styled regional bodies (FSRBs) including the Asia/Pacific Group on Money Laundering (APG), the Council of Europe's Moneyval, formerly known as the Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (PC-R-EV, and the Caribbean Financial Action Task Force (CFATF). INL also provided financial support to the evolving ESAAMLG and the South American Financial Action Task Force, Grupo de Accion Financiera de Sudamerica Contra el Lavado de Activos (GAFISUD), the FATF-styled regional body in South America.

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 in assessments and training programs. This allows for an extensive dialogue and exchange of information. This approach has been used successfully in Asia, Central and South America, Russia, the New 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 (ILEAs).

International Law Enforcement Academies (ILEAs)

The ILEAs are a progressive concept in the area of international assistance programs. These four—soon to be five—academies offer a core law enforcement management program, regional seminars, and specialized training programs tailored to region-specific needs and emerging global threats, such as terrorism. Indeed, underscoring the ability of ILEAs to adapt quickly, the United States has already amended the money laundering portion of the “core” course presented at each ILEA to address terrorist financing, and the ILEA program is working on finalizing a new “specialized” course that would focus specifically and in detail on terrorist financing. 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 and Treasury, and with foreign governments to implement the ILEA programs. To date, the combined ILEAs have trained over 10,000 officials from 50 countries. The annual ILEA budget averages approximately \$18-19 million.

Europe. ILEA Budapest (Hungary) opened in 1995 to provide assistance to Russia, Central Asian and Eastern European countries. Trainers from the United States, Hungary, Canada, Germany, Great Britain, Holland, Ireland, Italy, Russia, INTERPOL and the Council of Europe provide instruction. ILEA Budapest trains approximately 750 students annually.

Asia. ILEA Bangkok (Thailand) opened in March 1999. The curriculum and structure of this Academy are similar to Budapest, except for the shorter duration of the core course and an added emphasis in narcotics matters. Participation is open to members of the Association of South East Asian Nations (ASEAN) and the Peoples Republic of China. Trainers from the United States, Thailand, Japan, Netherlands, Australia, Philippines and Hong Kong provide instruction. ILEA Bangkok trains approximately 550 students annually.

Africa. ILEA Gaborone (Botswana) opened in 2001. Its overall instructional format is similar to Budapest and Bangkok, but adjusted to suit the needs of the region. Participation is open to members of the Southern African Development Community (SADC), with expectations of future expansion to East African and other sub-Saharan African countries. ILEA Gaborone trains approximately 450 students annually.

Global. ILEA Roswell (New Mexico) opened in September 2001. It offers a curriculum similar to that of a Criminal Justice university. The courses have been designed by, and are taught by academicians, for graduates of the regional ILEAs. This Academy is unique in its format and composition, with an academic focus targeted to a worldwide audience. ILEA Roswell trains approximately 450 students annually.

Latin America. The Department of State is in the process of establishing an ILEA in San Jose, Costa Rica, along the lines of the existing academies in Budapest, Bangkok and Gaborone. A Bilateral Agreement establishing the ILEA was signed with the government of Costa Rica in June 2002, and training activities are expected to begin in 2003.

Board of Governors of the Federal Reserve System (FRB)

The FRB is active in the effort to deter money laundering, primarily through ensuring compliance with the Bank Secrecy Act and the USA PATRIOT Act by the domestic and foreign banking organizations that it supervises. In another initiative to combat money laundering, FRB staff conducted training in anti-money laundering tactics and provided technical assistance to banking supervisors and law enforcement officials throughout the world. Programs for Malaysia, Dominican Republic, Argentina, Barbados, Turkey, and the Philippines were provided in 2002.

In addition to its international training programs, the FRB presented training courses to U.S. law enforcement agencies, including the Federal Law Enforcement Training Center, Internal Revenue Service, Federal Bureau of Investigation, U.S. Customs Service, and Drug Enforcement Administration. The FRB

also participated in financial sector assessment trips to several countries in the Middle East as a member of U.S. interagency teams.

Drug Enforcement Administration (DEA)

The DEA Office of Training, International Training Section, conducts the International Asset Forfeiture and Money Laundering Seminar portions of the U.S. Department of Justice Asset Forfeiture Program. The intent of these seminars is to share, compare, and contrast U.S. legislation with that of other countries, building a relationship and fostering communications with foreign narcotics enforcement officials and prosecutors. Approximately 35 foreign government officials attend each seminar.

The week-long seminars employ lectures, presentations, case studies, and practical application exercises. The Department of Justice Asset Forfeiture Section, the U.S. Customs Service, the U.S. Marshal Service, and various divisional offices of DEA provide the guest lecturers.

The course curriculum includes instruction addressing money laundering and its relation to central bank operations, asset identification, seizure and forfeiture techniques, financial investigations, document exploitation, and international banking. Overviews of U.S. asset forfeiture law, country forfeiture and customs law, and prosecutorial perspectives are also included.

All seminars are conducted in-country. In 2002, seminars were conducted in Germany, Guatemala, Ecuador, Netherlands, Dominican Republic, and the United Kingdom.

Federal Bureau of Investigation (FBI)

During 2002, FBI agents and analysts assigned to the Terrorist Finance Operations Section (TFOS) provided training and presentations relating to terrorism financing methods and money laundering to law enforcement and banking officials of Australia, Belgium, Canada, Germany, Kuwait, the Netherlands, New Zealand, Finland, Germany, Jordan, Paraguay, Pakistan, Philippines, Russia, Singapore, Switzerland, Turkey, Thailand, United Arab Emirates and the United Kingdom. In many instances additional course instruction was also provided on topics ranging from evidence acquisition and case organization to computer forensic examination techniques. Additionally, in November 2002, TFOS sponsored an international seminar in the United States on the informal value transfer system hawala. Officials from India, Pakistan, Jordan, and the United Kingdom attended this week-long conference.

Federal Deposit Insurance Corporation (FDIC)

The FDIC is working in partnership with several agencies against money laundering and the global flow of terrorist funds. Additionally, the agency participates in the planning and conduct of missions to assess vulnerabilities to terrorist financing activity worldwide, and to develop and implement plans to assist foreign governments in their efforts in this regard. To better achieve this end, the FDIC solicited employees interested in providing examination and other pertinent expertise. The response was overwhelming, with almost 100 candidates. Twenty individuals were selected to participate in foreign missions.

A training session was held in June 2002 that provided mission participants with background information on the international conventions on money laundering and terrorism, and expectations for foreign mission participants. A multi-agency team of instructors brought varying perspectives and experience to the session.

The FDIC's Division of Supervision and Consumer Protection participated in the decision-making process of the Basel Committee that led to the approval, and April 17, 2002 issuance of the Sharing of Financial Records Between Jurisdictions in Connection with the Fight Against Terrorist Financing.

Periodically, FDIC staff meets with supervisory and law enforcement representatives from various countries to discuss anti-money laundering 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 2002, such presentations were given to Antigua, Barbados, Brazil, Chile, Dominica, Grenada, Russia, St. Lucia, St. Vincent and the Grenadines, and Thailand.

In April 2002, the FDIC sponsored the FDIC International Visitors Training Program. In addition to sessions on deposit insurance, bank closing procedures and general supervisory issues, one of the segments addressed the USA PATRIOT Act and anti-terrorist financing efforts. The session covered international conventions and specific requirements of the USA PATRIOT Act that will affect the international community. Attendees represented Armenia, Bosnia and Herzegovina, Bulgaria, Canada, China, Czech Republic, Estonia, Germany, Hong Kong, Hungary, Indonesia, Japan, Mozambique, Serbia, Thailand, Turkey and Venezuela.

FDIC provided anti-money laundering training and technical assistance to the Republic of the Marshall Islands (RMI) in February 2002. Staff assisted RMI in developing anti-money laundering regulations and examination procedures. The RMI had been on the FATF NCCT list, and the U.S. Treasury Department had issued financial advisories to U.S. banks warning them to scrutinize RMI transactions. Among the deficiencies cited by FATF was the lack of a regulatory scheme to detect money laundering in financial institutions. FDIC's assistance to the RMI was a valuable part of the RMI's efforts to be removed from the NCCT list.

FDIC staff also provided anti-money laundering technical assistance to the Government of Fiji in February 2002. The technical assistance request came from the Asia/Pacific Group on Money Laundering through the U.S. Treasury Department. Working collaboratively with anti-money laundering experts from Malaysia and New Zealand, the FDIC's staff evaluated Fiji's compliance with the FATF Forty Recommendations on Money Laundering.

In September 2002, FDIC staff gave an anti-money laundering presentation to the Taiwan Academy of Banking and Finance, a group comprised of various banking supervisory agencies. Topics included the Bank Secrecy Act, the USA PATRIOT Act, components of anti-money laundering examination programs and procedures, and an effective bank anti-money laundering program.

Financial Crimes Enforcement Network

FinCEN, the U.S. Financial Intelligence Unit (FIU), a Bureau of the U.S. Treasury Department, coordinates and provides training and technical assistance to partner nations seeking to work against financial crimes, put in place anti-money laundering regulatory regimes, and establish Financial Intelligence Units. Its international training program focuses on providing training and technical assistance to a broad spectrum of foreign government officials, financial regulators, law enforcement personnel, and bankers. FinCEN's international training program has two main components: (1) instruction to a broad range of government officials, financial regulators, law enforcement officers, and others, on the subject of money laundering and FinCEN's mission and operation; and (2) financial intelligence analysis training and the operational aspects of FIUs such as FinCEN. For those FIUs that are fully functional the goal is to help them achieve an improved level of cooperation with U.S. and other FIUs in the exchange of information and the achievement of a better understanding of money laundering phenomena. As a member of the Egmont Group of FIUs, FinCEN also works closely with other members of the Egmont Group to provide training and technical assistance to various jurisdictions in establishing and operating their own FIUs.

During 2002, FinCEN conducted training courses independently, as well as with other agencies. In some instances courses are developed jointly with other agencies to address specific needs of the jurisdictions. A

number of these courses are provided abroad to maximize the utility to the FIU. Such training sessions were held in Bulgaria and Poland in 2002.

Much of FinCEN's work also involves strengthening existing FIUs and reinforcing channels for communicating operational information in support of anti-money laundering investigations. This includes participation in personnel exchanges (from the foreign FIU to FinCEN and vice versa) and regional and operational workshops. For instance FinCEN hosted a workshop on Informal Value Transfer Systems (IVTS) in Mexico in October 2002 that included presentations and discussions about the money laundering risks posed by IVTS service providers, such as hawala, and the law enforcement and regulatory challenges posed by such systems. Over 50 countries sent representatives. During the past year, FinCEN has also engaged in week-long personnel exchanges with the FIUs of Turkey and South Korea.

In 2002, representatives from well over 50 countries visited FinCEN to learn what is new in money laundering trends and patterns, details of the USA PATRIOT Act, international case processing, and the regulatory role of FinCEN. Additionally, FinCEN hosted delegations for more intensive seminars in computer software programs, data mining, and case processing from various jurisdictions of the Caribbean, the Middle East, Africa, Southeast Asia and the Pacific, Central and South America, the Gulf States, and Europe.

Internal Revenue Service (IRS)

In 2002, the IRS Criminal Investigation Division (IRS-CI) increased its commitment to international training, multi-agency training efforts and technical assistance programs to foreign law enforcement agencies.

IRS-CI continues to provide training in Financial Investigative Techniques and Money Laundering at the International Law Enforcement Academies (ILEA) at Bangkok, Budapest and Gaborone. In furtherance of this commitment IRS-CI has detailed a special agent to serve as Deputy Director at the ILEA in Bangkok, Thailand. IRS-CI also serves as coordinator of the annual Complex Financial Investigations course, which is provided to senior, mid-level, and first-line law enforcement supervisors, inspectors, investigators, prosecutors and customs officers.

In 2002, IRS-CI also presented training on money laundering, identifying and analyzing business and other types of financial records, indirect methods of proof, and tracing the proceeds of crime at U.S. Government-sponsored seminars for financial investigators of the Royal Thai police; prosecutors and national police from the Philippines; leaders from the Jamaican Tax Administration, Jamaican Bankers Association, the Legal Force and the Jamaican Police Organized Crime Units; and judges, prosecutors, investigators, and banking regulators from Macedonia, Albania, Hungary, and Bulgaria.

A regional Money Laundering/Financial Investigative Techniques course was also provided in St. Johns, Antigua to various law enforcement officials from financial investigative units, FIUs, customs, and local police fraud units. The overall goal was to enhance anti-money laundering efforts, foster an atmosphere of cooperation and exchange among these countries and the United States and to provide financial techniques that would be instrumental in combating financial crimes. The participants represented the nine Caribbean nations, two of which are on FATF's NCCT list. Attending were Anguilla, Antigua, Barbados, Dominica, Grenada, Montserrat, St. Kitts and Nevis, St. Lucia, and St. Vincent and the Grenadines. Similar courses were presented to financial investigators, police officers and prosecutors in the Czech Republic and Dar es Salaam, Tanzania.

Country-specific money laundering training was delivered to financial investigators, banking officials, prosecutors, customs agents, revenue agents, bank examiners, judges and police officers in Bogotá, Colombia and Abuja, Nigeria. The overall focus in both countries was to introduce techniques to combat money laundering and to foster cooperation among the local banking regulators, law enforcement officials, prosecutors and the U.S. Government.

IRS-CI assisted in conducting a Money Laundering and Evidence Control Training session sponsored by the Department of Justice in Bridgetown, Barbados. Participants included customs and law enforcement officials, prosecutors, and banking regulators. In particular, IRS-CI provided training on search warrants, its search warrant program, and seized evidence control and custody.

Technical assistance and guidance was provided to the Board of Inland Revenue in Trinidad and Tobago to assist with the design of its new Criminal Investigator Training Program.

Office of the Comptroller of the Currency (OCC)

The OCC supported and sponsored several anti-money laundering training initiatives during 2002. The following highlights the OCC's efforts:

- Presented four sessions of the four-day Anti-Money Laundering School to foreign banking supervisors: one in Barbados, two sponsored by the Asociacion de Supervisores de Bancos de las Americas in Peru and Panama, and one in Washington, D.C.
- Presented an Anti-Money Laundering Training Module in two Bank Examination schools for foreign supervisors in Turkey and the United States.
- Participated in a USAID anti-money laundering training mission to Russia for banking supervisors and industry representatives.

United States Department of Treasury Office of Technical Assistance (OTA)

Treasury's OTA is located within the Office of the Assistant Secretary for International Affairs. The office delivers interactive, advisor-based assistance to senior level representatives in various ministries and central banks in the areas of tax reform, government debt issuance and management, budget policy and management, financial institution reform, and more recently, law enforcement reforms related to money laundering and other financial crimes.

In 1997, the Enforcement Program was added to Treasury's advisory office. It is a long-term, advisor-based program developed out of concern that financial crime, corruption, organized criminal enterprises, and other criminal activities were undermining economic reforms promoted by the U. S. Government (USG). The Enforcement Program focuses on the development of legal foundations, policies, and organizations in three areas: (1) money laundering, terrorist financing and other financial crimes, (2) organized crime and corruption, and (3) the reorganization of law enforcement and financial entities in developing economies to help them prevent, detect, investigate and prosecute complex international financial crime. The Enforcement Program relies on intermittent and resident advisors to deliver its technical assistance. It works with embassy staff and host country clients on long-term projects designed to promote systemic changes and new organizational structures. The program receives funding from the State Department's Bureau for International Narcotics and Law Enforcement Affairs (INL), the State Department Africa Bureau, USAID country missions and direct congressional appropriations.

The Enforcement Program is comprised of a group of approximately 50 experienced advisors with backgrounds in various areas of investigating, prosecuting or regulating financial and economic crimes, such as money laundering, terrorist financing, white-collar crime, organized crime, securities fraud, internal affairs and corruption, criminal law, and organization administration. In 2002, advisors provided assistance to the governments of Albania, Armenia, Azerbaijan, Bosnia, Bulgaria, El Salvador, Guatemala, Hungary, Macedonia, Moldova, Montenegro, Nigeria, Paraguay, Romania, Russia, South Africa, Tanzania, Thailand, Uganda, Ukraine, Honduras, Poland, Serbia and the Eastern Caribbean countries.

OTA conducted several assessments of anti-money laundering regimes in 2002, often working in concert with the U.S. Embassy and/or international bodies. These assessments addressed legislative, regulatory, law enforcement and judicial components of the various programs. The assessments included the development of technical assistance plans to enhance a country's efforts to fight money laundering and terrorist financing. In 2002, such assessments were carried out in Georgia, Montenegro, Peru, Senegal, Ethiopia, Ghana, Guinea, Nicaragua, Bangladesh and Burkina Faso.

Africa

Nigeria. OTA collaborated with the Department of Justice's Overseas Prosecutorial Development, Assistance and Training to provide training to members of Nigeria's nascent Independent Corrupt Practice and Other Related Offenses Commission. The principal objective of the assistance is to strengthen Nigeria's capacity to investigate and prosecute corruption. OTA focused on the legislation and tools used to investigate and prosecute various types of financial crimes, such as money laundering and advanced fee fraud schemes.

Tanzania. An enforcement assessment team visited Tanzania in May 2002. Subsequently, the team completed three working trips, with the cooperation of the U.S. Embassy. A work plan was signed in a public ceremony by the U.S. Ambassador to Tanzania, during a meeting on the fundamentals of money laundering, held for more than 60 high-level government officials and representatives from the business community in Dar es Salaam. The OTA team conducted a seminar that familiarized senior level policy officials with issues of financial crimes and the need for legislation. The team began working with members of the Tanzanian Multi-Disciplinary Committee on Money Laundering, formed to develop anti-money laundering policy, laws, and regulations.

Uganda. An assessment trip to Kampala took place in July 2002. Since then, the Uganda enforcement team completed two additional work trips. OTA is working with a governmental interagency group establishing financial crimes and anti-money laundering policy, procedures and laws. Work has begun on drafting a law to criminalize money laundering. The enforcement team is also working closely with the other Uganda OTA advisors, who work in the Central Bank and in the Capital Markets Authority, to coordinate efforts to strengthen the government's ability to properly supervise financial institutions and markets, and with the IGG (Inspector General for the Government) on strengthening anti-corruption capacity.

Europe

Albania. An OTA advisor assisted the Albanian government in strengthening its asset forfeiture procedures and laws following a request made by the Bank of Albania that had discovered an account of an individual identified by the UN as having links to a terrorist organization.

Bulgaria. Program activities in 2002 included direct assistance to the Bulgarian Financial Intelligence Unit, the Bureau of Financial Intelligence Agency, in the development of its staff, analytic capacity, and information technology resources. The program also focused on the development of amendments to the Bulgarian Law on Measures Against Money Laundering; new legislation to address terrorist financing; and new legislation on asset forfeiture.

Armenia. From 1997 through 2001, OTA provided technical assistance in the areas of financial crimes, organized crime, gaming enforcement, insurance fraud, criminal tax case investigations and prosecutions. Liaison relationships were established between the Organized Crime Department of the Interior Ministry and the international law enforcement community, including federal and state entities in the United States. The Enforcement Team hosted a visit of the Prosecutor General and the Chief of Organized Crime along with members of their staffs, to Washington, D.C. and Los Angeles to further enhance that cooperation. A Financial Crimes Working Group was established.

Azerbaijan. OTA assisted law enforcement officials and regulatory agencies within Azerbaijan to better address financial and economic crimes by developing an improved legal foundation—including regulations and procedures—and to improve training and investigative techniques. The project specifically focuses on money laundering and terrorist financing crimes. In 2002, OTA sponsored a money laundering seminar in Baku, Azerbaijan. The seminar was attended by over 70 Azeri government officials, bankers and businesspeople, and highlighted the need for an effective anti-money laundering regime to fight transnational organized crime and combat groups involved in terrorist financing.

Macedonia. Advisors provided technical assistance regarding the newly implemented amendments to the money laundering law to bank examiners of the National Bank of Macedonia (the Central Bank) and to the compliance officers of the commercial and savings banks.

Moldova. OTA developed and delivered two separate training programs for the National Bank of Moldova and the Bankers Association of Moldova on bank examination procedures and methodologies of detecting and reporting suspicious financial transactions. The OTA team also provided technical assistance in drafting and implementing the Ministry of Finance Tax Law on the establishment of an investigative unit. The team assisted the bank fraud working group in the drafting of anti-fraud amendments to the “bank secrecy” law. Additionally, the team provided specialized forensic training and assistance in implementing the Law on Judicial Examination.

Russia. The current Resident Advisor assisted with the development of the Financial Intelligence Unit, the Financial Monetary Committee.

Asia

Bangladesh. An OTA Advisor participated in a World Bank/ International Monetary Fund-led assessment of Bangladesh’s financial sector, including Bangladesh’s anti-money laundering/anti-terrorist regime. The OTA Enforcement Advisor participated in the reviews of the regulatory systems in place for non-prudentially regulated sectors, specifically, moneychangers and money transmission companies, and the capacity and implementation of criminal law enforcement.

Thailand. In 2002, OTA placed a resident advisor in Bangkok to assist the Anti-Money Laundering Office.

Latin America

El Salvador. In addition to its ongoing assistance to El Salvador, in September 2002 an OTA team provided training to Salvadoran investigators and judges on money laundering concepts and financial analysis units.

Guatemala. OTA provides technical assistance, through the U.S. Embassy, in establishing, staffing and training a new financial analysis unit authorized by the Anti-Money Laundering Law passed in October 2001. In 2002, discussions were held with the governmental agencies on the front line of the anti-money laundering program. Discussions also were held with the National Civilian Police at the National Training Academy to determine the possibility of augmenting the current program of training in the areas of money laundering and financial crimes investigations.

Paraguay. A team of OTA Advisors provided anti-money laundering training to the Government of Paraguay.

Caribbean

In 2002, two resident advisors were placed in Barbados and Port of Spain, Trinidad. Their role is to provide advice on asset forfeiture and the strengthening of anti-money laundering regimes in Eastern Caribbean countries, primarily those countries on FATF’s NCCT list.

Overseas Prosecutorial Development Assistance and Training & the Asset Forfeiture and Money Laundering Section (OPDAT and AFMLS)

Training and Technical Assistance

During 2002, the Justice Department's OPDAT and the AFMLS continued to provide training to foreign prosecutors, judges and law enforcement.

Money Laundering/Asset Forfeiture

The seminars provided by OPDAT and AFMLS enhance 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 seminars varies depending on the specific needs of the participants, but topics addressed in 2002 included developments in money laundering legislation and investigations, the international standards for an anti-money laundering/terrorist financing regime, 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. In 2002, in-depth sessions of this seminar were presented to representatives from Antigua, Armenia, Barbados, Bosnia and Herzegovina, Croatia, Dominica, Georgia, Grenada, Hungary, Macedonia, Mexico, Russia, St. Kitts and Nevis, St. Lucia, St. Vincent, Thailand and United Arab Emirates.

Organized Crime

During 2002, a number of seminars were conducted that dealt with transnational or organized crime. The programs focused on current trends in organized crime, including corruption and money laundering, in each participant country. Topics addressed included how to implement complex financial investigations and special investigative techniques within a task force environment, international standards, legislation, mutual legal assistance, and effective investigation techniques. Seminars were presented to representatives from Azerbaijan, Bosnia and Herzegovina, Georgia, Jamaica, Kazakhstan, Kyrgyzstan, Moldova, Russia, Ukraine and Uzbekistan.

Fraud/Anti-Corruption

In 2002, OPDAT conducted programs on fraud and anti-corruption issues in the Dominican Republic, Mexico, Nigeria, Paraguay and South Africa. The programs covered organization of an anti-corruption unit, prosecutorial strategies, the role and techniques of financial and criminal fraud investigations and /or rules of conduct for police.

Terrorism/Terrorist Financing

OPDAT and AFMLS have intensified their efforts since September 11 to assist countries to develop their legal infrastructure to combat terrorism and terrorist financing. OPDAT and AFMLS, with the assistance of the Counterterrorism Section and 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 and AFMLS work as integral parts of the Interagency Working Group on Terrorist Financing, and in partnership with the Departments of State, Treasury and Commerce, and several other DOJ components.

In 2002, OPDAT, with funding from the Department of State's Anti-Terrorism Assistance Program, organized a number of programs aimed at strengthening counter-terrorism laws abroad. Officials from several regions, including Central Asia, the Middle East, the Caucasus and Russia, Southeast Asia, South Asia, Latin America and Africa, participated in seminars focused on counter-terrorism legislation. The seminars addressed trends in international terrorism, international conventions and agreements, basic investigative tools needed to combat terrorism (e.g., electronic surveillance, wiretaps, undercover operations), methods of financing terrorism, extradition and mutual legal assistance, border security and immigration, export controls, weapons of mass destruction, and model legislation. AFMLS and other U.S. agencies provided instructors for each of the courses. Country groups worked with U.S. experts during the seminar to develop action plans to strengthen their countries' counter-terrorism infrastructures. These programs were presented to representatives from Azerbaijan, Armenia, Bangladesh, Chile, Cote d'Ivoire, Cyprus, Djibouti, El Salvador, Egypt, Georgia, Guatemala, Guyana, India, Indonesia, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Laos, Malaysia, Maldives, Morocco, Nepal, Pakistan, Paraguay, Peru, Philippines, Russia, Sierra Leone, South Africa, Sri Lanka, Tajikistan, Thailand, Turkey, United Arab Emirates and Uzbekistan.

With the assistance of attorneys from AFMLS and the Counterterrorism Section, OPDAT implemented "The Financial Underpinnings of Terrorism Program," which provides intensive seminars covering all aspects of identifying and prosecuting methods of financing terrorism. An initial session for senior policy officials is followed by a longer, more hands-on session for investigators, judges and prosecutors. Officials from the Philippines and Turkey participated in these programs. A day-long roundtable on this topic was held in Washington, D.C. in September 2002 for a Saudi Arabian delegation, and a regional seminar for officials from Brazil, Panama, Paraguay, Argentina and Venezuela took place in December 2002.

OPDAT has organized several conferences at International Law Enforcement Academies (ILEA) relating to terrorism. In Bangkok, in March 2002, OPDAT and the International Criminal Investigative Training Assistance Program (ICITAP) organized a conference to address regional concerns involving terrorism. More than 30 senior criminal justice officials from Brunei, Cambodia, Hong Kong, Indonesia, Laos, Macau, Malaysia, China, Philippines, Singapore, Thailand and Vietnam exchanged views and experiences on tactics used by terrorist groups, anti-terrorism financing measures, and the prospects for regional anti-terrorism cooperation. AFMLS and the Counterterrorism Section supplied instructors. In March 2002, in Budapest, OPDAT organized a regional conference at the ILEA on the subject of money laundering, and AFMLS provided instructors. Issues addressed included international standards for legislation and investigations, the role of the FATF, asset forfeiture, mutual legal assistance and legislation countering money laundering, particularly as it relates to terrorist financing. Thirty-eight senior government officials from Azerbaijan, Georgia, Kazakhstan, Moldova, Russia and Ukraine attended. In Budapest, in June 2002, OPDAT organized a second conference at the ILEA to address regional approaches to investigating and prosecuting organized crime, with a large portion of the discussion focusing on money laundering and asset forfeiture, focusing on terrorist financing and international cooperation. Fifty prosecutors, investigators and criminal justice officials from Azerbaijan, Georgia, Kazakhstan, Moldova, Russia, Ukraine and Uzbekistan attended.

In July 2002, OPDAT's representative to the Southeastern European Cooperative Initiative Center in Bucharest, Romania, helped to organize a workshop on the relationship between terrorism and organized crime. The workshop helped advance regional sharing of intelligence on the organized crime groups that facilitate the objectives of terrorism. Participants developed "best practices" and produced a regional action plan on operations to address the connection between organized crime and terrorism.

AFMLS organized and conducted a regional conference on the financing of terrorism in London in September 2002. This conference brought together 50 prosecutors and law enforcement officials from the United States, the United Kingdom, UAE, Germany, Pakistan, France, and Turkey.

AFMLS provides technical assistance in connection with legislative drafting on all matters involving money laundering, asset forfeiture and the financing of terrorism. During 2002, AFMLS provided such

assistance to 26 countries, including the drafting of a model money laundering, asset forfeiture and terrorist financing law. In 2002, AFMLS assisted Pakistan, Indonesia, Philippines, Marshall Islands, El Salvador, Paraguay, Bulgaria, Georgia, Kazakhstan, Ukraine, Russia, Kosovo, St. Kitts and Nevis, and Thailand. OPDAT provided similar guidance to Azerbaijan.

AFMLS has participated in the Financial Systems Assessment Team (FSAT) led by the Department of State's Coordinator for Counterterrorism Office and the Bureau for International Narcotics and Law Enforcement Affairs.

United States Customs Service/Operation Green Quest

The U.S. Customs Service (Customs) and its Operation Green Quest are extensively involved in multi-agency international money laundering and financial-related terrorism training programs. Drawing on their expertise in undercover drug money laundering, as well as in traditional money laundering techniques related to all types of criminal activity, Customs and Operation Green Quest strive to impart their broad experience to law enforcement, the regulatory and trade communities, and banking officials of all jurisdictions.

Operation Green Quest's goal is to assist foreign/domestic agencies to develop the knowledge, skills and abilities needed to strengthen and coordinate terrorist-related financial investigative activities. Operation Green Quest also will benefit from providing training by furthering effective regional cooperation in attacking transnational financial terrorist crimes, particularly financial crimes relating to money laundering in support of terrorist entities; strengthening regional law enforcement; and enhancing the banking and trade communities' efforts in activities having an impact on the United States.

The Financial Terrorist Investigations Training seminar is intended as an introduction to international money laundering linked to terrorism. The seminar is focused on providing the necessary skills to policy makers, law enforcement personnel, and management officials of financial institutions so that they can recognize and combat money laundering by terrorists. This course is specifically designed to address terrorism, its relationship to money laundering issues, and country-specific problems. The training program addresses many of the same topics as the more generalized Customs training, but focuses the discussions on the relationship between money laundering techniques and terrorist financing. Charities and alternative remittance systems are also covered, and specifically their use by terrorists. Reinforced through the use of interactive exercises, students learn techniques used to recognize and investigate terrorist-related money laundering.

Operation Green Quest conducted the Financial Terrorist Investigation seminars domestically and abroad for officials from various nations, including Armenia, Australia, Azerbaijan, Barbados, China, Cyprus, Dominican Republic, Egypt, Georgia, Guyana, Hungary, Jordan, Kazakhstan, Kyrgyzstan, Morocco, Pakistan, Philippines, Russia, St. Kitts and Nevis, Suriname, Tajikistan, Thailand, Trinidad, Turkey, United Arab Emirates and Uzbekistan.

Customs also provides training that addresses the trends and patterns concerning money laundering and international banking, focusing on issues relating to transnational money laundering. The seminars cover the use of free trade zones, offshore banking practices, international monetary flows, bulk-cash and electronic funds transfers, and capital flight. Specialized sessions address the black market peso exchange system, the Money Laundering Coordination Center, and/or an overview of Operation Green Quest. The course addresses both the investigation and prosecution stages of money laundering.

United States Secret Service

The Secret Service continues to send instructors to the International Law Enforcement Academies (ILEA) in Budapest, Hungary, Bangkok, Thailand and Gaborone, Botswana; providing training and strategies to foreign police representatives in the detection of counterfeit U.S. currency and fraud schemes.

The Secret Service's continued presence overseas and the training provided through the ILEAs are paramount in ongoing United States efforts to suppress and seize the ever increasing amount of foreign-produced counterfeit U.S. currency being sold, shipped and trafficked into this, and other, countries throughout the world. The Secret Service estimates that nearly 50 percent of all counterfeit U.S. currency passed in the United States originated overseas. The Secret Service's established relationship with the counterfeit suppression program has generated training at the ILEA sites.

Bilateral overseas development includes training and education for law enforcement prosecutors and financial officials. Added benefits include deterrence, intelligence gathering and education regarding the organized criminal networks involved in transnational crime. An integral part of the Secret Service's efforts in this area is the Combating Economic Fraud and Counterfeiting Seminar. In 2002, this seminar was offered to representatives from Trinidad, Bulgaria, Romania, Macedonia, Turkey, Dominican Republic, and Bulgaria.

Treaties, Agreements, and Other Mechanisms for Information Exchange

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 United States 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, Brazil, Canada, Cyprus, Czech Republic, Dominica, Egypt, Estonia, France, Grenada, Greece, Hong Kong SAR, Hungary, Israel, Italy, Jamaica, Latvia, Lithuania, Luxembourg, Mexico, Morocco, the Netherlands, 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 ratified by the United States but not yet brought into force with the following countries: Belize, Colombia, Cyprus, India, Ireland, Liechtenstein, Nigeria, 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 China (PRC) and Nigeria. The American Institute in Taiwan and the Taipei Economic and Cultural Representative Office in the United States have a mutual legal assistance agreement in force.

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, and Mexico.

Financial Information Exchange Agreements (FIEAs) facilitate the exchange of currency transaction information between the U.S. Treasury Department and other finance ministries. The United States has FIEAs with Colombia, Ecuador, Mexico, Panama, Paraguay, Peru, and Venezuela. Treasury's Financial Crimes Enforcement Network (FinCEN) has memoranda of understanding or an exchange of letters in place with other Financial Intelligence Units to facilitate the exchange of information between FinCEN

and the country's Financial Intelligence Unit. FinCEN has an MOU or an exchange of letters with the FIUs in Argentina, Australia, Belgium, France, Netherlands, Slovenia, Spain, and the United Kingdom.

Asset Sharing

Pursuant to the provisions of the 1988 U.S. law, 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 law enforcement. The long-term goal has been to encourage governments to improve asset forfeiture laws and procedures, so that 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, Switzerland and the United Kingdom have shared forfeited assets with the United States.

From 1989 through December 2002, the international asset sharing program, administered by the Department of Justice, resulted in the net forfeiture in the United States of \$404,196,504.61 of which \$178,789,015.71 was shared with foreign governments that cooperated and assisted in the investigations. In 2002, the Department of Justice transferred forfeited proceeds to: Canada (\$546,058.14); Greece (\$2,267,959.05); Luxembourg (\$686,842.66); Switzerland (\$4,035,060.00); and Turkey (\$264,846.42). Prior recipients of shared assets (1989-2001) include: Anguilla, Argentina, the Bahamas, Barbados, British Virgin Islands, Canada, the Cayman Islands, Colombia, Costa Rica, Dominican Republic, Ecuador, Egypt, Guatemala, Guernsey, Hong Kong, Hungary, Isle of Man, Israel, Liechtenstein, Luxembourg, Netherlands Antilles, Paraguay, Romania, South Africa, Switzerland, the United Kingdom and Venezuela.

From FY1994 through FY2002, the international asset sharing program, administered by the Department of Treasury, shared \$23,329,648.00 with foreign governments that cooperated and assisted in the investigations. In FY2002, the Department of Treasury transferred forfeited proceeds to: Cayman Islands (\$9,061.00); Canada (\$686,863.00); China (\$216,555.00); Isle of Man (\$300,802.00); Mexico (\$843,388.00); and the Netherlands (\$64,407.00). Prior recipients of shared assets (1995-1999) include: Aruba, the Bahamas, the Dominican Republic, Egypt, Guernsey, Honduras, Jersey, Nicaragua, Panama, Portugal, Qatar, Switzerland and the United Kingdom.

Multilateral Activities

United Nations

United Nations Security Council Resolutions

Several UN Security Council Resolutions (UNSCR) 1267/1390/1455 require UN Member States to implement certain measures—namely, asset freezing, travel restrictions, and an arms embargo—against individuals and entities that are related to Usama Bin Ladin, and members of al-Qaida and the Taliban, and those associated with them. The UN 1267 Sanctions Committee maintains a consolidated list, regularly updated, of such individuals and entities, against which Member States are required to impose the measures. UNSCR 1452 allows for limited exceptions to the asset freeze provisions under certain circumstances. A Monitoring Group reports to the UN 1267 Sanctions Committee on the implementation of the resolutions.

United Nations Security Council Resolution 1373

On September 28, 2001 the United Nations Security Council adopted Resolution 1373 (UNSCR 1373) concerning terrorism. UNSCR 1373 requires States to take certain specified measures to combat terrorism. Among other things, it requires States: to freeze without delay funds, financial assets or other economic resources of persons who commit, attempt to commit, facilitate or participate in the commission of terrorist acts; to prohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or other related services available—directly or indirectly—for the benefit of persons who commit, attempt to commit, facilitate or participate in the commission of terrorist acts; to ensure that terrorist acts are established as serious criminal offenses in domestic laws and regulations and that punishment duly reflects the seriousness of such terrorist acts; to deny safe haven to those who finance, plan, support or commit terrorist acts; and to ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts is brought to justice. The Resolution calls upon States to exchange information and cooperate to prevent the commission of terrorist acts.

UNSCR 1373 established a Committee, the UN Counter-Terrorism Committee (CTC), to monitor implementation of the resolution and to receive reports from States on steps they have taken to implement the resolution. To facilitate this reporting, the Committee sent out a self-assessment questionnaire. By year-end 2002, 181 of the UN's 191 Member States had submitted reports to the CTC.

UN International Convention for the Suppression of the Financing of Terrorism

On December 9, 1999, the United Nations General Assembly adopted the International Convention for the Suppression of the Financing of Terrorism. It was opened for signature from January 10, 2000 to December 31, 2001. This Convention requires parties to criminalize the provision or collection of funds with the intent that they be used, or in the knowledge that they are to be used, to conduct certain terrorist activity. Article 18 of the Convention requires states parties to cooperate in the prevention of terrorist financing by adapting their domestic legislation, if necessary, to prevent and counter preparations in their respective territories for the commission of offenses specified in Article 2. To that end, Article 18 encourages implementation of numerous measures also included among the FATF's Forty Recommendations on Money Laundering. These measures, which states parties may implement at their discretion, include: prohibiting accounts held by or benefiting people unidentified or unidentifiable; verifying the identity of the real parties to transactions; and requiring financial institutions to verify the existence and the structure of the customer by obtaining proof of incorporation.

The Convention also encourages states parties to obligate financial institutions to report complex or large transactions and unusual patterns of transactions that have no apparent economic or lawful purpose, without incurring criminal or civil liability for good faith reporting; to require financial institutions to maintain records for five years; to supervise (for example, through licensing) money-transmission agencies; and to monitor the physical cross-border transportation of cash and bearer-negotiable instruments. Finally, the Convention addresses information exchange, including through the International Criminal Police Organization (Interpol). As of December 31, 2002, 64 states had become parties to the Convention; 75 other states had signed, but not ratified, the Convention. It entered into force internationally on April 9, 2002. The United States became a party to the Convention on June 26, 2002.

UN Convention Against Transnational Organized Crime

The UN Convention against Transnational Organized Crime (Convention), signed by 125 countries including the United States at a high-level signing conference December 12-14, 2000 in Palermo, Italy, is the first legally binding multilateral treaty specifically targeting transnational organized crime. Two supplemental Protocols addressing trafficking in persons and migrant smuggling were also signed by many countries in Palermo. Each instrument will enter into force on the ninetieth day after the 40th state deposits an instrument of ratification, acceptance, approval or accession. As of the end of 2002, 147 countries had signed the convention and 28 countries had deposited instruments of ratification.

The Convention takes aim at preventing and combating transnational organized crime through a common toolkit of criminal law techniques and international cooperation. It requires states parties to have laws criminalizing the most prevalent types of criminal conduct associated with organized crime groups, including money laundering, obstruction of justice, corruption of public officials and conspiracy. The article on money laundering regulation requires parties to institute a comprehensive domestic regulatory and supervisory regime for banks and financial institutions to deter and detect money laundering. The regime will have to emphasize requirements for customer identification, record keeping and reporting of suspicious transactions.

The Financial Action Task Force

The Financial Action Task Force on Money Laundering (FATF), established at the G-7 Economic Summit in Paris in 1989, is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering.

The FATF was given the responsibility of examining money laundering techniques and trends, evaluating counter-money laundering measures, and recommending measures still needed. In 1990, FATF issued Forty Recommendations on Money Laundering. These recommendations are designed to prevent proceeds of crime from being utilized in future criminal activities and from affecting legitimate economic activity. Revised in 1996 to reflect changes in money laundering patterns, the recommendations are currently undergoing another revision, scheduled to be completed by June 2003, to reflect new trends in money laundering.

FATF monitors members' progress in implementing anti-money laundering measures, reviews money laundering techniques and counter-measures, and promotes the adoption and implementation of anti-money laundering measures globally. In performing these activities, FATF collaborates with other international bodies.

In June 2000, membership of the FATF expanded from 26 to 29 jurisdictions and two regional organizations, representing the major financial centers of North America, Europe and Asia. The delegations of the FATF's members are drawn from a wide range of disciplines, including experts from the Ministries of Finance, Justice, Interior and External Affairs; financial regulatory authorities; and law enforcement agencies.

FATF focused on several major initiatives during 2002:

Non-Cooperative Countries and Territories Exercise

In response to the G-7 Finance Ministers 1998 Birmingham Summit, FATF formally created the Ad Hoc Group on Non-Cooperative Countries and Territories (NCCT). In 1999, this group developed 25 criteria by which to determine those jurisdictions undermining the global effort to combat money laundering. These criteria encompass four broad areas:

- Loopholes in financial regulations
- Obstacles raised by other regulatory requirements
- Obstacles to international cooperation
- Inadequate resources for preventing and detecting money laundering activities

FATF initiated its review process with a limited number of jurisdictions in February 2000. Based on this process, FATF identified fifteen jurisdictions as non-cooperative in the international fight against money laundering at its June 2000 Plenary.

In deciding whether a jurisdiction should be removed from the NCCT list, the FATF Plenary must be satisfied that the jurisdiction has addressed the previously identified deficiencies. The FATF relies on its collective judgment, and attaches particular importance to reforms in the areas of criminal law, financial supervision, customer identification, suspicious activity reporting, and international co-operation. As necessary, legislation and regulations must have been enacted and have come into effect before removal from the list can be considered. In addition, the FATF seeks to ensure that the jurisdiction is implementing the necessary reforms. Thus, information related to institutional arrangements, the filing and utilization of suspicious activity reports, examinations of financial institutions, and the conduct of money laundering investigations, is considered.

Throughout 2002, the FATF monitored the progress made by NCCTs to address deficiencies and implement corrective measures. In June 2002, four jurisdictions, Hungary, Israel, Lebanon, and St. Kitts and Nevis, were removed from the NCCT list. The FATF also published its third NCCT Review. In October 2002, the FATF again removed four countries from the NCCT list: Dominica, Marshall Islands, Niue and Russia. At the same time, it decided to recommend that its members impose counter-measures on Nigeria and Ukraine starting December 15, 2002, unless the two countries took immediate steps to remedy deficiencies previously identified by the FATF. Ultimately Nigeria took actions sufficient to avoid counter-measures, while on December 20, 2002, FATF again called for the imposition of counter-measures against Ukraine. FATF subsequently called for the removal of countermeasures against Ukraine at its February 2003 plenary because it had passed the necessary amendments to its anti-money laundering law.

Revision of the FATF Forty Recommendations on Money Laundering

The FATF Forty Recommendations on Money Laundering represent the international standard for counter-money laundering regimes. They cover such areas as regulatory, supervisory, and criminal law, as well as international cooperation.

Money laundering methods and techniques change as new measures to combat money laundering are implemented and new technologies are developed. Therefore, in 2001, FATF embarked on another review of the FATF Forty to ensure that they were up-to-date. In May 2002, FATF released a consultation document in order to obtain comments from countries, international organizations, the financial sector and other interested parties. The FATF identified a number of areas where possible changes could be made to the FATF framework, broadly including customer due diligence and suspicious transaction reporting, beneficial ownership and control of corporate vehicles, and the application of anti-money laundering obligations to non-financial businesses and professions. A revised set of the Forty Recommendations on Money Laundering is expected in June 2003.

Combating Terrorist Financing

In response to September 11, FATF expanded its mission beyond money laundering to focus its energy and expertise on the worldwide effort to combat terrorist financing. During an extraordinary plenary meeting in Washington, DC on October 29-30, 2001, FATF agreed to Eight Special Recommendations on Terrorist Financing. These Special Recommendations now represent the international standards in this area. The recommendations are reprinted in the Appendix to this report.

The first phase of FATF's self-assessment exercise for the Eight Special Recommendations—that is, the collection and preliminary analysis of relevant data for FATF members—was completed and the results published by the FATF Plenary in June 2002. FATF then called on non-FATF members to take part in the self-assessment process beginning in February 2002. As of December 2002, 95 non-FATF countries have completed the self-assessment exercise.

In order to secure the swift and effective implementation of these new standards, FATF has developed a best practices paper on combating the abuse of non-profit organizations (www.fatf-gafi.org/pdf/SR8-NPO_en.pdf). FATF will also issue Interpretive Notes on Special Recommendations VI (alternative remittance) and VII (wire transfers) in 2003.

In June 2002, FATF initiated a process to identify jurisdictions that lack appropriate measures to combat terrorist financing and is working with the UNCTC, the UN Global Programme Against Money Laundering PML, International Financial Institutions (IFIs), and FATF style regional bodies (FSRBs) to coordinate the delivery of technical assistance to such jurisdictions.

Charities

This year, the United States and the international community devoted more time and resources to combating the abuse of charitable organizations by terrorists, and achieved some noteworthy successes. One key step forward was taken by FATF, when it adopted and disseminated a paper outlining international best practices for combating the abuse of non-profit organizations. These suggestions go far toward setting international standards for encouraging greater transparency in the financial, programmatic, and administrative practices of organizations that raise funds from donors. In addition, the United States has issued best practice guidelines to provide guidance for U.S. charities and donors about how to protect their organizations and donations from being diverted to support terrorism.

FATF, the IMF, and the World Bank

Money laundering and the financing of terrorism are worldwide concerns that increase the risks to domestic and global financial systems and can impact national security. In the wake of the events of September 11, 2001, the international community adopted a broad and comprehensive agenda to address both. As an important part of that effort, the IFIs agreed to take on an enhanced role in the global fight against money laundering and the financing of terrorism.

At the 2001 Annual Meeting of the IMF and World Bank in November 2001, the United States and other nations stressed the importance of integrating anti-money laundering and counter-financing of terrorism (AML/CTF) issues into the IFIs' financial sector assessment, surveillance and diagnostic activities. There was increased recognition of the need for the IMF and World Bank to increase their involvement in strengthening financial regulatory frameworks and to provide technical assistance to authorities on AML/CTF issues. A number of nations stressed the importance of a collaborative effort between the FATF and the IFIs in this effort.

Significant progress was made toward meeting these objectives during 2002. The IMF and World Bank are now including assessments of members' AML/CTF regimes in the course of their Financial Sector Assessment Program (FSAP) reviews and in other aspects of their engagement with members. The IMF and Bank collaborated closely with the FATF, other international standard setters (the Basel Committee of Banking Supervisors, the International Association of Insurance Supervisors, and the International Organization of Securities Commissions), and the Egmont Group of Financial Intelligence Units to develop a comprehensive and unified methodology for measuring countries' implementation of AML/CTF principles, based on the FATF Forty Recommendations on Money Laundering and the FATF Eight Special Recommendations on Terrorist Financing.

In the fall of 2002, the FATF membership endorsed, and the IMF and World Bank Executive Boards approved use of the comprehensive methodology to assess member compliance with AML/CTF principles. As an integral part of the enhanced program, the Executive Boards of the IMF and World Bank approved a twelve-month pilot project to assess members' compliance with AML/CTF principles in participation with FATF and FATF-style regional bodies. The pilot project adds the FATF Forty Recommendations on Money Laundering and the FATF Eight Special Recommendations on Terrorist Financing (the FATF 40 + 8) to the list of areas and associated standards and codes that are incorporated into the operational work of the IMF and the World Bank. The United States and other G-7 members have volunteered to be assessed using the new AML/CTF methodology.

FATF 2002-2003 Typologies Exercise

FATF conducted its annual typologies exercise (November 19-20, 2002, in Rome, Italy) to identify current and emerging methods, trends, and patterns in money laundering and terrorist financing, and to discuss effective counter-measures. This year's exercise focused on terrorist financing; money laundering vulnerabilities in the securities sector; the links between money laundering and terrorist financing and the diamond, gold and precious metals trades; and contrasting methods used for money laundering and fiscal offenses.

FATF-Style Regional Bodies (FSRBs)

Asia/Pacific Group on Money Laundering

The Asia/Pacific Group on Money Laundering (APG) is comprised of 25 members from South Asia, Southeast Asia, East Asia and the South Pacific. Australia, Bangladesh, Chinese Taipei, Cook Islands, Fiji Islands, Hong Kong China, India, Indonesia, Japan, Korea (Republic of), Macau China, Malaysia, Marshall Islands, Nepal, New Zealand, Niue, Pakistan, Palau, Philippines, Samoa, Singapore, Sri Lanka, Thailand, United States of America and Vanuatu are APG members. There are also thirteen observer jurisdictions and thirteen observer international and regional organizations

The APG's mission is to contribute to the global fight against money laundering, organized crime and terrorist financing by enhancing anti-money laundering and anti-terrorist financing measures in the Asia/Pacific region.

Major achievements during the year include the following: a further expansion of APG membership with the addition of Nepal, the Marshall Islands, and Palau; the completion of five mutual evaluations (Malaysia, Cook Islands, Fiji, Indonesia and Thailand); further expansion of the APG's work in the area of technical assistance and training; a successful typologies meeting in October in Vancouver, Canada; and, with the assistance of the Asian Development Bank, the launch of a comprehensive APG website (www.apgml.org).

The Fifth Annual Meeting of the APG, held at Brisbane, Australia in June 2002 was quite successful. The meeting was the largest APG meeting to date. The Plenary reached agreement on a range of issues, including revised Terms of Reference (to include a formal commitment to combat the financing of terrorism), the adoption of the five mutual evaluation reports, discussion of the current review of the FATF's Forty Recommendations on Money Laundering and consideration of technical assistance and training outcomes and priorities for the next few years. Outcomes of the meeting included further expansion of the APG's work in the area of technical assistance and training and a Special Forum on Technical Assistance and Training. It was further decided at this meeting that the Republic of Korea would assume the rotating Co-Chair position for two years when Malaysia's term expired. The new Commissioner of the Korea Financial Intelligence Unit, Mr. Gyu-Bok Kim, is now the co-chair.

At the June Annual Meeting, members adopted a revised mission statement and a number of goals as a part of its strategic plan. The APG wants to develop a better understanding of the nature, extent and impact of money laundering in the region, and expand regional awareness of money laundering issues and the role of the APG. The APG intends to identify, agree on, oversee and facilitate implementation of comprehensive anti-money laundering measures appropriate for each jurisdiction in the region, which will include the facilitation and coordination of technical assistance. Finally, the APG plans to facilitate the implementation of the FATF Special Eight Recommendations on Terrorist Financing and the relevant United Nations instruments in all member jurisdictions. The revised mission statement and goals contained in the APG's Strategic Plan July 2001 to June 2004 build on the APG's Strategic Plan 1999 to 2001 and recognize in particular the importance of combating terrorist financing.

Additional outcomes and highlights of the Annual Meeting included:

The presentation of a significant new study on the Negative Effects of Money Laundering on Economic Development; consideration of a draft First Yearly Report on money laundering trends and methods in the region; a detailed discussion of the current review of the FATF Forty Recommendations on Money Laundering and the APG's further input into that process; a discussion of possible areas where regional anti-money laundering measures might be explored in the future, including underground banking/alternative remittance systems, information sharing and the implications of the cash economy; and progress reports from the five previously evaluated jurisdictions—Vanuatu, Samoa, Macau, China, Labuan IOFC and Chinese Taipei.

The APG has an ambitious 2002-03 work program. Among other goals, the APG intends to conduct a number of new mutual evaluations, including South Korea, the Philippines and Bangladesh; coordinate and deliver increased technical assistance and training; contribute to the review of the FATF Forty Recommendations on Money Laundering and subsequently assist with implementation; increase anti-terrorist financing activities; continue work by the APG Working Group on Alternative Remittance and Underground Banking Systems and the APG Working Group on Information Sharing; conduct the Sixth Annual Meeting in Manila in May 2003; and continue to cooperate with related organizations and bodies, including the FATF, other regional anti-money laundering bodies, international and regional financial institutions, the UN Global Programme Against Money Laundering, Interpol, the World Customs Organization, the Commonwealth Secretariat and the Pacific Islands Forum Secretariat.

Caribbean Financial Action Task Force

The Caribbean Financial Action Task Force (CFATF), comprised of 29 jurisdictions, continues to advance its anti-money laundering initiatives within the Caribbean basin. CFATF members include Anguilla, Antigua and Barbuda, Aruba, Commonwealth of the Bahamas, Barbados, Belize, Bermuda, the British Virgin Islands, the Cayman Islands, Costa Rica, Dominica, the Dominican Republic, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Montserrat, the Netherlands Antilles, Nicaragua, Panama, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname, Trinidad and Tobago, Turks and Caicos Islands, and Venezuela. Members of the CFATF subscribe to a Memorandum of Understanding (MOU) that delineates the CFATF's mission, objectives, and membership requirements. All members are required to make a political commitment to adhere to and implement the FATF Forty Recommendations on Money Laundering, the FATF Special Eight Recommendations against Terrorist Financing, as well as the CFATF's additional 19 Recommendations, and to undergo peer review in the form of mutual evaluations to assess their level of implementation of the recommendations. Members are also required to contribute to the CFATF budget and to participate in the activities of the body.

In October 2002, Guatemala, Guyana, and Honduras became full Members of the CFATF, increasing its membership to 29 governments. Also, in October 2002, Alfred Sears, Attorney General and Minister of Education of The Bahamas, assumed Chairmanship of the CFATF.

In July 2001, the CFATF initiated its second round of mutual evaluations, focused on the effective implementation of the FATF and CFATF Recommendations, as well as the FATF's NCCT 25 criteria. In October 2002, the CFATF's Council of Ministers adopted six mutual evaluation reports—on The Bahamas, Cayman Islands, Costa Rica, Dominican Republic, Panama, and Trinidad and Tobago. Mutual evaluation reports on Antigua and Barbuda, Barbados, and the Turks and Caicos Islands, for which on-site visits were conducted during 2002, will be presented and discussed at Plenary XVII in Panama during March 2003. The CFATF plans to conduct workshops for mutual evaluation examiners during 2003, and annually thereafter.

The CFATF has established an initiative to compile annual country reports on each member to assess compliance with the international anti-money laundering and counter-terrorist financing standards. This project is intended to complement the Mutual Evaluation Program and enhance the CFATF's monitoring capacity. The first set of country reports was drafted during 2002 and is expected to be adopted and published during 2003.

In April 2002, the CFATF and GAFISUD conducted a joint two-day typologies exercise in Trinidad and Tobago, focused on terrorist financing and economic citizenship programs (ECPs). During this exercise, 27 presenters from 13 countries and six international organizations shared expertise focused on detecting and combating terrorist financing, as well as on criminal abuse of ECPs.

During the April 2002 CFATF Plenary meeting, CFATF members considered both the FATF Eight Special Recommendations on Terrorist Financing and the associated Self-Assessment Questionnaire (SAQTF). In October 2002, the Council of Ministers endorsed the FATF Eight Special Recommendations, agreed to extend the CFATF mandate to include terrorism and terrorist financing, as well as to participate in the FATF global self-assessment exercise, and to extend the remit of the CFATF Secretariat to facilitate the provision of technical assistance and training relative to terrorist financing to Members. The majority of CFATF member governments have now fully participated in the FATF global assessment.

Council of Europe Moneyval

Formerly known by the French acronym, PC-R-EV (Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures), Moneyval is a FATF-style regional body that includes within its membership those Council of Europe member states that are not members of the FATF. Moneyval members include Albania, Andorra, Armenia, Azerbaijan, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Georgia, Hungary, Latvia, Liechtenstein, Lithuania, Malta, Moldova, Poland, Romania, the Russian Federation, San Marino, Slovakia, Slovenia, Former Yugoslav Republic of Macedonia, and Ukraine. Moneyval aims to encourage legal, financial and punitive measures among its members that are in line with international standards. To accomplish this, it relies on a system of mutual evaluations and peer pressure.

In 2002, Moneyval continued its second round of mutual evaluations and began a first round of evaluations for new members. The second round of mutual evaluations, covering 22 jurisdictions, will run through December 2003. Reports for Slovenia, Cyprus, and the Czech Republic were discussed and adopted at the 9th plenary meeting of Moneyval in June 2002. At its 10th plenary meeting in December 2002, mutual evaluation reports on Hungary and Andorra were discussed and adopted. Consideration of reports on Slovakia and Malta were postponed for technical reasons until 2003. First round evaluation visits took place in Monaco (October) and Azerbaijan (December) during 2002.

Moneyval agreed at its June 2002 Plenary to apply certain compliance enhancing measures with regard to four member countries lacking sufficient anti-money laundering regimes. Under these special procedures, Moneyval's actions will range from requiring regular reporting to the delivery of high-level warnings. Moneyval's plenary sessions will examine progress by the affected countries, each of which will be monitored closely to ensure that deficiencies in the jurisdiction are addressed.

Like the FATF, Moneyval has taken on additional responsibilities in the area of counter-terrorist financing. In the first half of 2002, the Council's European Committee on Crime Problems revised Moneyval's terms of reference to specifically include the issue of financing terrorism. The new text recognizes the FATF Special Eight Recommendations on Terrorist Financing as international standards and authorizes the evaluation of the performance of Moneyval member states in complying with these standards. By December 2002, 21 out of 24 member states had submitted their self-assessment questionnaires on terrorist financing.

A significant accomplishment of 2002 involved convening the 3rd Moneyval Training Seminar, which took place in Paphos, Cyprus in November 2002. This was a first joint training session for Moneyval and GRECO (the Council's anti-corruption committee) mutual evaluators. Hosted by the Government of Cyprus and its Financial Intelligence Unit, there were general as well as parallel sessions for the Moneyval and GRECO evaluators focusing on the conduct of their respective assessments.

Moneyval is currently discussing with two member States the modalities of a comprehensive technical assistance program to be funded by the European Commission. In addition, it had organized a round-table at its June 2002 plenary meeting on technical assistance needs in the area of counter-terrorist financing and subsequently has forwarded a list of suggested activities to the World Bank for dissemination among potential donor states.

Eastern and Southern African Anti-Money Laundering Group (ESAAMLG)

ESAAMLG was launched at a meeting of ministers and high-level representatives in Arusha, Tanzania, in August 1999 and held its first meeting in April 2000. The group maintains its Secretariat in Dar es Salaam, Tanzania. Its member countries are: Kenya, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, and Uganda. Botswana, Lesotho, Zambia, and Zimbabwe are invited to ESAAMLG meetings, but are not considered full members because they have not yet signed the Memorandum of Understanding. The United States, United Kingdom, Commonwealth Secretariat, United Nations, and World Bank serve as cooperating nations and organizations. In February 2003, a new Executive Secretary is expected to take office.

The most recent annual meeting of the ESAAMLG's Ministers and senior officials was held in August 2002, in Mbabane, Swaziland. The Ministers endorsed the group's work program for 2003, which includes a mandate to begin the mutual evaluation process. Six countries—Mauritius, Swaziland, Lesotho, South Africa, Mozambique, and Namibia—volunteered to be evaluated during the first round. Mutual evaluation training is scheduled for January 2003, and the first two evaluations are to take place soon after. Also at the August plenary, Swaziland assumed the one-year presidency of ESAAMLG.

In October 2002, a mentor selected by the United Nations Global Programme against Money Laundering began a two-year assignment advising the ESAAMLG Secretariat in Dar es Salaam.

The ESAAMLG has also launched a self-assessment exercise vis-à-vis the FATF Forty Recommendations on Money Laundering and the Eight Special Recommendations on Terrorist Financing. Thus far, seven member countries have completed the exercise on the Forty Recommendations and five on the Special Eight. A full report on the self-assessments will be submitted at the next Plenary in March 2003.

Financial Action Task Force Against Money Laundering in South America (GAFISUD)

The Memorandum of Understanding establishing the South American Financial Action Task Force, (Grupo de Acción Financiera de Sudamerica Contra el Lavado de Activos-GAFISUD) was signed on December 8, 2000 by nine member states: Argentina, Bolivia, Brazil, Colombia, Chile, Ecuador, Peru, Paraguay, and Uruguay. Mexico, Portugal, Spain, the United States, the Inter-American Development Bank, the International Monetary Fund, the United Nations Office for Drug Control and Crime Prevention, and the World Bank have joined GAFISUD as cooperating and supporting observer members (PACOS). In addition, the Organization of American States' Inter-American Drug Abuse Control Commission (OAS/CICAD) is a special advisory member of GAFISUD. GAFISUD is a FATF-style regional body committed to the adoption and implementation of the FATF Forty Recommendations on Money Laundering. GAFISUD's mission also includes member self-assessment and mutual evaluation programs. Headquarters and a permanent Secretariat have been officially established in Buenos Aires, Argentina, and Uruguay has offered a training center as a permanent training venue for GAFISUD.

Colombia was elected as the first President of the organization for a one-year term and served additionally as the provisional Executive Secretariat. At the fourth Plenary in Santiago, Chile in December 2001, the presidency was turned over to Chile's Minister of the Interior. The Plenary also resulted in the adoption by GAFISUD of the FATF Eight Special Recommendations on Terrorist Financing. GAFISUD is now preparing a regional study to facilitate proper implementation of the FATF Special Eight Recommendations.

At the May 2002 Plenary in Buenos Aires, GAFISUD finalized and adopted Mutual Evaluation Reports for Colombia and Uruguay. Additionally, GAFISUD circulated a draft Action Plan to Counter Terrorism that proposed, among other things, the adoption and ratification of the FATF Special Recommendations Against Terrorism. As a prelude to final adoption of this plan, GAFISUD initiated a self-evaluation exercise to determine current levels of compliance by GAFISUD members with these recommendations.

At the December 2002 Plenary in Montevideo, Uruguay was elected to assume the Presidency of GAFISUD. In addition, the Plenary finalized and adopted the FATF Mutual Evaluation Reports on Argentina and Brazil, formally adopted the May Action Plan to Counter Terrorism, and agreed to use the new FATF/World Bank/IMF FSAP methodology, which includes assessments of counter-terrorist financing programs, for the second round of mutual evaluations of its membership.

GAFISUD has also been increasingly active in training and technical assistance. In April 2002, GAFISUD and CFATF organized a joint two-day typologies exercise in Trinidad and Tobago. This unprecedented exercise focused on terrorist financing and 27 presenters from 13 different countries and six international organizations shared their knowledge on defending the Americas from terrorist financiers.

Since the December 2001 Plenary, GAFISUD made a commitment to coordinate training activities in the region. Towards that end, GAFISUD participated in a Technical Assistance Coordination meeting in April 2002 hosted by the World Bank/IMF. Seminars and workshops coordinated for the region in 2002 included a second seminar for mutual evaluators, a forum for coordination and information exchange within national anti-money laundering regimes, and a seminar for FIUs.

In September 2002, GAFISUD, with funding provided by the Inter-American Development Bank, organized and conducted a three-day training session for experts who will conduct mutual evaluation exercises. This session, held in Montevideo, Uruguay, included three experts (legal, bank regulatory and law enforcement) from each GAFISUD member country.

The Plenary adopted a far-reaching training work plan for 2003 that will focus on enhancing legislation to more broadly permit the use, with appropriate safeguards, of special investigative techniques such as the use of informants, under cover operations, task forces, and electronic surveillance as well as advanced training for financial investigators.

Inter-Governmental Action Group against Money Laundering (GIABA)

The Heads of State and Government of the Economic Community of West African States (ECOWAS) established GIABA in December 1999. GIABA's first meeting was held in Dakar, Senegal, in November 2000. Members include: Benin, Burkina Faso, Cape Verde Islands, the Gambia, Ghana, Guinea, Guinea-Bissau, Ivory Coast, Liberia, Mauritania, Mali, Niger, Nigeria, Senegal, and Togo. A Senegalese magistrate serves as the acting head of GIABA.

At the first meeting, GIABA endorsed the FATF Forty Recommendations on Money Laundering, recognized the FATF as an observer, and provided for self-assessment and mutual evaluation procedures to be carried out by GIABA. While the text prepared by the experts provided for a strong involvement of ECOWAS in the activities of GIABA, the Ministers agreed to give more autonomy to the new body.

In November 2002, GIABA held a meeting with representatives from 14 of the member countries (Liberia was not represented) to discuss the money laundering situation in the region and international efforts to combat money laundering. Representatives of FATF, the Government of the United Kingdom, the UN Global Programme against Money Laundering, and the U.S. Treasury Department made presentations. GIABA did not set a date for its next meeting.

Other Multi-Lateral Organizations & Programs

Caribbean Anti-Money Laundering Programme

The U.S. Government, in partnership with the European Union and the U.K. Government launched the Caribbean Anti-Money Laundering Programme (CALP) on March 1, 1999. The Programme has been designed to assist the 21 Caribbean Basin member countries of CARIFORUM (the representative organization for Caribbean countries) to develop their anti-money laundering procedures.

The two primary objectives of CALP are:

- To reduce the incidence of the laundering of the proceeds of all serious crime by facilitating the prevention, investigation, and prosecution of money laundering and the seizure and forfeiture of property connected to such laundering activity.
- To develop a sustainable institutional capacity in the Caribbean region to address the issues related to anti-money laundering efforts at a local, regional and international level, by strengthening existing institutional capacity at the regional level, and developing new, or enhancing existing, institutional capacity at the local level.

The holistic approach undertaken by CALP consists of three separate, yet interlinked, sub-programs, detailed as follows using the theme “Taking the Profits out of Crime”:

Legal/Judicial

The lawyer responsible for delivering this sub-program is heavily involved in worldwide research of anti-money laundering laws, regulations and working practices. Appropriate recommendations are then made to the respective governments of the member countries to ensure they have the necessary legal structures in place to combat money laundering. Countries with very limited facilities are additionally assisted with drafting of the recommended introduction of our changes to their legislation. Within this sub-program, training is also given to prosecutors, magistrates and judges, and awareness training for other organizations within the financial and law enforcement sectors. In 2002, the CALP legal advisor developed a Model Terrorist Financing Law for use by the common law countries covered by CALP.

Financial Sector

Experience has shown that much of the intelligence and evidence related to money laundering comes from various financial organizations, in particular, banks, casinos and insurance companies. This sub-program has been developed to train, at all levels, staff within such organizations to identify suspicious financial activity and unusual business transactions. Staff members are made aware of the legal requirements and protection in their respective countries. A particular target is compliance officers within the financial industry who are normally responsible for some staff training. Most of such individuals have anti-money laundering issues, as part of their responsibility, so a “train the trainer” theme has been encouraged in an effort to ensure that this aspect of training is sustainable once the Programme has completed.

Law Enforcement

The Law Enforcement expert is principally concerned with the development of training to enable Caribbean law enforcement officers to effectively investigate offenses brought to their attention. The training, from basic to advanced level, has been developed in association with Caribbean law enforcement training establishments. The objective again being for such establishments to take over continued training once the Programme has been discontinued. A further objective of this sub-program is to encourage all member countries to form their own Financial Intelligence Units, with staff trained to liaise with the

financial sector, consider reported suspicious financial activity and prepare intelligence reports to assist the law enforcement officers to investigate suspected offenses.

All experts employed within the overall program are always available to advise investigators, prosecutors and judges on any aspect of anti-money laundering issues.

When the Programme commenced, very few Caribbean countries had any form of anti-money laundering legislation. None had used laws to pursue an anti-money laundering case to completion. As a consequence, most investigators, prosecutors and judges had no experience with such cases.

Since 1999, members of CALP, working with other aid programs and agencies have witnessed a major change in the attitudes of Caribbean governments with respect to money laundering. As of August 2002, all member countries have legislation, although a number of laws or procedures still need to be updated. A majority of countries have effective Financial Intelligence Units, and those who do not have all declared their intention to introduce these units within the foreseeable future.

As a consequence of these advances, a considerable number of money laundering investigations have been undertaken, with many substantial cases now before the courts, and a few have been successfully prosecuted to conviction.

The life of the Programme now extends to December 2004 when it is anticipated that all countries will have effective legislation, and investigative ability. During 2003, it is intended that an independent review will be undertaken to consider the anti-money laundering needs of member countries.

The Egmont Group of Financial Intelligence Units (FIU)

An important recent development in the international approach to combating money laundering is the creation of Financial Intelligence Units (FIUs) around the world. An FIU is a centralized unit for financial intelligence, formed by a nation to protect its financial services sector, to detect criminal abuse of its financial system, and to ensure adherence to its laws against financial crime and money laundering. Since 1995, a number of FIUs have begun working together in an informal organization known as the Egmont Group (named for the location of the first meeting at the Egmont-Arenberg Palace in Brussels). The numbers have grown dramatically. In 1995, 14 units met in Brussels; seven years later, 169 FIUs were recognized in Monaco. The newest FIUs to join the Egmont Group in 2002 are located in Andorra, Barbados, Canada, Israel, Marshall Islands, Poland, Russia, Singapore, South Korea, United Arab Emirates, and Vanuatu.

The Egmont Group serves as an international network, fostering improved communication and interaction among FIUs in such areas as 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 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 web system permits members of the group to communicate with one another via secure e-mail, 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 55 FIUs connected to the ESW.

Within the Egmont Group, working groups (Legal, Training/Communications, and Outreach) meet three times a year. The Legal Working Group reviews the candidacy of potential members and enhances information exchange between FIUs. The Training/Communications 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 Training/Communications Working Group co-hosted an FIU training seminar for analysts in Mexico, in conjunction with an international informal value transfer system seminar hosted by FinCEN in October 2002. This working group has also published a collection of sanitized terrorist and money laundering cases that were used at the typology exercises of

the FATF and other entities. The group intends to publish sanitized cases submitted from various FIUs on a quarterly basis. In addition, Britain's FIU, NCIS, sponsored a technical workshop for information technology specialists in the FIUs. The workshop focused on data mining, information fusion, security, and artificial intelligence.

The Outreach Working Group works to create a global network of FIUs to facilitate international cooperation. The Outreach Working Group identifies countries that the Egmont Group should approach to offer assistance in FIU development. The chair of the Outreach Working Group anticipates at least another 10-11 candidate FIUs may be ready for admission into the Egmont Group at the next plenary in Spring 2003.

The historic and expected future growth of the Egmont Group, as well as its now recognized value to law enforcement in the area of information exchange, necessitated the creation of an infrastructure to handle many of the activities that arise between plenary meetings. One of the most significant events during 2002 was the creation by the "Heads of FIUs" of the Egmont Committee (Committee). This Committee will serve to assist the Egmont Group in a range of activities from internal coordination and administrative consultation to representation with other international fora. Specifically, the Egmont Committee will consult and co-ordinate with the working groups and the Heads of FIUs. FinCEN will chair the newly formed Egmont Committee, with two co-chairs from the FIUs of Colombia and Australia. The Committee is currently composed of regional representation from Asia, Europe, the Americas, and Oceania, and meets three times a year in conjunction with the working groups.

As of June 2002, the members of the Egmont Group were Andorra, Aruba, Australia, Austria, Bahamas, Barbados, Belgium, Bermuda, Bolivia, Brazil, British Virgin Islands, Bulgaria, Canada, Cayman Islands, Chile, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, El Salvador, Estonia, Finland, France, Greece, Guernsey, Hong Kong, Hungary, Iceland, Ireland, Isle of Man, Israel, Italy, Japan, Jersey, Latvia, Liechtenstein, Lithuania, Luxembourg, Marshall Islands, Mexico, Monaco, Netherlands, Netherlands Antilles, New Zealand, Norway, Panama, Paraguay, Poland, Portugal, Romania, Russian Federation, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, Turkey, United Arab Emirates, United Kingdom, United States, Vanuatu, and Venezuela.

The Group of Experts to Control Money Laundering (OAS/CICAD)

OAS/CICAD is the OAS body responsible for combating illicit drugs and related crimes including money laundering. During 2002, OAS/CICAD continued its peer review of member anti-money laundering measures through the Multilateral Evaluation Mechanism (MEM) process, which periodically reviews the progress of individual countries in combating the illicit narcotics and related crimes. The first round of evaluations of all 34 OAS/CICAD member countries was concluded in December 2000. A report on the second round of full evaluations, based on an evaluation of MEM questionnaires that the countries have completed, will cover the years 2001-2002, and is expected to be released in January 2003.

The Group of Experts to Control Money Laundering is the specialized body within CICAD that is responsible for combating money laundering, and works closely with the OAS/Inter-American Committee Against Terrorism (CICTE), on combating terrorist financing. Among the notable achievements of the experts group were:

- Extension of the mandate of the Group of Experts for the Control of Money Laundering to include terrorist financing as well as money laundering.
- Revision of the Model Regulations Concerning Laundering Offenses connected to Illicit Drug Trafficking and other Serious Offenses to incorporate the FATF Special Eight Recommendations on Terrorist Financing.

- Increasing the effectiveness of money laundering legislation by assisting members in making money laundering a separate, autonomous offense.
- Strengthening Financial Intelligence Units through training and measures to enhance information sharing.
- Conducting typologies (analysis of current trends, patterns and techniques related to corruptions and terrorist financing).

CICAD continues to be active in training and technical assistance. CICAD successfully concluded the initial stage of a joint CICAD-Inter American Development Bank (IADB) Project that trained over 350 judges and prosecutors in seven South American countries (Argentina, Bolivia, Chile, Ecuador, Peru, Uruguay and Venezuela). A follow-up stage of this program has begun in these countries, and it is expected that the courses will be replicated—in a first stage round—in Argentina, Chile and Uruguay. In addition, a training course was conducted during the first week of September, in cooperation with the Spanish Government, for judges, prosecutors and legislators in Guatemala, and for representatives from Costa Rica, El Salvador, Honduras, Nicaragua, and Panama. Professors from Spain and Uruguay taught classes.

In August 2002, the OAS General Secretariat and the IADB signed Non-Reimbursable Technical Cooperation Agreement No. ATN/SF-7884-RG, whereby CICAD will carry out a two-year project to establish and strengthen Financial Intelligence Units (FIUs) in South America. This \$1.9 million project will directly benefit Argentina, Bolivia, Brazil, Chile, Ecuador, Peru, Uruguay and Venezuela. The program began in August 2002, and depending on countries' needs and the state of development of their FIUs, will provide assistance in four areas: (1) legal framework development; (2) institutional development; (3) training; and (4) technology for information and communication.

Outreach

CICAD actively participated in a number of outreach efforts designed to increase member awareness of money laundering risks and the components of an effective anti-money laundering regime, including for example, the XXXVI Conference of the Inter-American Bar Association (Working Group on Money Laundering) held in Cochabamba, Bolivia. CICAD also made presentations at the "Third Latin American Conference in Money Laundering" organized by Alert Global Media, which took place in San Juan, Puerto Rico in October.

As a special advisory member, CICAD participated in the GAFISUD Plenary Meetings IV and V held in Buenos Aires and Montevideo in May and December, respectively. Also it participated in the Egmont Group X Meeting, held in June 2002. CICAD representatives also attended FATF and CFATF meetings held in Paris and Trinidad respectively.

Pacific Islands Forum

The Pacific Islands Forum (PIF) was formed in 1971, and includes all the independent and self-governing Pacific Island countries, Australia and New Zealand. The 16 members are: 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. Annual meetings are held by the heads of member governments, followed by dialogue at the ministerial level with partners Canada, China, European Union, France, Indonesia, Japan, Korea, Malaysia, Philippines, United Kingdom and the United States.

The PIF's mission is to work in support of PIF member governments to enhance the economic and social well being of the South Pacific people by fostering cooperation between governments and international agencies, and by representing the interests of PIF members. Senior government officials from these jurisdictions meet periodically to discuss mutual concerns and regional issues. Meetings have focused heavily on regional trade and economic development issues and, in recent years, the environment. Acting

under the Honiara Declaration, PIF members have developed model legislation on extradition, mutual assistance in criminal matters and forfeiture of the proceeds of crime. In 1994, PIF achieved observer status at the UN. It also is an observer at APEC and APG meetings.

Because many of the PIF members are hampered by a lack of resources, the UN Global Program Against Money Laundering, the United States, Australia and New Zealand are providing assistance to the other PIF members through the PIF Secretariat to enable them to develop and enact laws and procedures to prevent terrorism and transnational crime, and to comply with the provisions of UNSCR 1373 and the FATF Special Recommendations on Terrorist Financing. In addition, the program will help maintain stability in the region by promoting regional cooperation. A multi-lateral legal experts working group will be established to achieve these goals.

United Nations Global Programme against Money Laundering (GPML)

The United Nations is one of the most experienced providers of training and technical assistance to legal, financial and law enforcement authorities globally. The United Nations Global Programme against Money Laundering (GPML) was established in 1997 to assist Member States to comply with the United Nations Conventions and other instruments that deal with money laundering by providing technical assistance and training in the development of the infrastructure and requisite institutions needed to counter the laundering of criminally derived proceeds.

Since 2001, the GPML has broadened this work to help Member States counter the financing of terrorism. GPML now incorporates a focus on counter-financing of terrorism (CFT) in all its technical assistance work. In addition, the Programme collaborates closely with the United Nations Counter-Terrorism Committee (CTC) in New York. In 2002, GPML began drafting model CFT legislative provisions for both common and civil law systems, and worked closely with the U.S. Department of Justice and the Organization for Security and Cooperation in Europe (OSCE) to deliver CFT training.

In 2002, the GPML continued to concentrate on its core activities of assistance to governments with the drafting of legislation, and the development of Financial Intelligence Units (FIUs). Much of the legislative assistance was, as in 2001, delivered in conjunction with the International Monetary Fund (IMF). GPML was among the first technical assistance providers to recognize the importance of countries' creating a financial intelligence capacity, and the Programme's Mentors worked extensively with the development and the implementation phases of FIUs in several countries. Also, in 2002, GPML again supported the Egmont Group's FIU training seminar. More than 200 FIU officials attended the seminar held in Oaxaca, Mexico in October.

In 2002, GPML rapidly expanded its Mentor Programme, providing "on-the-job" training that adapts international standards to specific local/national situations, rather than the traditional, more generic training seminars. The concept originated in response to repeated requests from Member States for longer-term international assistance in this technically demanding and rapidly evolving field. 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. Regional Mentors in Africa, Asia-Pacific and the Caribbean have significantly added to GPML's capacity.

The UN's Mentor Programme has key advantages over more traditional technical assistance. First, the mentor offers 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.

Pre-requisites for the Mentor Programme include candidate suitability, the commitment of the requesting Member State, and the available timing. The success of the program relies on GPML's selecting the appropriate expert for each circumstance.

In 2002, the GPML's Caribbean Region Mentor provided technical assistance in the development of FIUs in Dominica, Grenada, St. Kitts and Nevis, St. Lucia and St. Vincent and the Grenadines. The joint United Nations-Commonwealth Secretariat Pacific Region Anti-Money Laundering Initiative began in October 2002. The two organizations share the costs of the project, which is designed to enhance the financial investigations capacity of jurisdictions in the Pacific Region. GPML's financial investigations expert is spending 12 months providing technical assistance to the Cook Islands, Fiji, Samoa, and Vanuatu. Additionally, a GPML Regional Mentor began work with the Secretariat of the Eastern and Southern Africa Anti-Money Laundering Group (ESSAMLG) to work with the Secretariat on the development of its activities. At the national level, the GPML Mentors undertook technical assistance work in Antigua and Barbuda, Barbados, Canada, and the Republic of the Marshall Islands. GPML staff members, meanwhile, supplied national technical assistance to other countries, including Georgia, Haiti, and Indonesia.

GPML used both established and new collaborations with other international organizations as a key means of increasing technical assistance and training supply, as well as of ensuring synergy with the activities of other providers in the field. In 2002, the Programme collaborated with the IMF on global legislative assistance, the Commonwealth Secretariat on the joint Mentor in Asia-Pacific, the OSCE in Kyrgyzstan and Kazakhstan, and the World Bank in Russia.

In addition to collaborations with partner organizations which work to enhance the provision of technical assistance at the regional level, GPML has also been working with FATF-style regional bodies to develop their capacity to assist their Member States, particularly in Africa with the Groupe Intergouvernemental Anti-Blanchiment en Afrique (GIABA); the Groupe Anti-Blanchiment d'Afrique Centrale (GABAC), and ESAAMLG.

Research activities in 2002 focused on practitioner tools that could add value to the technical assistance delivered by the United Nations and its partner organizations. The Programme began collaborating with the United Nations Office on Drugs and Crime (UNODC) Field Office in Bangkok to produce computer-based training. The objective is to provide governments with the necessary resources and expert guidance to develop and maintain self-sustaining training programs. The output will be a comprehensive ongoing computer-based interactive anti-money laundering training program that will significantly raise skill levels, knowledge and awareness within the anti-money laundering community.

GPML also maintains a database of legislation and legal analysis of national money laundering laws. The International Money Laundering Information Network (IMoLIN—www.imolin.org) is a practical tool in daily use by government officials, law enforcement and lawyers. The Programme runs this database on behalf of the United Nations and eight major international partners in the field of anti-money laundering: the Asia/Pacific Group on Money Laundering (APG), the Caribbean Financial Action Task Force (CFATF), the Commonwealth Secretariat, the Council of Europe, the Financial Action Task Force (FATF), Interpol, the Organization of American States (OAS), and the World Customs Organization. The process of adding and updating relevant information on international/national measures, conventions and legislation to combat the financing of terrorism is ongoing. Work on the present phase involves scanning the existing legislation that is not available in electronic format, and adding it to the virtual library of anti-money laundering legislation. In addition, GPML runs the Anti-Money Laundering International Database (AMLID) on IMoLIN, a password-restricted global review of national legislation, available only to public officials. In 2002, GPML updated the AMLID analytical questionnaire to reflect new trends in legislation and policy. Applications for access to AMLID rose in 2002 by 33 percent.

In March, the Programme launched the GPML Global Press Review, which it distributes to the United Nations System, and to governments and partner international organizations involved in anti-money laundering activities as a means of keeping them updated on global developments in the field.

The World Bank and the International Monetary Fund

The World Bank (the Bank) has undertaken a number of steps to raise awareness of AML/CTF issues in its member countries and is providing technical assistance to countries to strengthen AML/CTF regimes.

In 2002, the Bank established the Global Dialogue Series, in order to bring together by videoconference leading experts and senior country officials responsible for formulating public policy on AML/CTF for a constructive exchange of ideas. Nine Global Dialogues have been held since January 2002 for countries in Eastern Europe and Central Asia, Latin America, Africa, South Asia, and East Asia and the Pacific. Government officials from a total of 42 countries have participated in these Dialogues.

In September, the International Monetary Fund (IMF), in collaboration with GAFISUD, organized a conference in Uruguay to develop coordination strategies in South America in the fight against money laundering and financing of terrorism. This workshop brought together the nine member countries of GAFISUD to share experiences with national and regional counterparts, discuss best practices, identify gaps in systems, and formulate practical cooperation strategies. In December, the Bank organized a regional conference in Moscow. The conference focused on building effective Financial Intelligence Units (FIUs). The seminar provided countries that are at a relatively early stage of addressing AML/CTF concerns and do not have fully operational FIUs with the basic information necessary for establishing and operating an FIU that meets international standards. Representatives from 23 countries attended, mostly from Europe and Central Asia but also including Egypt and China.

In addition to the regional conferences, the Bank provided technical assistance to an additional 12 countries in 2002 in response to individual requests. Drafting legislation for AML/CTF and building capacity to implement the AML/CTF standards are among the most frequent requests received in 2002.

Finally, the Bank and the IMF have launched an initiative intended to improve the international coordination of anti-money laundering and counter-terrorist financing technical assistance. On April 22, 2002, the Bank and IMF hosted a meeting in Washington to develop a mechanism for coordinating technical assistance, involving the participation of the FATF, FATF-style regional bodies (FSRB), the UN Global Programme against Money Laundering and UN Counter Terrorism Committee, the regional development banks, including the Asian Development Bank, the Department of State and other key bilateral training and technical assistance providers. Following this meeting, the Bank and IMF have been working closely with the FSRBs to assist them coordinate and meet the technical assistance needs in their region.

As part of this initiative, the Bank and the IMF have established a database of technical assistance requests and responses. The database is intended to support the strategic objectives of the Bank's technical assistance coordination initiative, including identifying high priority needs and filling gaps, strengthening the roles of the regional secretariats in coordinating technical assistance at the regional level, and enhancing information flow on needs and activities among all of the relevant partners.

The Bank is providing the infrastructure and support for the database, including training FSRBs in using the database. The initial technical assistance requests were entered into the database by the Bank based on surveys carried out in 2002 by the regional secretariats. Subsequently, information on technical assistance requests and responses will be maintained primarily by the FSRB secretariats. Technical assistance donors/providers have web-based access to the database in order to view outstanding technical assistance requests and recent technical assistance activities. The Bank will periodically circulate reports to technical assistance providers in order to assess progress in meeting requests on the database.

Offshore Financial Centers

The pressure being brought to bear by the international community on offshore financial centers to comply with anti-money laundering standards has not abated since the 1999 edition of the INCSR first

discussed the issue. Since the inception of its Non-Cooperative Countries and Territories (NCCT) exercise the FATF has designated twenty-three jurisdictions as NCCTs. Sixteen of the 23 NCCTs have either been Offshore Financial Centers (OFCs) or jurisdictions which offer services and products commonly associated with the OFCs. While 12 OFCs have remedied FATF-identified deficiencies in their legal and regulatory regimes and have been de-listed as NCCTs, four OFCs remained on the list of 11 NCCTs as of December 31, 2002.

Nearly simultaneously with the onset of the FATF NCCT exercise, the Financial Stability Forum (FSF), a body created by the G-7 in 1999, comprised primarily of officials from international regulatory bodies established the Offshore Working Group (OWG). The OWG concluded that a number of the OFCs were perceived as having weaknesses in financial supervision, cross-border cooperation and transparency. The OFCs were divided into three groups: eight OFCs (Group I) were described as “largely of a good quality”; nine Group II OFCs were found to be of lower quality than Group I OFCs, but somewhat more cooperative, more transparent and better supervised than the 26 OFCs in Group III. All 35 OFCs in Groups II and III were found to have regulatory deficiencies that could allow financial market participants to engage in regulatory arbitrage of several forms, thereby undermining efforts to strengthen the global financial system.¹

The FSF requested the International Monetary Fund (IMF) to develop, organize and conduct assessments of OFC adherence to international financial standards, including to several of the FATF Forty Recommendations that involved supervision and regulatory matters. The FSF recommended giving “highest priority to those in Group II” and “high priority to those OFCs in Group III whose scale of financial activity has the greatest potential impact on global financial stability.”

The IMF agreed to conduct assessments only of those OFCs that volunteered and first completed a self-assessment of their supervisory regimes, focused principally on the supervisory and regulatory arrangements in place for banking, securities and insurance activities. The self-assessment would be followed by an IMF-led assessment (Module II Assessment, because the self-assessment constituted the first assessment.). Following the Module II assessment, a broader and more complex IMF-led assessment (Module III) would be undertaken to assess the status of a jurisdiction’s modifications recommended in the Module II assessment. The IMF will make no assessments public unless the assessed jurisdiction voluntarily consents. During 2001, the IMF completed Module II assessments of Aruba, Belize, Cyprus, Gibraltar, Macau and Panama, and in 2002, completed Module II assessments of Andorra, Palau, Samoa, the Seychelles and the Bahamas.

While the IMF assessments performed to date confirm that many of the offshore jurisdictions are taking positive steps to increase compliance with anti-money laundering standards, as have the eight OFCs that have been de-listed from the FATF NCCT list, many OFCs continue to be inadequately regulated. The IMF assessments suggest that jurisdictions with a higher gross domestic product (GDP) are more likely to increase compliance supervision. The smaller the GDP, the more likely it is that a jurisdiction does not have adequate resources to devote to supervision and compliance. The tiny NCCT offshore jurisdiction of Niue recognized that it did not have either the necessary infrastructure to adequately regulate its five offshore banks or the financial or human resources to implement essential regulation of an offshore financial sector. As a result, in October of 2002, Niue abolished its offshore banking sector and was removed from the FATF NCCT list.

Regardless of the adequacy of resources, many of the OFCs have attracted a large non-resident customer base by intentionally offering a combination of accommodating legislation, services and products that by definition are designed to protect the anonymity of the client, while providing the client relief from home-country regulators and law enforcement. At least 90 percent of all jurisdictions offering offshore financial services restrict access to the offshore sector to non-residents, thereby creating a highly confidential and under-regulated parallel financial system within their own borders. Many jurisdictions with OFCs conduct financial transactions only in currencies other than the local currency. The vast majority of OFCs also differ from onshore jurisdictions in their regulatory regimes and legal frameworks. Many OFCs lack

Money Laundering and Financial Crimes

political will and/or resources to implement the stringent regulatory and supervisory regimes found in developed onshore jurisdictions. In the majority of OFCs, banks are not required to adhere to a wide range of regulations normally imposed on onshore banks; in some not even a physical presence is required. In most OFCs, non-bank financial industries, such as the insurance and securities industries, are subject to even less, if any, regulation than is the banking sector.

In many OFCs, a bank can be formed, registered and its ownership placed in the hands of nominee directors via the Internet. However formed, there are few, if any, disclosure requirements, bank transactions are often free of exchange and interest rate restrictions, minimal or no capital reserve requirements are in place and transactions are mostly tax-free. Some OFCs permit the licensing and registration of “shell banks”—generally understood as banks that exist on paper only and do not have a physical presence in any jurisdiction. Of the more than 4,000 offshore banks thought to exist, the number that are shell banks remains unknown.

A principal attraction of the OFCs is the frequent existence of legal frameworks designed to obscure the identity of the beneficial owner, to promote regulatory and supervisory arbitrage, and to provide mitigation or evasion of home-country tax regimes. Some of these OFCs offer the ability to form and maintain the confidentiality of a variety of international business companies (IBCs) and “exempt” companies, trusts, investment funds and insurance companies, many with nominee directors, nominee officeholders and nominee shareholders. When combined with the use of bearer shares (shares that do not name the owner and ownership is based on physical possession) and “mini-trusts” (instruments used to further insulate the beneficial owner while bridging the ownership and management of the corporate entity), IBCs can present impenetrable barriers to law enforcement.

This lack of transparency and the ability to engage in regulatory arbitrage, coupled with a concomitant reluctance or refusal of many OFCs to cooperate with regulators and law enforcement officials from other jurisdictions, attract those with both legitimate and illegitimate purposes. Narcotics-traffickers, terrorist organizations and their supporters, money launderers, tax evaders and other criminals have found the OFCs a particularly inviting venue in which to conduct and conceal their activities. With the advent of the Internet and other technological advances, funds can be transferred around the globe instantaneously, providing further opportunities to engage in the placement and layering of illicitly gained funds.

Post September 11, there is also a growing concern that terrorists and other criminals are increasingly enlisting the services of unethical lawyers, accountants and other professionals to help them discover and manipulate new money laundering and terrorist financing opportunities afforded by the new technologies and the newer, less economically developed OFCs. The attraction of establishing an offshore financial services market for small states is a dependable source of income that in some instances exceeds 50 percent of a jurisdiction’s GDP.

Other practices found in some OFCs cause additional problems for law enforcement. One such practice, well advertised on the Internet, is the selling of “economic citizenship”—a practice that, if improperly controlled, can enable individuals suspected of committing crimes to purchase citizenship in an OFC jurisdiction that may not have an extradition agreement with the purchaser’s original home country. Purchasers of economic citizenships can change their names to go along with their new passports, creating yet another impediment to law enforcement. During 2002, two Caribbean Basin OFCs, Dominica and St. Kitts & Nevis, had inadequately controlled economic citizenships. In the Pacific region, only Nauru sold improperly controlled economic citizenships. The Marshall Islands abolished this practice several years ago; however, the government has not yet been able to recover all the unauthorized passports.

Internet gaming executed via the use of credit cards and offshore banks represents yet another powerful vehicle for criminals to launder funds from illicit sources as well as to evade taxes. Advertised on the Internet as being located primarily in the Caribbean Basin, virtual casinos can be extremely profitable for governments that sell the licenses, but exert inadequate controls, and likely share in the operator’s profits. Costa Rica licenses more Internet gambling and sports betting sites than any country in the Western Hemisphere. Reportedly, 70 such sites are currently registered in Costa Rica as compared to three sites

three years ago. These sites represent a particularly difficult problem for law enforcement, as the Internet server frequently is located in a country other than the country that has licensed the website.

While many of the OFCs have been undertaking reforms to their regulatory systems and have demonstrated a growing willingness to share information with foreign law enforcement and regulatory agencies, issues of transparency still remain. Shell banks, IBCs and other corporate entities with nominee directors, trusts, bearer shares and the lack of transparency associated with them need resolution in the short-term, whether offered onshore or offshore. In a time when terrorist organizations have the capacity to disrupt global political stability, all international financial standard-setters have an obligation to move quickly to resolve these issues. The USA PATRIOT Act that prohibits transactions (directly or indirectly) between U.S. financial institutions and shell banks is but a first step in the right direction.

Explanatory Notes—Offshore Financial Services Table

Public information regarding offshore financial centers (OFCs) can be difficult to obtain. Industry publications, discussions with regulators of the OFCs, foreign government finance officials, embassy reports, analyses from United States Government (USG) agencies, international organizations, and secondary sources provided the data for the table.

Excluded are jurisdictions that provide low or no taxes to individuals but offer no other services or products normally associated with the offshore financial service sector. Also excluded are jurisdictions that have established OFCs but for which the USG has little or no information regarding the operations of the OFC. Within most categories presented on the table, the designations Y and N are used to denote the existence (Y) or the non-existence (N) of the entity or service in a specific jurisdiction. *Where there is no information regarding specific categories, or available information is inconclusive, the corresponding cells on the chart are left blank.* In some categories, symbols other than, or in addition to, a Y or N are used. Explanations for additional symbols are provided below.

Explanations of the categories themselves are either provided in the preceding text, are considered to be self-evident, or are provided below.

Category Designations—Offshore Financial Services Table

Offshore Banks: The number is provided if known. A Y indicates that although a jurisdiction that offers offshore financial services (OFC) licenses offshore banks, the number of such banks is not known. An N indicates that no offshore banks are known to be licensed in the jurisdiction. A blank cell indicates no or inconclusive information regarding whether offshore banks are offered within the OFC.

Trust and Management Companies: These are companies that provide fiduciary services, as well as serving as marketing agents, representatives, lawyers, accountants, trustees, nominee shareholders, directors, and officers of international business companies.

International Business Companies (IBCs) & Restricted Companies: Numbers are provided when known and public; in many cases, the numbers are significantly underreported. A P indicates that the jurisdiction does not publicize the number of IBCs registered within it.

Bearer Shares: Share certificates can be issued without the name of the beneficial owner. A Y indicates that the OFC offers bearer shares; an N indicates that it does not; and a blank cell indicates that the USG does not know if bearer shares are offered within the OFC.

Asset Protection Trusts (APTs): Trusts that protect assets from civil judgment. A Y indicates that the OFC offers APTs; an N indicates that it does not; and a blank cell indicates no or inconclusive information regarding whether APTs are offered within the OFC.

Insurance and Re-insurance Company Formation: A Y indicates that the OFC allows formation of insurance and re-insurance companies; an N indicates that it does not; and a blank cell indicates no or inconclusive information regarding whether insurance and re-insurance companies are allowed within the OFC.

Sells “Economic Citizenship”: A Y indicates that the OFC sells economic citizenships; an N indicates that it does not; and a blank cell indicates no or inconclusive information regarding whether the OFC sells economic citizenships. An S indicates that an OFC has suspended or ceased sales in 2001.

Internet Gaming: Licenses granted by jurisdictions that enable grantees to establish “virtual casinos” on the Internet, in which customers can pay via credit card. A Y indicates that the OFC licenses Internet gaming; an N indicates that it does not; and a blank cell indicates no or inconclusive information regarding whether Internet gaming is offered within the OFC.

Criminalized Drug Money Laundering: A D indicates that the OFC has a law criminalizing narcotics-related money laundering only. A BD indicates that crimes other than those related to narcotics are considered to be predicate crimes for money laundering in the OFC. An N indicates that there is no legislation criminalizing money laundering in the OFC.

Financial Action Task Force (FATF) Non-Cooperative Exercise: This column provides the FATF finding. NC indicates the jurisdiction was determined to be non-cooperative; R indicates that the jurisdiction was reviewed and was not identified as non-cooperative; a blank cell indicates that the jurisdiction was not reviewed. RM indicates that FATF removed the jurisdiction from the NCCT list.

Membership in International Organizations: This cell lists the multinational organizations that have been formed to combat money laundering and/or to establish a sound supervisory regime in which the OFC participates.

Offshore Financial Services Table

Jurisdictions	Offshore Banks	Trust & Management Companies	IBCs/Exempt and/or Restricted Companies	Bearer Shares	Asset Protection Trusts	Insurance and Re-insurance	Sells Economic Citizenship	Internet Gaming	Criminalized Drug Money Laundering (D) & Beyond Drugs (BD)	FATF Noncooperative Exercise	Membership in International Organizations (A, C, CE, F, O, OC, I, S)
The Americas											
Anguilla	2	Y	2,792	Y	Y	Y	N	N	BD		C, IO ¹
Antigua and Barbuda	21	Y	13,500	N	Y	Y	N	Y	BD	R	C, OC
Aruba	2	Y	3,762	Y	N	Y	N	N	BD		C, F, O, IO, EG
Bahamas	305	Y	47,040	N	Y	Y	N	N	BD	RM	C, O, OC, I, S, EG
Barbados	55	Y	4,206	N	Y	Y	N	N	BD		C, O, OC, S, EG
Belize	7	Y	18,000	Y	Y	Y	N	Y	BD	R	C, OC, S, IO
Bermuda	N	Y	13,020	N	Y	Y	N	N	BD	R	C, O, EG
British Virgin Islands	13	Y	360,000	N	Y	Y	N	N	BD	R	C, EG
Cayman Islands	580	Y	45,000	N	Y	Y	N	N	BD	RM	C, O, I, EG
Costa Rica	44	Y	20	N	N		N	Y	BD	R	C, OC, S, EG
Dominica	2	Y	1,435	N	Y	Y	Y	Y	BD	RM	C, OC
Grenada	13	Y	2,775	N	Y	Y	N	Y	BD	NC	C, OC
Guatemala	13	N		Y	N			N	BD	NC	OC

¹ A = Asia/Pacific Group; C = Caribbean Financial Action Task Force; CE = Council of Europe Select Committee on Money Laundering; E = Eastern and Southern Africa Anti-Money Laundering Group; EG = The Egmont Group; F = Financial Action Task Force; I = Offshore Group of Insurance Supervisors (OGIS); IO = Observer to the OGIS; O = Offshore Group of Banking Supervisors; OC = OAS/Inter-American Drug Abuse Control Commission; S = International Organization of Security Commissioners.

Money Laundering and Financial Crimes

Jurisdictions	Offshore Banks	Trust & Management Companies	IBCs/Exempt and/or Restricted Companies	Bearer Shares	Asset Protection Trusts	Insurance and Re-insurance	Sells Economic Citizenship	Internet Gaming	Criminalized Drug Money Laundering (D) & Beyond Drugs (BD)	FATF Noncooperative Exercise	Membership in International Organizations (A, C, CE, F, O, OC, I, S)
Montserrat	15		22	Y		N	N	N	BD		C
Netherlands Antilles	39	Y	18,750	Y	N		N	Y	BD		C, EG, O, I,
Panama	34	Y	370,000		Y	Y	N	N	BD	RM	C, O, OC, S, EG
St. Kitts & Nevis				N	Y	N	Y	Y	BD	RM	C, OC
(St. Kitts)	N	Y	450								
(Nevis)	1	Y	17,000								
St. Lucia	1	Y	733	N	Y	Y	N	N	BD	R	C, OC
St. Vincent & The Grenadines	15	Y	9,734	N	Y	Y	N	Y	BD	NC	C, OC
Turks and Caicos	8	Y	13,952	N	Y	Y	N	Y	BD	R	C, I
Uruguay	12	N	Y	Y	N	Y	N	N	BD	R	OC, S
Europe											
Andorra											
Cyprus	28	Y	57,600	N	Y	Y	N	N	BD	R	CE, O, S, EG
Gibraltar	21	Y	8,300	Y	Y	Y	N	Y	BD	R	O, I
Guernsey ¹	70	Y	15,910	N	N	Y	N	N	BD	R	O, I, S, EG
Alderney	N	Y	455		N		N	Y			
Sark	N	Y			N		N	N			
Hungary	N	N	600	Y	N	N	N	N	BD	RM	CE, EG
Ireland	N	Y	400	N	N	Y	N	N	BD		F, S, EG

¹ Guernsey, Jersey, the Isle of Man, Hong Kong, Liechtenstein, Luxembourg and Switzerland are unique. Residents are able to avail themselves of many OFC services and products normally reserved for nonresidents.

Jurisdictions	Offshore Banks	Trust & Management Companies	IBCs/Exempt and/or Restricted Companies	Bearer Shares	Asset Protection Trusts	Insurance and Re-insurance	Sells Economic Citizenship	Internet Gaming	Criminalized Drug Money Laundering (D) & Beyond Drugs (BD)	FATF Noncooperative Exercise	Membership in International Organizations (A, C, CE, F, O, OC, I, S)
Isle of Man ¹	Y	Y	24,300	Y	N	Y	N	N	BD	R	O, I, S, EG
Jersey ¹	Y	Y	30,000	N	N	Y	N	N	BD	R	O, I, S, EG
Liechtenstein ¹	17	Y	75,000	Y	N	Y	N	N	BD	RM	CE, EG
Luxembourg ¹	200	Y	68,000	Y	N	Y	N	N	BD		F, S, EG
Malta	1	Y	285	N	N	Y	N	N	BD	R	CE, O, S
Monaco	N		Y		N		N	N	BD	R	EG
Switzerland ¹	500	Y	Y	Y	N		N	N	BD		F, S, EG
"Turkish Republic of No. Cyprus"	32	N	54		N	N	N	N	D		
Africa & Middle East											
Botswana	1	Y	Y					N			E
Bahrain	51	Y	Y	N	N	N	N		BD		O, S
Liberia			Y	Y	Y		N	N	N		
Mauritius	11	Y	10,700	Y	Y		N	N	N	R	E, O, S
Madeira (Portugal)	27	Y	4,100	Y	N	Y	N	N	BD		
Seychelles	Y		4,800	Y	Y	Y	N	Y	BD	R	E
Tunisia	12		1,500		N		N	N	N		S
Asia											
Brunei	Y	Y	300	N	N	Y	N				
Hong Kong ¹	Y	Y	500,000	N	N	Y	N	N	BD		A, F, O, S, EG

¹ Guernsey, Jersey, the Isle of Man, Hong Kong, Liechtenstein, Luxembourg and Switzerland are unique. Residents are able to avail themselves of many OFC services and products normally reserved for nonresidents.

Money Laundering and Financial Crimes

Jurisdictions	Offshore Banks	Trust & Management Companies	IBCs/Exempt and/or Restricted Companies	Bearer Shares	Asset Protection Trusts	Insurance and Re-insurance	Sells Economic Citizenship	Internet Gaming	Criminalized Drug Money Laundering (D) & Beyond Drugs (BD)	FATF Noncooperative Exercise	Membership in International Organizations (A, C, CE, F, O, OC, I, S)
Labuan (Malaysia)	53	Y	2,070	N	Y	Y	N	N	BD		A, I, O, S
Macau	Y		Y		N		N	N	BD		A, O
Singapore	59	N	Y	N	N	Y	N	N	BD		A, F, O, S, EG
Pacific											
Cook Islands	25	Y	1,200	Y	Y	Y	N	N	BD	NC	A
Marshall Islands	N	Y	5,500	Y	N	N	N	N	BD	RM	A, EG
Nauru	400	Y	Y	Y	N	Y	Y	N	N	NC	
Niue	N	Y	6,000	Y	Y	Y	N	N	BD	RM	A
Palau	Y	N	N	Y		N	N	Y		R	
Samoa	8	Y	7,553	Y	Y	Y	N	N	BD	R	A, IO
Vanuatu	55	Y	2,500	Y	N	Y	N	Y	BD	R	A, O, EG

Major Money Laundering Countries

Each year, U.S. officials from agencies with anti-money laundering responsibilities meet to assess the money laundering situations in more than 185 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 2002 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 can 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.

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 the right 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 non-bank 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 non-bank 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, underskilled 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.
- 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, 2002-2003

Upgrades	Downgrades
Costa Rica Concern → Primary	Grenada Primary → Concern
Haiti Concern → Primary	St. Vincent & the Grenadines Primary → Concern
Bosnia & Herzegovina Other → Concern	

The following countries were added to the Money Laundering & Financial Crimes report this year and are included in the “Other” Column: Andorra, Burkina Faso, Chad, Democratic Republic of the Congo, Republic of the Congo, Gabon, The Gambia, Guinea, San Marino, Sao Tome & Principe, Sierra Leone, and Syria.

In the **Country/Jurisdiction Table** on the following page, “major money laundering countries” are identified for purposes of 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 or the degree of its cooperation in the international fight against money laundering.

Country/Jurisdiction Table

Countries/Jurisdictions of Primary Concern		Countries/Jurisdictions of Concern		Other Countries/Jurisdictions Monitored	
Antigua and Barbuda	Taiwan	Albania	St. Vincent	Afghanistan	Macedonia
Australia	Thailand	Argentina	Turks & Caicos	Algeria	Madagascar
Austria	Turkey	Aruba	Vanuatu	Andorra	Malawi
Bahamas	Ukraine	Bahrain	Vietnam	Angola	Maldives
Brazil	United Arab Emirates	Barbados	Yemen	Anguilla	Mali
Burma	United Kingdom	Belgium	Yugoslavia FR	Armenia	Malta
Canada	USA	Belize		Azerbaijan	Mauritius
Cayman Islands	Uruguay	Bolivia		Bangladesh	Micronesia FS
China, People Rep	Venezuela	Bosnia & Herzegovina		Belarus	Moldova
Colombia		British Virgin Islands		Benin	Mongolia
Costa Rica		Bulgaria		Bermuda	Montserrat
Cyprus		Cambodia		Botswana	Morocco
Dominica		Chile		Brunei	Mozambique
Dominican Rep		Cook Islands		Burkina Faso	Namibia
France		Czech Rep		Cameroon	Nepal
Germany		Ecuador		Chad	New Zealand
Greece		Egypt		Congo, Dem. Rep. of	Niger
Guernsey		El Salvador		Congo, Rep. of	Norway
Haiti		Gibraltar		Cote d'Ivoire	Oman
Hong Kong		Grenada		Croatia	Papua New Guinea
Hungary		Guatemala		Cuba	Qatar
India		Honduras		Denmark	Sao Tome & Principe
Indonesia		Ireland		Eritrea	Saudi Arabia
Isle of Man		Jamaica		Estonia	Senegal
Israel		Korea, North		Ethiopia	Sierra Leone
Italy		Korea, South		Fiji	Slovenia
Japan		Latvia		Finland	Soloman Islands
Jersey		Malaysia		Gabon	Sri Lanka
Lebanon		Marshall Islands		Gambia	Suriname
Liechtenstein		Monaco		Georgia	Swaziland
Luxembourg		Netherlands Antilles		Ghana	Sweden
Macau		Nicaragua		Guinea	Syria
Mexico		Niue		Guyana	Tajikistan
Nauru		Palau		Iceland	Tanzania
Netherlands		Peru		Iran	Togo
Nigeria		Poland		Jordan	Tonga
Pakistan		Portugal		Kazakhstan	Trinidad and Tobago
Panama		Romania		Kenya	Tunisia
Paraguay		Samoa		Kuwait	Turkmenistan
Philippines		Seychelles		Kyrgyzstan	Uganda
Russia		Slovakia		Laos	Uzbekistan
Singapore		South Africa		Lesotho	Zambia
Spain		St. Kitts & Nevis		Liberia	Zimbabwe
Switzerland		St. Lucia		Lithuania	

Comparative Table

The comparative table that follows the Glossary of Terms below identifies the broad range of actions that jurisdictions have, or have not, taken to combat money laundering, that were effective as of December 31, 2002. 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 non-drug-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.
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 non-bank financial institutions to meet the same customer identification standards and adhere to the same reporting requirements that it imposes on banks.

Money Laundering and Financial Crimes

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, 2001, 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, 2002, 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 Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Gibraltar, Montserrat and Turks and Caicos are Overseas Territories of the United Kingdom. Guernsey, the Isle of Man and Jersey are Crown Dependencies of the United Kingdom. As such, they are not members of the United Nations. Niue is not a member of the United Nations; nor is Taiwan.

Comparative Table

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions	Financial Intelligence Unit	System for Identifying/Forfeiting Asset	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
	Government/Jurisdiction															
Afghanistan	N	N	N	N	N	N	N	N	N	N	Y	N	N	Y	N	N
Albania	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	N	N	Y	N	Y
Algeria	N	N	N	N	Y	N	Y	N	N	Y	N	N	Y	Y	Y	Y
Andorra	Y	Y	N	Y	Y	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	N	N	N
Anguilla	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N
Antigua & Barbuda	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Argentina	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Armenia	N	N	N	Y	N	N	Y	N	N	N	N	N	N	Y	N	N
Aruba	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N
Australia	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Austria	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y
Azerbaijan	N	N	N	N	N	N	N	N	N	Y	Y	N	N	Y	N	Y
Bahamas	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
Bahrain	Y	Y	N	Y	Y	Y	Y	N	Y	N	Y	N	Y	Y	Y	N
Bangladesh	Y	Y	N	Y	N	N	N	N	N	N	Y	N	N	Y	N	N
Barbados	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Belarus	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	Y	N	N
Belgium	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Belize	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y	Y	N
Benin	Y	N	Y	N	Y	N	Y	N	Y	Y	N	N	Y	Y	N	Y
Bermuda	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N
Bolivia	Y	Y	N	Y	Y	Y	Y	N	N	N	Y	N	Y	Y	N	Y
Bosnia & Herzegovina	N	N		Y	Y	N	Y	N			N	N		Y	Y	N

Money Laundering and Financial Crimes

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions	Financial Intelligence Unit	System for Identifying/Forfeiting Asset	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
Botswana	Y	Y	Y	Y	N	N	Y	Y	N	N	N	N	N	Y	N	Y
Brazil	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
British Virgin Islands	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
Brunei Darussalam	Y	Y	N	Y	Y	N	Y	N	N	N	N	Y	N	Y	N	Y
Bulgaria	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Burkina Faso	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N
Burma	Y	Y	N	Y	Y	N	Y	N	N	N	Y	N	N	Y	N	N
Cambodia	Y	N	Y	Y	N	N	N	N	Y	N	N	N	N	N	N	N
Cameroon	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N
Canada	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Cayman Islands	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
Chad	Y	Y	Y	Y	Y	N	Y	N	N	N	N	N	N	Y	N	N
Chile	Y	N	N	Y	N	Y	N	N	Y	N	Y	N	N	Y	N	Y
China (PRC)	Y	Y	Y	N	Y	N	Y	N	Y	Y	Y	N	N	Y	Y	N
Colombia	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Comoros	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N
Cook Islands	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	N
Congo (Dem. Republic)	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Congo (Republic)	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Costa Rica	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
Cote D'Ivoire	Y	Y	Y	Y	Y	N	Y	N	N	Y	Y	N	Y	Y	N	Y
Croatia	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Cuba	Y	Y	N	N	N	N	Y	N	N	Y	N	N	N	Y	N	Y
Cyprus	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Czech Republic	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Denmark	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Dominica	Y	Y	N	Y	Y	Y	Y	Y	Y	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	Financial Intelligence Unit	System for Identifying/Forfeiting	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
Dominican Republic	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Ecuador	Y	N	Y	Y	Y	N	N	Y	Y	N	Y	N	N	Y	N	N
Egypt	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
El Salvador	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Eritrea	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N
Estonia	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	N	N	Y	N	Y
Ethiopia	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	Y	N	N
Fiji	Y	Y	N	Y	Y	N	Y	N	Y	Y	Y	N	N	Y	N	N
Finland	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y
France	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Gabon	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Gambia	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	Y	N	N
Georgia	N	N	N	N	N	N	N	N	N	N	Y	N	N	Y	N	Y
Germany	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y	Y	N
Ghana	Y	Y	N	Y	N	N	Y	N	Y	Y	Y	Y	Y	Y		Y
Gibraltar	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	N	Y	N
Greece	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Grenada	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
Guatemala	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y
Guernsey	Y	Y	N	N	Y	Y	Y	Y	Y	N	Y	Y	N	Y	Y	N
Guinea	Y	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N
Guyana	Y	Y	N	Y	Y	N	Y	N	N	Y	Y	N	Y	Y	N	N
Haiti	Y	Y	Y	Y	Y	N	Y	N	N	Y	N	Y	Y	Y	N	N
Honduras	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Hong Kong	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Hungary	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y
Iceland	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y		Y

Money Laundering and Financial Crimes

Actions by Governments																
	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions	Financial Intelligence Unit	System for Identifying/Forfeiting Asset	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
India	Y	N	Y	Y	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	N
Indonesia	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	N	N	Y	Y	N
Iran	N	N	N	N	N	N	N	N	N	N	Y	N	N	Y	N	N
Ireland	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Isle of Man	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Israel	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Italy	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Jamaica	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	N	N
Japan	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Jersey	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Jordan	Y	Y	N	Y	Y	N	N	N	N	N	Y	N	Y	Y	Y	N
Kazakhstan	Y	N	N	Y	Y	N	N	N	N	Y	Y	N	N	Y	N	N
Kenya	Y	N	Y	Y	N	N	Y	N	Y	N	Y	N	N	Y	N	N
Korea (DPRK)	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Korea (Republic of)	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Kuwait	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y	Y	N	N
Kyrgyzstan	N	N	N	N	N	N	Y	N	N	N	N	N	N	Y	N	N
Laos	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Latvia	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	N	Y
Lebanon	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	N	N
Lesotho	N	N	Y	N	Y	N	N	N	N	N	N	N	N	Y	N	Y
Liberia	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N
Liechtenstein	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	N	N
Lithuania	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y	N	N
Luxembourg	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N
Macau	Y	Y	N	Y	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N
Macedonia	Y	Y	N	Y	Y	N	Y	N	Y	Y	Y	N	Y	Y	N	N

Actions by Governments																
	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions	Financial Intelligence Unit	System for Identifying/Forfeiting	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
Madagascar	Y	N	N	N	N	N	N	N		N	N	N	N	Y	N	N
Malawi	N	N	Y	Y	N	N	N	N		N	N	N	N	Y	N	N
Malaysia	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Maldives	Y	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N
Mali	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	Y
Malta	Y	Y	N	Y	Y	Y	Y	N	Y	N	Y	Y	N	Y	Y	Y
Marshall Islands	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	N	N
Mauritius	Y	Y	N	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	N
Mexico	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y
Micronesia	Y	Y	N	Y	N	N	Y	N	N	N	Y	N	N	N	N	Y
Moldova	Y	Y	N	Y	Y	N	N	N	N	Y	Y	Y	Y	Y	Y	Y
Monaco	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Mongolia	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Montserrat	Y	Y	N	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	N	N
Morocco	N	N	N	Y	N	N	N	N	N	N	Y	N	N	Y	N	Y
Mozambique	Y	Y	Y	Y	Y	N	Y	N	N	Y	Y	Y	Y	Y	N	Y
Namibia	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N
Nauru	Y	Y	N	Y	Y	N	Y	Y	Y	N	Y	N	Y	N	N	N
Nepal	N	N	N	Y	N	N	N	N	Y	N	Y	N	N	Y	N	N
Netherlands	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Netherlands Antilles	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
New Zealand	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Nicaragua	Y	N	Y	Y	Y	N	Y	N	N	Y	Y	N	N	Y	N	Y
Niger	N	N	Y	N	N	N	Y	N		N	N	N	N	Y	N	N
Nigeria	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y	Y	N
Niue	Y	Y	N	Y	Y	N	N	N	Y	N	Y	Y	Y	N	N	N
Norway	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Money Laundering and Financial Crimes

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions	Financial Intelligence Unit	System for Identifying/Forfeiting	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
Oman	Y	Y	Y	Y	Y	N	Y	N	Y	N	Y	Y	Y	Y	N	N
Pakistan	Y	N	N	Y	N	N	Y	N	Y	N	Y	N	Y	Y	N	N
Palau	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y
Panama	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
Papua New Guinea	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Paraguay	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	N	N
Peru	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	N	Y
Philippines	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Poland	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	Y	N	Y	N	N
Portugal	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Qatar	Y	Y	Y	Y	Y	N	Y	N	Y	N	Y	Y	Y	Y	N	N
Romania	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y	Y	Y
Russia	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Samoa	Y	Y	N	Y	Y	N	Y	N	N	Y	Y	Y	Y	N	Y	Y
Sao Tome & Principe	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N
Saudi Arabia	Y	Y	N	Y	Y	N	Y	N	Y	N	Y	Y	Y	Y	N	N
Senegal	Y	N	N	Y	Y	N	Y	N	N	N	Y	N	N	Y	N	N
Seychelles	Y	Y	N	Y	Y	N	Y	N	N	N	N	N	Y	Y	N	N
Sierra Leone	N	N	N	Y	Y	N	N	N	N	N	N	N	N	Y	N	N
Singapore	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Slovakia	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N	Y	N	Y	N	Y
Slovenia	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Solomon Islands	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
South Africa	Y	Y	N	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	N	N
Spain	Y	Y	Y	Y	Y	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	N	Y	Y	Y
St Kitts & Nevis	Y	Y	Y	Y	Y	Y	Y	Y	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	Financial Intelligence Unit	System for Identifying/Forfeiting	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
St. Lucia	Y	Y	N	Y	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N
St. Vincent/Grenadines	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y
Suriname	Y	Y	N	Y	Y	N	Y		N	N	Y	Y	Y	Y	N	N
Swaziland	Y	Y	Y	Y	Y	N	Y	N	Y	N	Y	N	Y	Y	N	N
Sweden	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Switzerland	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	N	N
Syria	N	N	N	N	N	N	Y	N	N	N	Y	N	N	Y	N	N
Taiwan	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
Tajikistan	Y	Y	N	N	N	N	N	N	Y	N	Y	N	N	Y	N	N
Tanzania	Y	N	Y	Y	N	N	Y	N	Y	N	Y	N	Y	Y	Y	Y
Thailand	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	N	N	N
Togo	Y	N	Y	Y	N	N	Y	N		N			Y	Y	Y	Y
Tonga	Y	Y	Y	Y	N	N	Y	N	Y	Y	N	N	N	Y	N	Y
Trinidad & Tobago	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N
Tunisia	N	N	N	N	N	N	N	N	N	Y	N	N	N	Y	N	N
Turkey	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	N	Y
Turkmenistan	Y	Y			N	N	N	N		Y				Y	N	N
Turks & Caicos	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	N	N
Uganda	Y	N	N	N	N	N	N	N		N	N	N	N	Y	Y	N
Ukraine	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	N	Y
United Arab Emirates	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y	N	Y	N	N
United Kingdom	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
United States	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Uruguay	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	N	N
Uzbekistan	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	N	N	Y	Y	Y
Vanuatu	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	N
Venezuela	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N

Money Laundering and Financial Crimes

Actions by Governments																
	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions	Financial Intelligence Unit	System for Identifying/Forfeiting	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
Vietnam	Y	Y	N	N	N	N	N	N	N	N	Y	N	N	Y	N	Y
Yemen	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N
Yugoslavia/Serbia	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y
Yugoslavia/Montenegro	Y	Y	N	N	Y	N	Y	N	Y	N	Y	N	N	Y	N	Y
Zambia	Y	Y	Y	Y	Y	N	Y	N	N	N	N	N	N	Y	N	N
Zimbabwe	Y	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

Appendix

FATF Special Recommendations on Terrorist Financing

Recognizing the vital importance of taking action to combat the financing of terrorism, the FATF has agreed these Recommendations, which, when combined with the FATF Forty Recommendations on money laundering, set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts.

I. Ratification and implementation of UN instruments

Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

II. Criminalizing the financing of terrorism and associated money laundering

Each country should criminalize the financing of terrorism, terrorist acts and terrorist organizations. Countries should ensure that such offenses are designated as money laundering predicate offenses.

III. Freezing and confiscating terrorist assets

Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organizations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organizations.

IV. Reporting suspicious transactions related to terrorism

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organizations, they should be required to report promptly their suspicions to the competent authorities.

V. International co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organizations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organizations, and should have procedures in place to extradite, where possible, such individuals.

VI. Alternative remittance

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.

VII. Wire transfers

Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).

VIII. Nonprofit organizations

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organizations are particularly vulnerable, and countries should ensure that they cannot be misused:

- (i) by terrorist organizations posing as legitimate entities;
- (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and
- (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organizations.

Country Reports

Afghanistan. Afghanistan is not a regional financial or banking center. Its financial and credit institutions are rudimentary. Afghanistan does not have anti-money laundering or terrorist financing legislation. Efforts are being made to strengthen police and customs forces, but there are few resources or expertise to combat financial crimes.

Much of the money laundering in Afghanistan is linked to the trade of narcotics. Afghanistan accounts for the large majority of the world's opium production. The opium is refined into heroin, often broken into small shipments, and smuggled across porous borders via truck or mule caravan for resale broad. Payment for the narcotics is generated through a variety of means, including trade based money laundering. Narcotics are sometimes thought of as just another commodity or trade good. There are reports that the going rate for a kilo of heroin is a color television set. A kind of barter system has developed where narcotics in Afghanistan and neighboring Pakistan are exchanged for foodstuffs, vegetable oils, electronics, and other goods. Many of these trade goods are smuggled into Afghanistan from neighboring countries or enter through the Afghan Transit Trade without payment of customs duties or tariffs. Invoice fraud, corruption, indigenous smuggling networks, and legitimate commerce are all intertwined. Hawala networks are also widespread, and often times trade goods are used to provide counter-valuation in balancing the books. There are allegations that these alternative remittance systems within Afghanistan have also been involved with the financing of terrorist organizations.

Afghanistan is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Much work is required to develop and modernize Afghanistan's infrastructure, financial framework, judiciary, and civil service including its police and customs service. An effective first step in constructing an anti-money laundering program would be to enact anti-money laundering and anti-terrorist finance legislation that complies with international standards.

Albania. Albania remains at significant risk for money laundering because it is a transit country for trafficking in narcotics, arms, contraband, and illegal aliens. Organized crime groups use Albania as a base of operations for conducting criminal activities in other countries. Albanian organized crime groups active outside the country send large sums of illegitimately earned money—estimated by the European Union at \$15 billion annually—back to Albania. The proceeds from these activities are easily laundered in Albania because of weak government controls. Albania's economy is primarily cash-based.

Albania criminalized all forms of money laundering through Article 287 of the Albanian Criminal Code of 1995. In 2000, the International Monetary Fund (IMF) assisted Albania in drafting anti-money laundering legislation that was subsequently approved by Albania's legislature. Law No. 8610 "On the Prevention of Money Laundering" (passed in 2000) requires financial institutions to report to an anti-money laundering agency all transactions that exceed approximately \$10,000 as well as those that involve suspicious activity. Financial institutions are required to report transactions within 48 hours if the origin of the money cannot be determined. In addition, private and state entities are required to report all financial transactions that exceed certain thresholds. The Bank of Albania has established a task force to confirm banks' compliance with customer verification rules.

The legislation also mandates the establishment of an agency to coordinate the Government of Albania's (GOA) efforts to detect and prevent money laundering. The Agency for Coordinating the Combat of Money Laundering (ACCML) is Albania's Financial Intelligence Unit. The ACCML 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. The ACCML has the ability to enter into bilateral or multilateral information sharing agreements on its own authority. The legislation, however, does not mandate staffing and funding of the ACCML.

Money Laundering and Financial Crimes

Albania has not criminalized terrorist financing, and Albanian law does not authorize freezing or confiscating assets belonging to terrorists. However, the GOA has used its anti-money laundering law to freeze the assets of individuals and organizations on the UN 1267 Sanction Committee's consolidated list of terrorists.

Coordination against money laundering and terrorist financing among agencies is sporadic. Authority and responsibility remains unclear among agencies, and therefore, duplication and confusion are possible.

Albania became a party to the UN International Convention for the Suppression of the Financing of Terrorism on April 10, 2002. On August 21, 2002, Albania ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Albania is a party to the 1988 UN Drug Convention. Albania is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, formerly known as PC-R-EV).

The GOA should clarify interagency anti-money laundering responsibilities and should provide adequate legal and financial resources to the ACCML. It should also criminalize terrorist financing.

Algeria. Algeria is not a financial center and the extent of money laundering in Algeria is not known.

On April 7, 2002, the Government of Algeria adopted Executive Order 02-127, which established the Cellule du Traitement du Renseignement Financier (CTRF), an independent unit within the Ministry of Finance. The 2003 Finance Law, approved on December 25, 2002, requires all financial institutions to report suspicious activity to the CTRF. All financial institutions are also obligated to comply with requests for information from the CTRF or face penal liability. The Finance Law allows the CTRF to freeze assets for up to 72 hours based on suspicious activity. Additionally, the Finance Law provides for state protection for officials or informants who cooperate with the CTRF.

The Central Bank monitors all international financial operations carried out by public or private banking institutions. Individuals entering Algeria must declare all foreign currency to the customs authority.

Algeria criminalized terrorist financing by adopting Ordinance 95.11 on February 24, 1994, making the financing of terrorism punishable by 5-10 years of imprisonment.

Algeria is a party to both the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. On October 7, 2002, Algeria became a party to the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Algeria should enact a comprehensive anti-money laundering regime and criminalize money laundering for all serious crimes.

Andorra. Due to its geographical location in the Pyrenees, its relatively strong financial system, and the free movement of money across its frontiers, Andorra is likely to attract money laundering operations.

Andorra substantially revised its anti-money laundering regime in December 2000 with the passage of its Law on International Criminal Co-operation and the Fight against the Laundering of Money and Securities Deriving from International Delinquency. Essentially, this law imposes reporting obligations upon Andorran financial institutions, insurance and re-insurance companies and on natural persons or entities whose professions or business activities involve the movement of money or securities that may be susceptible to laundering. It goes on to specifically cover external accountants and tax advisors, real estate agents, notaries and other legal professionals when acting in certain professional capacities, as well as casinos and dealers in precious stones and metals. Reports of suspicious transactions are made to the Unit for the Prevention of Laundering Operations (UPBO), Andorra's Financial Intelligence Unit. Predicate offenses for money laundering are defined in the criminal code and include drug trafficking, hostage taking, sales of illegal arms, prostitution and terrorism. Article 49 of this law contains a tipping off prohibition and Article 50 provides a safe harbor in that individuals or entities who report suspicious activities or transactions under this law are not liable for violations of any other secrecy or confidentiality statutes.

A decree to set up specific regulations to cover all administrative aspects of the Act of December 2000 was approved in August 2002. The decree requires retail establishments to notify the government of any transactions for gems and jewelry where the payment made in cash is greater than 15,000 euros. The law also requires banks to notify the FIU of any currency exchanges where the amount is over 1,250 euros.

Customer identification, including identification of the beneficial owner, is required at the time a business relationship is established and before any transaction when the obligation to take due care calls for verification of the identity of the beneficial owner. Records verifying identity must be kept for a period of at least ten years from the date when the business relationship ends.

The entirety of Title I of this same law pertains to the organization of international judicial help, generally easing previous restrictions that had applied when a foreign authority requested information protected by Andorran bank secrecy. Information may be furnished in response to requests otherwise conforming to Andorran law.

The UPBO was established in 2001 and has become a member of the Egmont Group. Andorra complies with the Financial Action Task Force (FATF) 40 recommendations plus the Special Recommendations on Terrorist Financing. UPBO, with a staff of four, is an administrative unit with no law enforcement powers of its own. But the police work closely with the FIU, and a newly passed article authorizes the use of telephone taps and undercover officers in money laundering investigations. The UPBO can administratively freeze assets for five days without a judicial order. If the assets need to be held for a longer period, the UPBO can seek a judicial order, which normally occurs within the five-day period the UPBO is authorized to hold the accounts. Judicial freeze orders can be effective for an indefinite period of time. UPBO also acts in a supervisory role, and provides education regarding compliance and money laundering prevention to financial services providers.

The UPBO works closely with its Spanish and French counterparts. During the first seven months of operation (July 24, 2001—February 22, 2002), the UPB received 24 suspicious transaction reports filed by obligated institutions. To date it has not dealt with any cases involving terrorism, but it has frozen assets in some non-terrorist related money laundering cases.

Andorra has signed, but not yet ratified, the UN International Convention on the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Although not a member of the European Union, Andorra has very close cultural and geographic ties to Spain and France. In fact, Andorra does not have a requirement for cross-border currency declarations, because with Spain's threshold at 8,000 euros and France's at 6,000 euros, it would be impossible to enforce.

Andorra should continue to enhance its anti-money laundering regime by broadening its definition of money laundering to expand the list of predicate offenses, and if it has not already done so, should criminalize the financing of terrorism.

Angola. Angola has an underdeveloped financial sector and money laundering does not appear to be a significant problem. Yet the laundering of funds derived from corruption is a concern, as is the illegal trade in diamonds and the usage of diamonds as a conduit for money laundering schemes. It is possible that links exist between the illegal diamond trade and international drug and criminal organizations. Angola is participating in the "Kimberley Process," which is a globally coordinated effort to halt trade in "conflict" diamonds in countries such as Angola by domestically implementing rough diamond trade control regimes. Angola has already implemented a domestic system in accordance with the Kimberley Process.

Angola has no comprehensive laws, regulations, or other procedures to detect money laundering and financial crime. Angola's counternarcotics laws criminalize money laundering related to narcotics-trafficking.

Angola has not deposited its instruments of ratification to the 1988 UN Drug Convention. Angola has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Angola should criminalize terrorist financing and money laundering related to all serious crimes and should develop a viable anti-money laundering regime.

Anguilla. Anguilla's offshore financial sector renders it vulnerable to money laundering. As with the other U.K. Caribbean overseas territories, Anguilla underwent an evaluation of its financial regulations in 2000, co-sponsored by the local and British governments.

Anguilla's domestic financial sector includes four domestic banks and 17 insurance companies. The Eastern Caribbean Central Bank (ECCB) supervises Anguilla's four domestic banks. The offshore sector includes two banks, one captive insurance company, and approximately 2,792 international business companies (IBCs) and 43 trusts. IBCs may be registered using bearer shares that conceal the identity of the beneficial owner of these entities. The Financial Services Department (FSD) Director is responsible for inspecting Trust Companies, Offshore Banks, the Registrar of Insurance and is the Inspector of Company Management.

The Proceeds of Criminal Conduct Act (PCCA), 2000 extends the predicate offenses for money laundering to all indictable offenses and allows for the forfeiture of criminally derived proceeds. It provides for suspicious activity reporting and a safe harbor for this reporting. The Money Laundering Reporting Authority Act (MLRA), 2000 requires persons involved in the provision of financial services to report any suspicious transactions derived from drugs or criminal conduct. The MLRA establishes requirements for customer identification, record keeping, reporting, and training procedures. It also details provisions for a Reporting Authority that will receive the suspicious transaction reports required and may forward information to the police for further investigation. The Reporting Authority is now operational, but it is not a member of the international Egmont Group of FIUs. The Criminal Justice (International Co-operation) (Anguilla) Act, 2000 enables Anguilla to directly cooperate with other jurisdictions through mutual legal assistance.

The U.S./U.K. Mutual Legal Assistance Treaty concerning the Cayman Islands was extended to Anguilla in November 1990. Anguilla is also subject to the U.S./U.K. Extradition Treaty. Anguilla is a member of the Caribbean Financial Action Task Force (CFATF), and is subject to the 1988 UN Drug Convention.

Anguilla should continue to strengthen its anti-money laundering regime by adopting measures to immobilize bearer shares and ensure that beneficial owners of IBCs can be identified. Legislation should be passed granting operational independence for the FSD, with its own funding source and a supervisory board.

Antigua and Barbuda. Antigua and Barbuda has comprehensive legislation in place to regulate its financial sector, but it remains susceptible to money laundering because of its loosely regulated offshore financial sectors and its Internet gaming industry. In August 2001, as a result of the enactment of new laws and their substantial implementation, both the U.S. and the UK lifted April 1999 financial advisories recommending that their respective financial institutions give enhanced scrutiny to all financial transactions routed into or out of Antigua and Barbuda.

In response to these advisories, the Government of Antigua and Barbuda (GOAB) in 1999 repealed the 1998 amendments to Antigua and Barbuda's Money Laundering (Prevention) Act (MLPA) of 1996 that had effectively strengthened bank secrecy, inhibited money laundering investigations and infringed on international cooperation. Additional amendments to the MLPA in 2000, 2001 and 2002 enhanced international cooperation, strengthened asset forfeiture provisions and created civil forfeiture powers.

Antigua and Barbuda in October 2001 enacted the Prevention of Terrorism Act, which empowers the Supervisory Authority under the MLPA to nominate any entity as a "terrorist entity" and to seize and forfeit terrorist funds. The law specifies any finances in any way related to terrorism. Antigua circulated all the various "terrorist" lists to all financial institutions in Antigua. The lists did not produce any

disclosures. All institutions were personally contacted to ensure compliance. Thus, no terrorist funds were detected in Antigua. The GOAB has responded to the FATF Self-Assessment for Implementation of the Special Recommendations on Terrorist Financing; based on its responses, it was determined to be compliant with six of the seven recommendations and partially compliant with the recommendation concerning alternative remittances. The GOAB has acceded to the International Convention for the Suppression of the Financing of Terrorism. 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 charitable and non-profit entities.

In 2000, the GOAB amended the International Business Corporations Act (IBCA) of 1982 in order to excise 1998 amendments that had given the International Financial Sector Regulatory Authority (IFSRA) responsibility to both market and regulate the offshore sector as well as to allow members of the IFSRA Board of Directors to maintain ties to the offshore industry. The GOAB further amended the IBCA that year to require that registered agents ensure the accuracy of the records and registers that are kept at the Registrar's office, as well as to know the names of beneficial owners of IBC's and to disclose such information to authorities upon request. In December 2000, the GOAB issued a Statutory Instrument, which has the force of law, requiring banks to establish the true identities of account holders and to verify the nature of an account holder's business, source of funds and beneficiaries. In 2002, the IFSRA was replaced by a new entity entitled the Financial Services Regulatory Commission (FSRC). The Director of IFSRA was removed from her position and replaced by a new director. FSRC, was reportedly created, to create a unified regulatory structure of Antigua's financial services' sector. FSRC now has the responsibility of regulating the offshore banking sector, the formation of international business corporations, Internet gaming, and domestic financial services, such as insurance and trusts.

From 1999 through 2002, the GOAB conducted an extensive review of the offshore banking sector. As a result, 26 offshore banks had their licenses revoked, were dissolved, placed in receivership or otherwise put out of business. Currently, Antigua and Barbuda has 21 licensed offshore banks in operation. Of these, however, 11 are foreign shell banks that have no physical presence in Antigua and Barbuda.

Unlike some of the other countries in the Eastern Caribbean, the GOAB has not yet chosen to initiate a unified regulatory structure or uniform supervisory practices for its domestic and offshore banking sectors. Currently, the Eastern Caribbean Central Bank (ECCB) supervises Antigua and Barbuda's domestic banking sector. A domestic entity, the FSRC is responsible for the regulation and supervision of the offshore banking sector as well as conducting examinations and on-site and off-site reviews of the country's offshore financial institutions and of some domestic financial entities, such as insurance companies and trusts. The FSRC, formed in 2002, represents on balance a weaker regulatory structure than its predecessor, the International Financial Services Regulatory Authority (IFSRA). Additionally, the FSRC issues licenses for the international business corporations and maintains the register of all corporations, of which there are approximately 13,500. Bearer shares are not permitted. The license application requires disclosure of the names and addresses of directors—who must be natural persons—the activities the corporation intends to engage in and the names of shareholders and number of shares that they will hold. Service providers are required by law to know the names of beneficial owners.

The Office of National Drug Control and Money Laundering Policy (ONDCP) directs the GOAB's anti-money laundering efforts in coordination with the FSRC. It has primary responsibility for the enforcement of the MLPA. ONDCP is a department of the Prime Minister's Ministry and the GOAB intends to introduce legislation designating the ONDCP as a law enforcement agency with statutory powers of investigation, search and arrest. The GOAB's Financial Intelligence Unit and Financial Investigations Unit are components of the ONDCP. In recent years, a number of GOAB civilian and law enforcement officials, both in and out of the ONDCP, have received anti-money laundering training from the Caribbean Anti-Money Laundering Program and bilateral Department of State, Bureau of International Narcotics and Law Enforcement Affairs funded anti-money laundering training programs.

Casinos and sports book-wagering operations in Antigua and Barbuda's Free Trade Zone are supervised by the ONDCP and the FSRC, of which the Directorate of Offshore Gaming (DOG)—13 professional and clerical employees—is a part. Antigua and Barbuda's domestic casinos, of which there are six, are required to incorporate as domestic corporations and Internet gaming operations, of which there are 39, are required to incorporate as IBC's. The FSRC and DOG have issued Internet Gaming Technical Standards and guidelines. The 2000 and 2001 amendments to the MLPA expand its coverage to include all types of gambling entities and set financial limits above which customer identification and source of funds information are required. Suspicious activity and suspicious transaction reports from domestic and offshore gaming are sent to the ONDCP and FSRC; currently, they are receiving 2-3 weekly. The GOAB has drafted and is considering legislation and regulations for the licensing of interactive gaming and wagering in order to address possible money laundering through client accounts of Internet gambling operations.

Antigua and Barbuda is a party to the 1988 UN Drug Convention, a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and a member of the Caribbean Financial Action Task Force (CFATF), of which it assumed the Vice-Presidency in 2002. The GOAB underwent its Second Round CFATF Mutual Evaluation in October 2002. In 1999, Antigua and Barbuda was the first country in the Eastern Caribbean to exchange instruments of ratification bringing into force a Mutual Legal Assistance Treaty and an Extradition Treaty with the United States. One extradition request related to a fraud and money laundering investigation remains pending under the Treaty, awaiting the outcome of an appeal against a Magistrate's deportation order. Antigua and Barbuda signed a Tax Information Exchange Agreement with the United States in December 2001 that allows the exchange of tax information between the two nations. Antigua and Barbuda ratified the UN Convention against Transnational Organized Crime on July 24, 2002. In 2002, the Bahamas sponsored Antigua and Barbuda for membership in the Egmont Group. The ONDCP expects to be admitted as a full member at the Group's 2003 Plenary.

In 2002 the GOAB continued its bilateral and multilateral cooperation in various criminal and civil investigations and prosecutions, including, in particular, the FBI's investigation into the activities in Antigua and Barbuda of John Muhammed, the alleged Washington, D.C. area sniper. The GOAB has provided assistance to U.S. and other countries' law enforcement officials and prosecutors investigating and prosecuting fraud and money laundering cases. The GOAB has benefited through an asset sharing agreement with Canada and has received other asset sharing revenues as a result of its cooperation in the freezing and forfeiture of illegal assets at the request of other countries. However, Antigua and Barbuda has not prosecuted a money laundering or forfeiture case, on its own.

The GOAB should continue its international cooperation and rigorously implement and enforce all provisions of its anti-money laundering legislation, as well as take the necessary legislative and regulatory steps to ensure that its gambling sector is properly covered by anti-money laundering legislation and is strictly supervised. Additionally, the GOAB should vigorously enforce its money laundering laws by actively prosecuting money laundering and asset forfeiture cases. The GOAB should ensure that all offshore banks licensed in Antigua and Barbuda have a physical presence, to avoid possibly losing correspondent accounts in U.S. banks under Section 313 of the USA Patriot Act.

Argentina. Argentina is neither an important regional financial center nor an offshore banking center. Money laundering related to narcotics-trafficking, corruption, contraband, and tax evasion is believed to occur throughout the financial system, in spite of the Government of Argentina's (GOA's) efforts, described below, to stop it. The severe financial crisis and capital controls of the past two years may have reduced the opportunities for money laundering through the banking system. However, transactions conducted through non-bank 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.

In the midst of the political and economic crisis that swept Argentina during 2002, the Government made efforts at implementing the regulations for anti-money laundering law number 25.246 of May 2000. Law 25.236 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 a Financial Intelligence Unit (FIU), in Spanish, Unidad de Informacion Financiera (UIF), under the Ministry of Justice and Human Rights. Under this 2000 law, requirements for customer identification, record keeping, and reporting of suspicious transactions now apply to all financial entities and businesses supervised by the Central Bank, the Securities Exchange Commission (Comisión Nacional de Valores—CNV), and the Superintendency of Insurance. These financial entities and businesses include banks; currency exchange houses; casinos; securities dealers; registrars of real estate; auto dealerships; dealers in art, antiques, and precious metals; insurance companies; issuers of travelers checks; credit card companies; armored car companies; postal money transmitters; notaries; and certified public accountants.

The law forbids the institutions to notify their clients when filing suspicious financial transactions reports, and provides a safe harbor from liability for reporting such transactions. The UIF is expected to establish reporting norms tailored to each type of business. The UIF began operating in June 2002 at a minimum capacity due to a lack of funds, since it was not included in the national budget for 2002. In addition, it has not received the technical and specialized personnel that were to join it from the Central Bank, CNV, and the Superintendency of Insurance. The UIF now has 28 staff, and their 2003 budget will support an increase in staff up to 60. However, that budgeted personnel level is not supported with funds for sufficient computer and security equipment or office furniture and supplies even for the current 28 staff.

Per a rule issued by the UIF, effective October 29, 2002, entities supervised by the Central Bank, CNV, and the Superintendency of Insurance must report all suspicious transactions over 500,000 Argentine pesos (approximately \$140,000) directly to the UIF. Transactions below 500,000 Argentine pesos will go to the appropriate supervisory body for pre-analysis and subsequent transmission to the UIF if deemed necessary. The UIF has now received approximately 200 SARs.

The UIF also issued a rule for the centralized registration at the UIF 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 (approximately \$2,700). The UIF further receives copies of the declarations to be made by all individuals (foreigners or Argentine citizens) entering or departing Argentina with over \$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. 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. The money laundering law of May 2000 (25.246) provides that proceeds of assets forfeiture under this law can also be used to fund the UIF.

The GOA remained active in multilateral counternarcotics and international anti-money laundering organizations. It is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention Against Transnational Organized Crime, which is not yet in force internationally. It 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 Financial Action Task Force (FATF) as well as the South American Financial Action Task Force (GAFISUD). The GOA and the United States Government (USG) have a Mutual Legal Assistance Treaty that entered into force in 1993, and an extradition treaty that entered into force on June 15, 2000. In March 2001, the GOA signed the UN International Convention for the Suppression of the Financing of Terrorism. On September 26, 2001, the Central Bank of Argentina issued Circular B-6986 instructing financial institutions to identify and freeze the funds and financial assets of the individuals and entities listed by the USG as possibly engaged in acts of terrorism. Although no assets were frozen, the Central Bank continues to monitor the financial institutions.

Argentina should take measures to implement the FATF's 8 Special Recommendations on Terrorist Financing. With strengthened mechanisms available under the May 2000 anti-money laundering law,

Money Laundering and Financial Crimes

including the creation of the UIF, Argentina seems poised to prevent and combat money laundering effectively. Disputes over information sharing between the UIF and the tax agency (AFIP) also need to be resolved for anti-money laundering efforts to succeed. In addition, further implementation efforts are needed in order to succeed: increased public awareness of the problem of money laundering and the requirements under the new law, forceful 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 provision of the necessary resources to the UIF to carry out its mission.

Armenia. Armenia is not a major financial center; however, high unemployment, low salaries, corruption, a large underground economy, and the presence of organized crime also contribute to Armenia's vulnerability to money laundering. Schemes used to launder funds include the under-invoicing of imports, double bookkeeping, and misuse of the banking system.

Under banking laws amended in October and November, 2002, the Central Bank requires banks in Armenia to demand certain information from people and businesses making large deposits in order to demonstrate that the funds are of legal origin. The new laws also require banks to confirm the identity of clients wishing to open a bank account. Also under the new laws, the Central Bank can freeze bank accounts suspected of containing funds used for terrorist financing or money derived from criminal activities. The Government of Armenia has drafted a law that would criminalize money laundering.

Armenia is a party to the 1988 UN Drug Convention. Armenia has signed, but not yet become a party to, both the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime, which is not yet in force internationally. In 2001, Armenia signed, but has not yet become a party to, the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime. It is, however, a party to the European Convention on Mutual Assistance in Criminal Matters.

Armenia should establish and implement a comprehensive anti-money laundering regime that criminalizes money laundering and terrorist financing.

Aruba. Aruba, which has full internal autonomy, is a part of the Kingdom of the Netherlands. As a transit country for cocaine and heroin, Aruba is both attractive, and therefore, vulnerable to money launderers. While not large, the offshore sector consists of 562 active limited liability companies and 3,762 active offshore tax-exempt companies referred to as Aruba Exempt Companies (AEC). Both types of companies can issue bearer shares. The financial sector is composed of the five onshore banks, two offshore banks, four bank-like institutions, and two credit unions; other financial sector entities include eight life insurance companies, 12 general insurance companies, two captive insurance companies, ten company pension funds, and 30 money remitters and exchange offices. There are also 11 casinos. Aruba's offshore industry constitutes about one percent of GDP and is due to be phased out by the end of 2005 as part of the Government's May 2001 commitment to the OECD in connection with the Harmful Tax Practices initiative.

Aruba offshore services currently include the offshore Naamloze Vennootschap (NV) or limited liability company, which is a low-tax entity, and the Aruba Exempted Company (AEC). A local director, usually a trust company, must represent offshore NVs. A legal representative that must be a trust company represents AECs. AECs pay an annual registration fee of approximately \$280, and must have a minimum authorized capital of \$6,000. AECs cannot participate in the economy of Aruba, and are exempt from several obligations: all taxes and currency restrictions, and the filing of annual financial statements. Trust companies provide a wide range of corporate management and professional services to AECs, including managing the interests of their shareholders, stockholders, and other creditors. In May 2000, the Government of Aruba (GOA) issued guidance notes on corporate governance practices.

The GOA has prepared a State Ordinance for the Supervision of Trust Companies. The draft ordinance, which was submitted to Parliament on January 23, 2001, provides for the oversight of thrift companies to

ensure that they follow “Know Your Customer” procedures. The International Monetary Fund (IMF) also reviewed the draft ordinance. The draft ordinance is still pending enactment.

To replace the offshore sector and keep Aruba competitive for international capital, the GOA is proposing a New Fiscal Framework (NFF or Dutch acronym: NFR) that reportedly contains elements such as a dividend tax and imputation credits. The proposal will have to be consistent with OECD standards regarding its “Harmful Tax Practices” regime. The full content and its practical application, however, cannot be fully assessed at this time.

Following up on the July 4, 2000, Parliamentary approval of the State Ordinance Free Zones Aruba (FZA), the Parliament unanimously approved the designation of a Free Zone Aruba NV entity to operate the free zones. One aspect of this designation requires free zone customers to reapply for authorization to operate within the zones. As a result of these tougher standards there was a 65 percent drop in free zone business in Aruba.

The Free Zone NV is preparing a “Best Practices” guide describing these standards for its companies. Aruba took the initiative in the Caribbean Financial Action Task Force (CFATF) to develop regional standards for free zones, where none existed, in an effort to control trade-based money laundering. The guidelines were adopted in April 2001 at the CFATF Plenary, and in October the CFATF Ministerial Council followed.

All financial and non-financial institutions are obligated to report unusual transactions to Aruba’s Financial Intelligence Unit (FIU), the Meldpunt Ongebruikelijke Transacties (MOT). The MOT has a staff of five that consists of three investigators and two administrative assistants. On March 12 the GOA authorized a doubling of the MOT’s staff to 12 and is committed to providing the MOT with additional computer equipment and software in 2003 to increase its effectiveness and efficiency.

The FIU is required to inspect all casinos, banks, money remitters, and insurance companies. On July 1, 2001, a State Ordinance was issued that extended reporting and identification requirements to casinos and insurance companies, and in early 2003, the MOT will begin on-site inspections. The State Ordinance on the Supervision of Insurance Business (SOSIB) and the Implementation Ordinance on SOSIB require insurance companies established after July 1, 2001, to obtain a license from the Central Bank of Aruba. Effective February 19, 2002, suspicious transaction reporting was extended to life insurance companies.

In June 2000, Aruba enacted a State Ordinance making it a legal requirement to report the importation and exportation via harbor and airport of currency in excess of 20,000 Aruban guilders (approximately \$11,000). The law is still pending implementation.

In July of 2002, there were two convictions for money laundering through supermarkets. In most cases the money laundering offense is integrated into investigations of the underlying offense.

Aruba signed a multilateral directive with Colombia, Panama, the United States, and Venezuela to establish an international working group to fight money laundering that occurs 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 next working group meeting will convene in July 2003 to review countries’ progress in implementing the recommendations and to report on results achieved in combating trade-based money laundering.

In October 2002, the MOT took the initiative to host a “Counter-terrorism Financing Anti-Money Laundering Conference” in Aruba for 120 participants drawn from the GOA, the private financial sector, FinCEN, and the FBI.

Through the Netherlands, Aruba participates in the Financial Action Task Force (FATF), and therefore, participates in the FATF mutual evaluation program. The GOA has a local FATF committee that oversees the implementation of the FATF recommendations, including the Eight Special Recommendations on Terrorist Financing. The local FATF committee reviewed the GOA anti-money

Money Laundering and Financial Crimes

laundrying legislation and proposed, in accordance with the FATF Eight Special Recommendations on Terrorist Financing, amendments to existing legislation and introduction of new laws. Currently, there are seven draft ordinances before Parliament. As part of its commitment to combat the financing of terrorism, the GOA formed another committee to ensure cooperation within the Kingdom of the Netherlands.

Aruba is a member of CFATF and served as its Chairman in 2001. In 1999, the Netherlands extended application of the 1988 UN Drug Convention to Aruba. The Netherlands's Mutual Legal Assistance Treaty with the United States applies to Aruba, though it is not applicable to requests for assistance relating to fiscal offenses addressed to Aruba.

The MOT is a member of the Egmont Group. A draft law, which would authorize the MOT to share information with foreign counterpart organizations through a memorandum of understanding (MOU), is now with Parliament. In June 2001, the MOT signed an agreement with the FIUs of the Netherlands and the Netherlands Antilles to exchange information.

Aruba's anti-money laundrying legislation adheres to the recommendations of FATF and the CFATF. The GOA has shown a commitment to combating money laundrying by establishing a solid anti-money laundrying program. Given the money laundrying vulnerability presented by bearer shares, the GOA should ensure that bearer shares are immobilized under the NFF. The GOA should also pass and implement legislation, regulations and MOUs to improve information sharing by its FIU and to improve adherence to the new FATF Eight Special Recommendations on Terrorist Financing. The GOA should also provide adequate resources to the MOT to enable it to properly carry out its mission of analyzing unusual transactions and conducting on-site inspections of all financial and non-financial institutions.

Australia. Australia is one of the key centers for capital markets activity in the Asia-Pacific region, with liquid markets in equities, debt, foreign exchange and derivatives. Activity across Australia's exchange and over-the-counter financial markets amounted to \$27.6 trillion through June 2002, an increase of 19.5 percent on the same period 12 months ago. The market capitalization of finance and insurance on the Australian stock exchange (ASX) has increased eightfold from \$18.8 billion in 1991 to \$147 billion in 2001. The Government of Australia (GOA) has put in place a comprehensive system to detect, prevent, and prosecute money laundrying. The major sources of illegal proceeds are fraud and drug trafficking. The last two years have seen a noticeable increase in activities investigated by Australian law enforcement agencies that relate directly to offenses committed overseas. The majority of these matters are connected to frauds committed in an overseas jurisdiction where money has either been laundered into Australia for the purpose of acquiring assets or has been laundered through Australia to overseas countries.

Australia criminalized money laundrying related to serious crimes with the enactment of the Proceeds of Crime Act of 1987. This legislation also contains provisions to assist investigations and prosecution in the form of production orders, search warrants, and monitoring orders. The Mutual Assistance in Criminal Matters Act of 1987 allows Australian authorities to assist other countries in identifying, freezing, seizing, and confiscating the proceeds of crime.

The Financial Transaction Reports Act (FTR) of 1988 was enacted to combat tax evasion, money laundrying, and serious crimes. Banks and financial institutions are required to verify the identities of all new account holders and new signatories to existing accounts, and must retain the 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 also establishes reporting requirements for Australia's financial services sector. Required to be reported are: suspicious transactions; cash transactions in excess of Australian \$10,000; and international funds transfers equivalent to or exceeding Australian \$10,000. FTR reporting also applies to non-bank 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. Lawyers also are

required to report significant cash transactions. Accountants do not have any FTR obligations. However, they do have an obligation under a self-regulatory industry standard not to be involved in money laundering transactions.

The Australian Transaction Reports and Analysis Center (AUSTRAC), Australia's Financial Intelligence Unit (FIU), estimates that approximately \$26 million in reported suspect transactions is reported annually from reporting cash dealers (financial institutions). Australian Federal Police (AFP), based on their intelligence on drug crime and major frauds, estimates that approximately \$1.75-2.1 million is laundered through the Australian economy each year. AUSTRAC was established under the FTR to oversee compliance with the reporting requirements imposed on the financial services sector. AUSTRAC also gathers and disseminates financial intelligence that supports revenue collection and law enforcement activities.

In June 2002, Australia passed the Suppression of the Financing of Terrorism Act 2002. The aim of the bill 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 bill 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 bill also addresses commitments Australia has made with regard to the UNSCR 1373 and the UN International Convention for the Suppression of the Financing of Terrorism. There have been no prosecutions or arrests under this legislation to date. The Security Legislation Amendment (Terrorism) Act 2002, which received Royal Assent on 5 July 2002, inserted into the Criminal Code offenses of receiving funds from, or making funds available to, a terrorist organization.

On September 6, 2002, the GOA froze three accounts in the name of a listed terrorist entity, the International Sikh Youth Federation (ISYF). A review of the FTR Act is currently being undertaken with regard to improving procedures, implementing international best practices, and addressing further aspects of terrorist financing to include alternative remittance systems.

Australia is a member of the Financial Action Task Force (FATF), co-chairs the Asia/Pacific Group on Money Laundering (APG) and is also a member of the Pacific Island Forum, and the Commonwealth Secretariat. Through its funding and hosting of the Secretariat of the APG, Australia has elevated money laundering issues to a priority concern among countries in the Asia/Pacific region. AUSTRAC is a member of the Egmont Group, and has bilateral agreements allowing the exchange of financial intelligence with 11 countries, with approximately 19 additional MOUs in various stages of negotiation. MOUs have recently been signed with Singapore, Isle of Man and Israel. An MOU with Canada is expected to be signed shortly. Other MOUs are with Vanuatu, United States, United Kingdom, New Zealand, Belgium, France, Italy and Denmark. MOUs with Malaysia and Thailand are expected to be signed early in 2003, and with Switzerland in April 2003. In September 1999, a Mutual Legal Assistance Treaty between Australia and the United States entered into force. In March 2002, Australia signed a bilateral agreement with Vanuatu.

Australia has signed and ratified the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, and the 1988 UN Drug Convention. Australia has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Australia ratified the UN International Convention for the Suppression of the Financing of Terrorism on September 26, 2002.

Australia continues to pursue a well-balanced, comprehensive and effective anti-money laundering regime that meets the objectives of the FATF Forty Recommendations and the Special Recommendations on Terrorist Financing. It gives high priority to dealing with money laundering and to international cooperation. AUSTRAC serves as a model for FIUs worldwide, because of its demonstrated commitment and competence in using financial reports and related information to identify money trails. The GOA

Money Laundering and Financial Crimes

should continue its efforts to emphasize money laundering issues and trends within the APG, and its commitment to providing training and technical assistance to the Asia/Pacific region.

Austria. Austria is not an important regional financial center, offshore tax haven or banking center. There is no hard evidence that Austria is a major money laundering country; however, like any highly developed financial marketplace, Austria's financial and non-financial institutions are vulnerable to money laundering. According to the Austrian Interior Ministry's 2001 National Security Report, organized crime has become a cross-border multinational problem in Austria, representing a considerable share of overall criminal activity. The percentage of undetected organized crime is believed to be enormous, with revenues derived from organized crime often mingled with legitimate income in legal firms. Organized crime, in particular from the former Soviet Union, is trying to launder money in Austria by investing in real estate, exploiting existing business contacts, and trying to establish new contacts in politics and business.

Austria criminalized money laundering in 1993. Adoption of 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, as well as insurance companies underwriting life policies. The Banking Act created the Austrian Financial Intelligence Unit (AFIU, formerly known as EDOK) within the Interior Ministry. In 2002, the AFIU was absorbed as one section of the newly established Austrian Bundeskriminalamt (Federal Crime Office). AFIU continues to serve as the central repository of suspicious transaction reports.

The Banking Act requires identification of all customers when entering an ongoing business relationship, i.e., in all cases of opening a checking account, a passbook savings account, a securities deposit account, etc. In addition, customer identification is required for all transactions of more than 15,000 euros, (\$14,016) for customers without a permanent business relationship with the bank. Banks and other financial institutions are required to keep records on customers and account owners. Bankers are protected 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. AFIU is, however, providing information to banks to raise awareness of large cash transactions.

The existence of anonymous numbered passbook savings accounts spurred the Financial Action Task Force (FATF) to threaten Austria with suspension from FATF if Government of Austria (GOA) did not take action to abolish the accounts. The European Commission had lodged a complaint with the European Court of Justice contending that these anonymous passbook savings accounts violated the Commission's anti-money laundering directive. The FATF lifted its warning about the anonymous passbook savings accounts following the GOA's enactment of legislation, effective November 2, 2000. Since then, new passbook savings accounts and deposits on existing accounts require customer identification. The deadline for identifying existing anonymous accounts was June 30, 2002; since then, special procedures, i.e., delaying payments and reporting such customers to the police, apply for accounts not yet identified. There are no statistics on how many accounts have not been identified. Banks and other financial institutions must maintain records on customer identification for at least five years after the termination of the business relationship. Records of all transactions are kept for at least five years following the execution of those transactions.

The anonymity of securities accounts was abolished in 1996 with the so-called "iceberg solution." Under this arrangement, withdrawals and sales of securities from anonymous accounts opened before August 1, 1996, were allowed without customer identification; these accounts would then "melt away" over time, since no new deposits were allowed. This arrangement expired June 30, 2002. However, for securities accounts not identified by June 30, 2002, special procedures, like those applied to passbook savings accounts, do not apply. In 1997, the GOA tightened restrictions on trustee accounts, applying requirements that encompass identification of the beneficial owner(s).

A planned amendment of the Banking Act to implement the EU's Money Laundering Directive on the prevention of the use of the financial system for the purpose of money laundering, as amended in 2001,

and to incorporate changes related to terrorism financing and implementation of stricter identification requirements (for trustees and beneficial owners, and by requiring banks to ask for and make a copy of an official picture ID and terminate entries of “personally known customer” in banks’ records) was not sent to Parliament due to the GOA’s early break-up in September 2002.

Another outstanding issue for the next government is the deferred amendment of the Customs Act addressing the problem of international transportation of illegal-source currency and monetary instruments. The planned amendment was to introduce border controls for cash. Presently, there are no cross-border reporting requirements, and there is no declaration requirement at the border relating to the amount of currency that can be legally brought into or taken out of Austria.

The Banking Act includes a due diligence obligation, and individual bankers are held legally responsible if their institutions launder money. In addition, banks have signed a voluntary agreement to prohibit active support for capital flight. On November 26, 2001, the Federal Economic Chamber’s banking and insurance department, in cooperation with all banking and insurance associations, published an official “Declaration of the Austrian Banking and Insurance Industries to Prevent Financial Transactions in Connection with Terrorism.”

Currently, there are no money laundering controls applied to non-banking financial institutions not subject to the Banking Act. However, an amendment of the Business Code taking effect June 15, 2003, will introduce money laundering regulations regarding 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, and real estate agents. Regulations for accountants, lawyers and notaries are in the drafting phase and will be incorporated in the occupational regulations for these professions, expected to be implemented by mid-2003. For casinos, a planned amendment of the Gambling Act, implementing a legal requirement for customer identification and a reporting requirement of suspected money laundering or terrorism financing activities, was not sent to Parliament due to the GOA’s early break-up, and is another issue for the next government. However, absent the legal regulation for customer identification, casinos licensed in Austria are already supervised by the Ministry of Finance, and require and record picture IDs of all visitors.

Legislation implemented in 1996 allows for asset seizure and the forfeiture of illegal proceeds; however, there is little evidence of enforcement to date. 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 banking secrecy regulations, though bank secrecy will be lifted for cases of suspected money laundering. Moreover, bank secrecy does not apply in cases when banks and other financial institutions are required to report suspected money laundering. Such cases are subject to instructions of the authorities (i.e., AFIU) with regard to processing such transactions.

The Criminal Code Amendment 2002, effective October 1, 2002, introduces the following new criminal offense categories: terrorist grouping, terrorist criminal activities, and financing of terrorism. “Financing of terrorism” is defined 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. Further, 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. The Austrian authorities have circulated to all financial institutions the list of individuals and entities included on the UN 1267 Sanctions Committee’s consolidated list and those designated by the United States or the EU. According to the Ministry of Justice and the AFIU, no accounts found in Austria ultimately showed any links to terrorist financing. After September 11, 2001, the AFIU froze several accounts on an interim basis, but in trying to establish evidence, only two accounts were designated for seizure. Both later turned out to be cases of mistaken identity.

The GOA has undertaken some initial efforts that may help thwart the misuse of charitable and/or non-profit entities as conduits for terrorist financing. The new law on associations (*Vereinsgesetz*, published in

Federal Law Gazette number I/66 of April 26, 2002) came into force on July 1, 2002, and covers charities and all other non-profit associations in Austria (including religious associations, sports clubs, etc.). Materially, the new law is very similar to the old law, but it does call for record keeping and auditing on the part of non-profit entities. The Vereinsgesetz regulates the establishment of associations, bylaws, organization, management, association register, appointment of auditors, and detailed accounting requirements. The Ministry of Interior's responsibility is limited to approving the establishment of associations, regardless of the purpose of the association, unless it violates legal regulations. There are no regular or routine checks made on associations established in Austria. Only in case of complaints will the Interior Ministry start investigations and, in case of serious violations of laws, may officially prohibit the association. As mentioned above, the planned amendment of the Banking Act to tighten ID requirements was not sent to Parliament due to GOA's early break-up in September 2002. The draft also included regulations to subject money remittance businesses to the Banking Act.

Austria has not enacted legislation that provides for sharing narcotics-related assets with other governments. However, mutual legal assistance treaties (MLATs) can be used as an alternative vehicle to achieve equitable distribution of forfeited assets. The MLAT that has been in force since August 1, 1998, between the GOA and the United States contains a provision relating to asset sharing. The GOA has been extremely cooperative with U.S. law enforcement investigations. Austria has a bilateral agreement with Hungary concerning the exchange of information related to money laundering. Austria has endorsed fully all core principles of the 1997 Basel Committee. In addition to the exchange of information with home country supervisors permitted within the EU, Austria has defined this information exchange more precisely in agreements with five other EU members (France, Germany, Italy, Netherlands, and UK) and with the Czech Republic, Hungary and Slovenia.

Austria is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. In December 2000, Austria signed, but has not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Austria ratified the UN International Convention for the Suppression of the Financing of Terrorism on April 15, 2002. Austria is a member of the FATF and the EU, and is an observer with the Council of Europe's select committee of experts on the evaluation of anti-money laundering measures (Moneyval, formerly PC-R-EV). The AFIU is a member of the Egmont Group.

The GOA has criminalized money laundering for all serious crime and passed additional legislation necessary to construct a viable anti-money laundering regime. The GOA should ensure its pending laws and regulations are adopted and implemented, particularly those covering financial intermediaries and gaming entities. Additionally, the GOA should adequately regulate its charitable and non-profit entities to reduce their vulnerability to misuse by terrorist organizations and their supporters.

Azerbaijan. Azerbaijan is not considered a major center for international money laundering given its small, underdeveloped banking sector. It is difficult, however, to determine the extent of the money laundering problem, due to existing bank secrecy laws and the number of formal and informal non-bank financial institutions. The large number of cash transactions, as well as the legacy of corruption and tax evasion, compounds the problem. Azerbaijan has not adopted a specific anti-money laundering law, although parliament has made amendments to its banking and currency laws in order to prevent money laundering activities. In November 2001, regulations were enacted that stipulated any person leaving or entering the country with \$50,000 or more in foreign currency must report the amount to customs.

Funds transfers abroad in excess of \$ 10,000 must have the approval of the National Bank of Azerbaijan (NBA). The NBA also has issued "know your customer" directives to individual banks. Reportedly, non-bank financial institutions are probably used to launder money related to tax evasion and avoidance of customs fees.

Article 214-1 of Azerbaijan's Criminal Code criminalizes the financing of terrorism. The NBA also distributes lists of individuals and entities added to the U.S. Executive Order 13224 asset freeze list and submitted to the UN 1267 Sanctions Committee to be included on its consolidated list of

entities/individuals whose assets UN member states are obligated to freeze pursuant to UNSCR 1267 and 1390. To date, NBA has identified and frozen the assets of one designated entity.

Azerbaijan is party to the 1988 UN Drug Convention. In October 2001, Azerbaijan became a party to the UN International Convention for the Suppression of the Financing of Terrorism. In November 2001, Azerbaijan signed the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime but has not yet ratified the Convention. Azerbaijan submitted the Financial Action Task Force (FATF) Terrorist Finance Self-Assessment Questionnaire in October 2002.

Azerbaijan should enact money laundering legislation that establishes a viable anti-money laundering regime that would require filing suspicious transactions to a Financial Intelligence Unit. Additionally, the Government of Azerbaijan should develop awareness programs for its law enforcement and customs agencies.

Bahamas. The Commonwealth of the Bahamas is an important regional and offshore financial center. The U.S. dollar circulates freely in the Bahamas, and is everywhere accepted on a par with the Bahamian dollar.

Money laundering in the Commonwealth of the Bahamas is mostly related to the proceeds of cocaine and marijuana trafficking, although a substantial portion is likely related to financial fraud. During 2001, the Government of the Commonwealth of the Bahamas (GCOB) implemented legislative reforms that strengthened its anti-money laundering regime and made it less vulnerable to exploitation by money launderers and other financial criminals. As a result, in June 2001, the Financial Action Task Force (FATF) removed the Bahamas from the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering. The United States and Canada also withdrew financial advisories for the Bahamas. Although removed from the NCCT list, FATF continues to monitor the Bahamas' progress in implementing its anti-money laundering regime. During 2002, the GCOB continued to implement legislative reforms, enacted in 2000, that strengthened its anti-money laundering regime and report such implementation efforts to the Americas Review Group of FATF.

Financial services are the second most important industry in the Bahamas, accounting for 15 percent of the Gross Domestic Product (GDP) and ranking just behind tourism. At the beginning of 2002, there were 356 licensed bank or trust companies, down 13 percent from 410 at the beginning of 2001. The decline was due to the Central Bank of the Bahamas' requirement that "managed banks" (those without a physical presence but which are run by an agent such as a lawyer or another bank) either establish a physical presence in the Bahamas (an office, separate communications links and a resident director) or cease operations. Some 227 of the 356 institutions were permitted to deal with the public and 129 had either restricted or non-active licenses. Of the public institutions, only 44 were Bahamian-based banks and trusts; 106 were subsidiaries of banks and trusts based outside the Bahamas; 53 were euro-currency branches of foreign banks and trusts based in the United States, the United Kingdom, Canada, Europe, South America, Central America and Asia; and 24 were clearing banks or trusts based outside the Bahamas and authorized to deal in Bahamian and foreign currency and gold.

During 2002, the Financial Intelligence Unit (FIU), created in 2000, continued to share financial information with its foreign counterparts, including FinCEN, the U.S. Financial Intelligence Unit. In 2001, the FIU received 246 suspicious transaction reports, and more than 80 reports have been received in 2002.

In 2002, the Bahamian Court of Appeal reversed a controversial lower court decision that had held unconstitutional a provision of the FIU Act 2000. The appellate decision confirmed the power of the FIU to freeze a financial account without first obtaining a court order. The plaintiff, a British Virgin Islands firm, Financial Clearing Corporation, did not pursue a possible appeal to the Judicial Committee of the Privy Council in London.

The Financial Transaction Reporting Act 2000 required financial institutions (including banks and trusts, insurance companies, real estate brokers, casino operators, and others who hold or administer accounts for clients) to report suspicious transactions to the FIU and to the police. That Act also established

Money Laundering and Financial Crimes

“Know Your Customer” (KYC) requirements for financial institutions and obliged them to verify by December 31, 2001 the identities of all their existing account holders and of customers without an account making transactions over \$10,000. The Act has been amended several times to extend the deadline, which is now December 31, 2003.

All new accounts established in 2001 or later had to be in compliance with KYC rules before they were opened. As of October 2002, only 229,000 accounts had been verified of 538,861 accounts (some 42 percent). From their introduction, the KYC requirements caused complaints by Bahamians who were unable to produce adequate documentation when attempting to open accounts in domestic banks. (The absence of house numbers on most Bahamian streets, the prevailing practice of utility companies issuing bills only in the name of landlords rather than tenants, and the scarcity of picture identification among Bahamians contributed to these documentation problems.) In October 2002, the Minister of Financial Services and Investments, a post created by the Progressive Liberal Party (PLP) government elected in April 2002, lamented that the rigid, overly prescriptive requirements of the KYC rules had caused financial institutions to harass long-standing, well-known clients for documents and observed that those rules had been applied to accounts of low-risk customers, including pensioners, whose opportunities for money laundering were minimal.

The Tracing and Forfeiture/Money Laundering Investigation Section of the Drug Enforcement Unit of the Royal Bahamas Police Force is the primary financial law enforcement agency in the Bahamas, with the responsibility for investigating suspicious transaction reports received from the FIU. This agency is also responsible for investigating all reports of money laundering in the Bahamas received from law enforcement agencies or the public. Furthermore, this agency investigates matters of large cash seizures, in addition to investigating local drug traffickers and other serious crime offenders to determine whether they benefited from their criminal conduct. From January through May 2002 the FIU forwarded 15 suspicious transactions reports to the Tracing and Forfeiture/Money Laundering Investigation Section. Eleven of the reports were investigated and one was forwarded to the Commercial Crime Section for further investigation. The Tracing and Forfeiture/Money Laundering Investigation Section also investigated matters involving seized cash during 2002. Several of these cases are currently before the courts.

The Central Bank of the Bahamas Act 2000 expanded the powers of the Central Bank to enable it to respond to requests for information from overseas regulatory authorities, and gave the Bank’s Governor the right to deny licenses to banks or trust companies he deems unfit to transact business in the Bahamas. The primary impact on the offshore sector has been the weeding out of many of the “managed” or “shell” banks that had no actual physical presence in the Bahamas. During 2001, the Governor revoked the licenses of 55 of these banks, including the British Bank of Latin America and the Federal Bank, both identified in a U.S. Senate Report as being at high risk of involvement in money laundering, and Al-Taqwa Bank, which in October 2001 was placed on the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 (on terrorist financing).

At the beginning of 2001, there were some 100,000 incorporated international business companies (IBCs) in the Bahamas. The International Business Companies Act 2000 eliminated anonymous ownership of IBCs by prohibiting bearer shares and imposing KYC requirements. As a result, the Bahamas became less attractive to both potential and existing IBC owners. During the first nine months of 2001, the number of new IBCs registered in the Bahamas was down to 4,148, compared to 14,454 during the same period of 2000. In February 2002, the GCOB approved the employment of nine persons in the Registrar General’s Department to assist in reviewing the 90,000 IBC files to verify the companies’ compliance with the provisions of the International Business Companies Act 2000. The project began on April 8, 2002, and continued through the year.

The Bahamas has two casinos in Nassau and one in Freeport/Lucaya, and a license for a fourth casino on San Salvador has been approved. Annual revenues for the three existing casinos are estimated at \$196 million. Cruise ships that overnight in Nassau may operate casinos. Betting in casinos on sporting events

is allowed except on horse races. There are no Internet gambling sites based in the Bahamas. Under Bahamian law, Bahamian residents cannot gamble in the casinos.

As of March 2002, there were 56 local insurers and 30 offshore insurance companies in the Bahamas. At the beginning of 2002 there were 724 Bahamas-based mutual funds (down 4 percent from 757 at the start of 2001) with a net asset value of \$94 billion.

While most money laundering in the Bahamas is narcotics related, a major money laundering case, that of prominent Bahamian attorney Leslie Vernon Rolle, is related to a \$1.7 million financial fraud scheme. (That much-delayed prosecution is scheduled for trial in the Supreme Court in 2003.)

Some Bahamian bankers contend that under the strengthened anti-money laundering regulations, it is more difficult to make deposits in a Bahamian bank than in other jurisdictions. That this increased strictness may have driven drug traffickers to keep cash in their homes and vehicles is supported by police seizures of large sums of drug-related money in those places in 2001 and 2002. According to the Royal Bahamas Police Force (RBPF), two trends characterized money laundering in the Bahamas in 2002: an increasing “professionalization” of money laundering by the use of professionals in the business and financial sectors, and the prevalent use of cash intensive businesses as fronts for co-mingling illegal gains with legitimate receipts. The RBPF noted that professional money launderers now receive a standard fee of 20 percent of the funds being laundered. The RBPF also cited the use of businesses such as restaurants, small hotels, bars, nightclubs, retail outlets, construction companies, and concert performances as fronts. The RBPF listed several “less creative” money laundering methods employed in the Bahamas, including purchasing of vehicles, placing properties and assets in the names of spouses, children and parents, paying small businesses to prepare false receipts, storing cash in safety deposit boxes, and attempting to smuggle money into the Caribbean and the United States in boxes, luggage, or strapped to the body.

The Bahamas FIU became a member of the Egmont Group in June 2001. The Bahamas FIU and the Belgian FIU signed a memorandum of understanding on November 30, 2001, to exchange information between the two units. The Bahamas FIU has also approached the FIU of Aruba and the Netherlands Antilles to begin drafting a memorandum of understanding. As a result of the Financial Intelligence Unit (Amendment) Act 2001, the Financial Intelligence Unit is now able to cooperate and render assistance to any foreign Financial Intelligence Unit that performs functions similar to the Financial Intelligence Unit and not only those units that are members of the Egmont Group.

On October 2, 2001, the Bahamas signed, but not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism. A Terrorism Bill is being drafted to present to Parliament. This Bill is intended to implement the provisions of the UN terrorism conventions and the UN Security Council Resolutions dealing with terrorism and terrorism financing. The Bahamas also participated in the FATF Self-Assessment Exercise on Terrorist Financing, and submitted the Self-Assessment Questionnaire to FATF in May 2002.

In April 2001, the Bahamas signed, but has not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. The Bahamas has a Mutual Legal Assistance Treaty with the United States, which entered into force in 1990, and also with the United Kingdom and Canada. The Attorney General has established an International Affairs Unit to deal specifically with mutual legal assistance matters. The Bahamas is party to the 1988 UN Drug Convention, currently sits as President of the Caribbean Financial Action Task Force, and is a member of the Offshore Group of Banking Supervisors.

The GCOB has enacted substantial reforms that could reduce its financial sector’s vulnerability to money laundering. The GCOB should continue to further its anti-money laundering efforts by criminalizing the financing of terrorists and terrorism. The Bahamas should continue with the enforcement of the anti-money laundering legislation and international cooperation.

Bahrain. Bahrain has one of the most diversified economies in the Gulf Cooperation Council (GCC). Unlike its neighbors, oil accounts for only 18 percent of Bahrain’s gross domestic product (GDP). Bahrain

Money Laundering and Financial Crimes

has promoted itself as an international financial center in the Gulf region. It hosts a mix of 178 diverse financial institutions, including 51 offshore banking units (OBUs), 34 investment banks, of which 16 specialize in Islamic banking, and 22 commercial banks, of which 14 are foreign owned. In addition, there are 34 representative offices of international banks, 17 money exchangers, four money brokers, and several other investment institutions. The vast network of its banking system, along with its geographical location in the Middle East as a transit point along the Gulf and into Southwest Asia may attract money laundering activities. It is thought that the greatest risk of money laundering stems from questionable foreign proceeds that transit Bahrain.

In January 2001, the Government of Bahrain (GOB) enacted a new anti-money laundering law that criminalizes the laundering of proceeds derived from any predicate offense. The law stipulates punishment of up to seven years in prison and a fine of up to one million dinars (\$2.65 million) for convicted launderers and those aiding or abetting them. If organized criminal affiliation, corruption, or disguising the origin of proceeds is involved, the minimum penalty is a fine of at least 100,000 dinars (approximately \$265,000) and a prison term of not less than one year.

Following enactment of the law, the Bahrain Monetary Agency (BMA), as the principal regulator, issued regulations requiring financial institutions to report suspicious transactions, to maintain records for a period of five years, and to provide ready access to account information to law enforcement officials. Immunity from criminal or civil action is given to those who report suspicious transactions. Even prior to the enactment of the new anti-money laundering law, financial institutions were obligated to report suspicious transactions greater than 6,000 dinars (approximately \$15,000) to the BMA.

The new law also provides for the formation of an interagency committee to oversee Bahrain's anti-money laundering regime. Accordingly, in June 2001, the National Anti-Money Laundering Policy Committee was established and assigned the responsibility for developing anti-money laundering policies and guidelines. The committee includes members from the BMA, the Bahrain Stock Exchange, and the Ministries of Finance, Interior, Justice, and Commerce. The new law further provides additional powers of confiscation, and allows for better international cooperation.

The law also provides for the creation of a Financial Intelligence Unit (FIU), known as the Anti-Money Laundering Unit (AMLU), which is housed in the Ministry of Interior. AMLU is empowered to receive reports of money laundering offenses, conduct investigations, implement procedures relating to international cooperation under the provisions of the law, and to execute decisions, orders and decrees issued by the competent courts in offenses related to money laundering.

There are 51 BMA-licensed offshore banking units (OBUs) that are branches of international commercial banks. Unlike other banks, these OBUs are exempt from foreign-exchange controls, cash reserve requirements, taxes on interest paid to depositors, and banking income taxes. Such treatment only applies to non-dinar denominated deposits. In exchange for these privileges, OBUs pay the government annual license fees, are prohibited from accepting deposits from citizens and residents of Bahrain, and must refrain from transactions involving Bahraini dinars. The OBUs are required by law to be audited yearly by outside firms, to have records available for examination by the BMA, and to submit statistical reports to the BMA twice a year.

Bahrain law permits the formation of offshore resident companies and offshore non-resident companies that are formed as international business companies (IBCs). Resident companies must have an office within Bahrain, a minimum capital of \$54,000, and a license from the BMA, in order to conduct financial activities.

Bahrain is a member of the GCC, which is a member of the Financial Action Task Force (FATF). In June 2000, Bahrain underwent a FATF mutual evaluation. Bahrain is also a member of the Offshore Group of Banking Supervisors and has agreed to undergo a mutual evaluation by this body. In January 2002, BMA issued a circular intended to implement the FATF Special Eight Recommendations on Terrorist Financing. BMA requested of its licensees that the FATF recommendations be considered part of the

Agency's money laundering regulations. In November 2001, Bahrain signed the UN International Convention for the Suppression of the Financing of Terrorism, but has not yet become a party to it. Terrorist financing is a predicate offense in Bahrain under Articles 1 and 2 of Law No. 4. In exercise of the Royal Prerogative, Law 4 empowers the GOB to issue Prime Ministerial Edicts to seize and confiscate assets used to finance terrorism. The BMA has frozen one account designated by the UN 1267 Sanctions Committee and six accounts listed under U.S. Executive Order 13224.

BMA Circular BC/1/2002 states that money changers may not transfer funds for customers in another country by any means other than Bahrain's banking system, under pain of legal sanctions. In addition, all BMA licensees are required to include details of 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 originator's information, as they are presumed to be suspicious transactions. Licensees that suspect, or have reasonable grounds to suspect, that funds are linked or related to suspicious activities—including terrorist financing—are required to file suspicious transaction reports (STRs). Licensees must maintain records of the identity of their customers in accordance with the agency's money laundering regulations, as well as the exact amount of transfers. The BMA requires all money exchanges to produce such information upon request. BMA regulations require high-value goods and bullion dealers to file STRs with the AMLU. The government is considering extending its STR reporting regime to encompass more sectors.

Decree No. 21 of 1989 governs the licensing of non-profit organizations. The Ministry of Labor and Social Affairs (MLSA) is responsible for licensing and supervising the charity organization in Bahrain. The BMA—in consultation with Ministries of Labor, Justice, and Finance and National Economy—is working on a draft regulation for charity organizations in order to insure that such organizations are not being used to finance illegal activities. Under the draft regulation, organizations must keep records of sources and uses of financial resources, organizational structure, and membership. Charitable societies are required to deposit their funds with banks located in Bahrain, and to report any changes in banking relations within a week. MLSA has the right to inspect records of the societies to insure their compliance with the laws.

Bahrain is a leading Islamic finance center in the region. Since the licensing of the first Islamic bank in 1979, the sector has grown considerably, today having 26 Islamic banks and financial institutions. Given the large share of such institutions in Bahrain's banking community, BMA is working to create an appropriate framework for regulating and supervising the Islamic banking sector, applying regulations and supervision as is the case with conventional banks. For example, in March 2002, the BMA developed the Prudential Information and Regulatory Framework for Islamic Banks (PIRI) that seeks to monitor the operations of the banks.

Bahrain has undertaken a number of significant steps in establishing an anti-money laundering regime. The GOB should follow through by enforcing the law and developing and prosecuting anti-money laundering cases. Its officials have attended orientation and training sessions in Bahrain and international locations. The new FIU will need time to train staff and gain experience in tracking suspicious transactions, and law enforcement will need to develop expertise in investigating money laundering offenses.

Bangladesh. Bangladesh is not an important regional financial center. There are no indications that substantial funds are laundered through the official banking system. The principal vulnerability remains the widespread use of the underground hawala or hundi system to transfer value outside the formal banking network. The vast majority of the hawala systems in Bangladesh are used to repatriate wages from Bangladeshi workers abroad. However, the hawala systems are also used to avoid taxes, customs duties and currency controls and as a compensation mechanism for the significant amount of goods smuggling into Bangladesh. There have been substantial seizures of gold at Bangladeshi ports this past year, which could be related to gold's use in the region to provide counter-valuation in hawala transactions.

Money Laundering is a criminal offense. In April 2002, Bangladesh enacted the Money Laundering Prevention Act (MLPA) that applies to all forms of money laundering. The MLPA authorizes the

Money Laundering and Financial Crimes

country's Central Bank, the Bangladesh Bank, to supervise the activities of banks, investigate all offenses related to money laundering, and take appropriate steps to address any problems. The MLPA requires financial institutions to accurately identify customers and to report suspicious transactions to Bangladesh Bank. The MLPA imposes penalties for money laundering and allows the Bangladesh Bank to fine financial institutions no more than 100,000 taka (less than \$2000) for failure to retain or report the required data on suspicious transactions. Because the MLPA has been enacted recently, banks in Bangladesh have not yet established implementing procedures.

Monetary exchanges outside the formal banking system are illegal. Bangladesh has not addressed the issue of international transportation of illegal-source currency and monetary instruments. Offshore financial accounts are not permitted in Bangladesh. There is no asset forfeiture law. Bangladesh does not have a Financial Intelligence Unit (FIU). There has been no known money laundering arrests or prosecutions in Bangladesh.

Bangladesh does not have a law that makes terrorist financing a crime. No terrorist assets have been identified, frozen, or seized to date. Bangladesh has not signed the UN International Convention for the Suppression of the Financing of Terrorism. Bangladesh is a party to the 1988 UN Drug Convention, and is a member of the Asia/Pacific Group on Money Laundering.

Bangladesh should criminalize terrorist financing. It should also create a centralized FIU to receive suspicious transaction reports and disseminate information to law enforcement. Training should also be given to law enforcement and customs authorities on how to recognize money laundering crimes and initiate investigations from the field. Customs should create a central computerized database that could help to counteract customs fraud, trade-based money laundering, and smuggling. Training should also be given to prosecutors and judicial authorities in order to enhance their understanding of money laundering and their ability to enforce the new MLPA.

Barbados. As a transit country for cocaine and heroin, Barbados is both attractive and vulnerable to money launderers. The Government of Barbados (GOB) has taken a number of steps in recent years to strengthen its anti-money laundering regime.

The GOB initially criminalized drug money laundering in 1990 through the Proceeds of Crime Act, No. 13, which also authorized asset confiscation and forfeiture, permitted suspicious transaction disclosures to the Director of Public Prosecutions and exempted such disclosures from civil or criminal liability. The Money Laundering (Prevention and Control) Act 1988 (MLPCA) criminalized the laundering of proceeds from unlawful activities that are punishable by at least one year imprisonment. The MLPCA made money laundering punishable by a maximum of 25 years in prison and a maximum fine of Barbadian dollars (BDS) 2 million (approximately \$1 million). The law also provided for asset seizure and 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.

The MLPCA applies to a wide range of institutions, including domestic and offshore banks, international business companies (IBCs) and insurance companies. These institutions are required to identify their customers, cooperate with domestic law enforcement investigations, maintain records of all transactions exceeding BDS 10,000 (approximately \$5,000), and report suspicious transactions to the Anti-Money Laundering Authority (AMLA). The AMLA forwards this information to the Commissioner of Police if it has reasonable grounds to suspect money laundering. Financial institutions must also establish internal auditing and compliance procedures. The MLPCA sets forth seizure and criminal forfeiture procedures.

The definition of a financial institution was widened in an amendment to the MLPCA in 2001 to include "any person whose business involves money transmission services, investment services or any other services of a financial nature." This amendment was designed to bring entities other than traditional

financial institutions into the class of persons or institutions that are supervised by the AMLA, and therefore, subject to the requirements of the MLPCA.

The AMLA was established in August 2000 to supervise financial institutions' compliance with the MLPCA and issue training requirements and regulations for financial institutions. The AMLA's FIU was established in September 2000. The FIU is now fully staffed and operational. It was admitted to the Egmont Group in 2002.

Barbados has achieved be the only money laundering conviction in the Eastern Caribbean2002. The money laundering conviction was in relation to a fraud scheme.

The Barbados Central Bank's 1997 Anti-Money Laundering Guidelines for Licensed Financial Institutions were revised in 2001. The revised Know—Your Customer Guidelines were issued in conjunction with the AMLA, and provide detailed guidance to financial institutions regulated by the Central Bank. The Central Bank undertakes regular on-site examinations of licensees and applies a comprehensive methodology that seeks to assess the level of compliance with legislation and guidelines.

The Offshore Banking Act (1980) gave the Central Bank authority to supervise and regulate offshore banks, in addition to domestic commercial banks. The International Financial Services Act replaced the 1980 Act in June 2002 in order to incorporate fully the standards established in the Basel Committee's "Core Principles for Effective Banking Supervision." The new law provides for on-site examinations of offshore banks. This allows the Central Bank to augment its offsite surveillance system of reviewing anti-money laundering policy documents and analyzing prudential returns. The Ministry of Finance issues banking licenses after the Central Bank receives and reviews applications, and recommends applicants for licensing. Offshore banks must submit quarterly statements of assets and liabilities and annual balance sheets to the Central Bank. Supervision of the financial sector is shared among the Central Bank, the Ministry of Commerce, Consumer Affairs and Business Development, the Supervisor of Insurance, the Registrar of Cooperatives and the Barbados Securities Commission.

As of November 30, 2002, six domestic banks (Barbadian, Canadian-parent, and U. K.-parent banks operate on equal terms in Barbados), 14 finance companies or merchant banks and 55 offshore banks were regulated and supervised by the Central Bank. The offshore sector also includes 4,206 international business companies (IBCs), 392 exempt insurance companies, and 1,575 foreign sales corporations (FSCs), specialized companies that permit persons to engage in foreign trade transactions from within Barbados. The Foreign Sales Corporation Act, which authorized establishment of FSCs, was repealed in 2000.

The International Business Companies Act (1992) provides for general administration of IBCs. The Ministry of International Trade and Business vets and grants licenses to IBCs after applicants register with the Registrar of Corporate Affairs. Bearer shares are not allowed and financial statements of IBCs are audited if total assets exceed \$500,000.

Barbados has bilateral tax treaties that eliminate or reduce double taxation with the United Kingdom, Canada, Finland, Norway, Sweden, Switzerland, and the United States. The treaty with Canada currently allows IBCs and offshore banking profits to be repatriated to Canada tax-free after paying a much lower tax in Barbados. A Mutual Legal Assistance Treaty and an Extradition Treaty between the United States and Barbados each entered into force in 2000. Barbados is a member of the Offshore Group of Banking Supervisors, the Caribbean Financial Action Task Force and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Barbados is a party to the 1988 UN Drug Convention. Barbados signed, but has not yet ratified, the UN Convention Against Transnational Organized Crime, which is not yet in force internationally. Barbados is a party to the UN International Convention for the Suppression of the Financing of Terrorism.

No evidence of terrorist financing has been known to be developed in Barbados. The GOB has not taken any specific initiatives focused on alternative remittance systems or the misuse of charitable and non-

Money Laundering and Financial Crimes

profit entities. The Barbados Anti-Terrorism Act, 2002-6, Section 4, gazetted on May 30, 2002, criminalizes the financing of terrorism.

The GOB should maintain strict control over vetting and licensing of offshore entities. The GOB should continue its efforts to prosecute and convict money launderers. The establishment of the AMLA and continued development of the AMLA's Financial Intelligence Unit should provide Barbados with the necessary tools to enforce compliance by financial and commercial sectors, and enable it to cooperate fully with foreign authorities to investigate and prosecute money laundering and other financial crimes.

Belarus. The absence of anti-money laundering laws or regulations makes Belarus vulnerable to money laundering. Banks are more inclined to focus on protecting the secrecy of their clients than on discovering and reporting irregular or unaccounted-for deposits. The growing number of casinos also could become venues for money laundering.

Belarus faces problems with organized crime that plague other countries of the former Soviet Union. The lack of anti-money laundering laws could lead organized crime to engage in more substantial money laundering in Belarus. Belarus made no effort in 2002 to enact an anti-money laundering regime.

Belarus has signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism. Belarus is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Belarus should enact comprehensive anti-money legislation that criminalizes money laundering and the financing of terrorists and terrorism.

Belgium. Belgium has a very comprehensive anti-money laundering regime. Despite this, Belgium's financial system remains vulnerable to money laundering. Most of the money laundering cases detected in Belgium are related to narcotics-trafficking, particularly with its neighboring countries, the Netherlands, Luxembourg, Germany, and France. According to a 2001-2002 report from Belgium's Financial Intelligence Unit (FIU), the Financial Intelligence Processing Unit (CTIF-CFI), the largest share of money laundering cases between July 1, 2001, and June 30, 2002, was connected to the unlawful trafficking in goods and merchandise, mainly automobiles, alcohol, and tobacco. There were also a growing number of cases tied to organized crime, fiscal fraud, prostitution, and human trafficking.

The main money laundering techniques are through bureaux de change, international fund transfers and payments, and payments into accounts. The top three venues are bureaux de change, credit establishments, and brokerage firms. Funds are also laundered through the diamond industry, real estate, offshore companies, gambling or amusement halls, and banks. Belgian officials noted in recent reports that "dummy companies," or front companies, figured prominently in cases turned over to legal authorities for prosecution for money laundering. They also stated that money launderers attempt to use notaries to create such companies or to buy property. They use such methods as selling property below its market value, making significant investments on behalf of foreign nationals with no connections to Belgium, making client property transactions whose value is disproportionate to the socio-economic status of the client, and creating a large number of companies in a short space of time.

On January 1, 2002, the FIU entered into an agreement with the Federal Police to expedite cases to the Public Prosecutor that are the focus of an active police investigation. The Government of Belgium (GOB) in 1990 criminalized money laundering related to all crimes. In 1993, it passed additional legislation that mandated reporting of suspicious transactions by financial institutions, and created the CTIF-CFI as its FIU, to receive, process, and analyze them. Since the founding of CTIF-CFI, 659 individuals have been successfully prosecuted under Belgian law, receiving combined total sentences of 1,332 years and 14.2 million euros in fines (approximately \$14.2 million). During the same time period Belgian authorities confiscated nearly 360 million euros. As of June 2002, the CTIF-CFI had created 12,948 distinct case files (representing 66,963 suspicious transaction reports) since becoming operational in 1993, including 2,845 between July 2001 and June 2002. During that time period over 1,045 files were turned over to the Public

Prosecutor. A total of 42 money laundering cases amounting to 2.8 million euros (approximately \$2.8 million), which were connected to the January 1, 2002, introduction of the euro, were submitted to the Public Prosecutor.

Belgian financial institutions are required to 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 \$10,000). Financial institutions also are required to train their personnel in the detection and handling of suspicious transactions that could be linked to money laundering. No civil, penal, or disciplinary actions can be taken against institutions or individuals for reporting such transactions in good faith. Non-reporting and non-compliance with other requirements of the 1993 law are punishable by a fine of up to 1.25 million euros, approximately \$1.25 million. Furthermore, a law adopted on April 8, 2002, increases the protection accorded to witnesses, including bank employees, who come forward with information about money laundering crimes.

In 1998, the GOB adopted legislation that mandates the reporting of suspicious transactions by notaries, accountants, bailiffs, real estate agents, casinos, cash transporters, external tax consultants, certified accountants, and certified accountant-tax experts. Under the legislation, casinos include any establishments that conduct casino-like gambling activities. CTIF-CFI has observed a marked increase in casino chip purchasing operations, much of it tied to Central and Eastern European organized crime syndicates. There is concern that casino operators are not keeping adequate records of the buying and selling of chips, or of customer identification documents, as required under the anti-money laundering law.

The GOB passed a new law on May 3, 2002, giving Belgium the authority to invoke countermeasures against “Non-Cooperative Countries and Territories” imposed by FATF. The GOB issued its countermeasures against Nauru in a June 10, 2002 Royal Decree. The May 2002 law also imposes further limitations on the operations of bureaux de change.

In July 2002 the Belgian Council of Ministers approved a proposal to establish, as part of Belgian domestic law, the Directive 2001/97/EC of the EU Parliament and Council of December 4, 2001, amending the Council Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering. Belgian law currently mandates that all financial institutions, and non-financial persons subject to the Belgian anti-money laundering law, be obliged to send an STR if there is a suspicion that the origin of money or assets is derived from the commission of an offense linked to terrorism. The new proposal of law extends this reporting obligation to the funds suspected of being derived from the financing of terrorism. Moreover, this new proposal extends the obligations of the anti-money laundering system to lawyers and dealers in diamonds.

On September 27, 2001, Belgium signed the UN International Convention for the Suppression of the Financing of Terrorism. The ratification process is in abeyance, pending Senate approval. Belgium intends to implement legislation by mid-2003 that would bring its domestic laws in line with the EU Council Common Position 2001/930 of December 27, 2001, on the application of specific measures to combat terrorism. Article 1 of Common Position 2001/930 requires that EU member states criminalize the willful provision or collection of funds to carry out terrorist acts. Under EU law, most recently EU Council Regulation No. 881/2002 of May 27, 2002, Belgium has implemented UN resolutions 1267 (1999), 1333 (2000) and 1390 (2002), imposing certain restrictive measures directed against persons and entities associated with Usama Bin Ladin, the al-Qaida network, and the Taliban. Belgium is also subject to enforcing Council Regulation No. 2580/2001 of December 27, 2001, which obligates EU member states to freeze the funds of individuals and entities listed in the Annex to the Council Common Position 2001/931 of December 27, 2001, and which are subject to the EU’s asset-freeze regulation.

CTIF-CFI is actively involved in the fight against terrorism and its financing. Belgium has circulated the list of Specially Designated Global Terrorists named by the United States pursuant to E.O. 13224. The GOB, however, lacks the executive-type powers that U.S. authorities have under Executive Order 13324 to administratively freeze accounts. As such, the GOB can freeze accounts with respect to any individual

Money Laundering and Financial Crimes

or entity only after those individuals or entities have been added to the UN Consolidated List pursuant to Security Council resolutions 1267, 1333 and 1390 and/or covered by an EU asset freeze regulation.

CTIF-CFI is currently investigating several cases of terrorist financing-related money laundering. These have involved both apparently legitimate sources (involving businesses acting as fronts or collected from associations with purported social, charitable, or cultural purposes) and illegal ones (involving illegal drugs, fiscal fraud, and diamond trafficking, among other activities). As of December 31, 2002, a total of 55 such cases have been transmitted to the Public Prosecutor, 49 of which (37.52 million euros) were forwarded following September 11, 2001. These funds originate from both legal and illicit activities. According to a CTIF-CFI report, there is growing evidence that some Belgian-based non-governmental organizations (NGOs) are being used to funnel terrorist funds. CTIF-CFI has identified financial links in Belgium to al-Qaida, and the FIU has indicated that addressing the problem of terrorist financing has become one of its highest priorities.

The Belgian FIU organized a meeting in October 2001 in Brussels that the 15 FIUs of the European Union attended. The purpose of the meeting was to enhance cooperation between the FIUs in their fight against the financing of terrorism.

Belgium is a party to the 1988 UN Drug Convention, and in December 2000 signed the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Belgium has a Mutual Legal Assistance Treaty with the United States, which entered into force on January 1, 2000. The GOB exchanges information with other countries through international treaties. Belgium is a member of the Financial Action Task Force (FATF) and the European Union. The CTIF-CFI is a member of the Egmont Group and has a cooperative relationship with 50 foreign FIUs worldwide.

Belgium should criminalize terrorist financing to enhance its comprehensive anti-money laundering regime. Through the enhanced scrutiny law enforcement agencies are devoting to all sectors of the global economy that may be abused by terrorist organizations and their supporters, the smuggling of diamonds and gems has been identified as a sector through which it is easy to move across international borders without detection. For that reason, the GOB should exert vigilance with regard to its diamond market to prevent its being used as a means to finance terrorism.

Belize. Belize's proximity to Mexico and Guatemala has made it a significant transshipment point for illicit drugs, notably cocaine and marijuana. Belize's growing offshore sector has seven offshore banks, an unknown number of international trusts, over 18,000 international business companies (IBCs), and an Internet gaming site. The transshipment of drugs and the growing offshore sector, regulated by those who promote it, make Belize vulnerable to money laundering.

Belize is aware that contraband smuggling generates funds that are laundered through the banking system; however, authorities believe that the funds are insignificant in amount and not related to narcotics money laundering. Belize believes that criminal proceeds are derived primarily from foreign criminal activity. To date all evidence of money laundering is the result of foreign criminal activity utilizing the services of the offshore financial sector.

The Money Laundering Prevention Act (MLPA), in force since 1996, criminalizes money laundering related to many serious crimes including arms and narcotics trafficking, fraud, extortion, terrorism, blackmail, and certain theft involving more than \$10,000. The Act also provides mechanisms for the freezing and forfeiture of assets; requires that all licensed financial institutions know their customers; mandates the recording of large currency transactions and the reporting of suspicious transactions by banks and non-bank financial institutions (exchange houses, insurance companies, lawyers, accountants but not casinos); exempts employees of financial institutions from civil, criminal or administrative liability for cooperating with regulators and law enforcement officials in investigating money laundering; specifies penalties for banks, non-bank financial institutions and intermediaries who assist and collaborate in money laundering; and authorizes international cooperation in money laundering cases. Additionally, persons

departing Belize must declare B\$20,000 (approximately \$5,000) or more in cash or negotiable bearer instruments.

Financial institutions are required to report complex, unusual, or large business transactions to the Governor of the Central Bank. Supporting Regulations and Guidance Notes were issued in 1998. The Central Bank forwards any reports warranting further investigation to the Director of Public Prosecutions (DPP) Office. Financial institutions are required to retain records for a minimum of five years, and can lose their licenses and face a maximum fine of \$50,000 for failing to do so. Individual bankers can be held responsible if their institutions are caught laundering money. However, bankers are protected from prosecution if they cooperate with law enforcement. Financial institutions must also comply with instructions from the Central Bank, and permit the Supervisory Authority to enter and inspect records.

The gaming industry is not regulated under the MLPA. Neither the Gaming Control Act, 1999, nor the Computer Wagering Licensing Act, 1995, require reporting of suspicious activity reports. The Government of Belize (GOB) has established legislation that facilitates computer and casino gaming; however, the legislation makes no provision for due diligence procedures, record keeping, or suspicious transactions reporting.

The International Financial Services Commission (IFSC) serves as the regulator for Belize's offshore sector. Members of the IFSC consist of individuals from the private and public sector. The IFSC promotes, protects, and enhances Belize as an offshore center. It also regulates and supervises the provision of international financial services within Belize through formulation of appropriate policies and the provision of advice to government on regulatory matters. The IFSC does not regulate domestic and offshore banks that are supervised by the Central Bank.

IBCs are regulated under the International Business Companies Act of 1990 and amendments to the Act issued in 1995 and 1999. The 1999 amendment to the IBC Act allows properly licensed IBCs to operate as banks and insurance companies. Registered agents have primary responsibility for the registration and ongoing operations of the IBCs registered in Belize. There is no legal requirement for identification of beneficial ownership or directors of IBCs to be disclosed to the registrar. Offshore banks are not permitted to issue bearer shares. IBCs are allowed to issue bearer shares; the registered agents of such companies must know the identity of the beneficial owner of the shares.

The Offshore Banking Act, 1996 (OBA), governs activities of Belize's offshore banks. The Act generally prohibits offshore banks from transacting business with residents of Belize. There are minimum capital requirements under the OBA and the shares of offshore banks must be in registered form and not in bearer form. Offshore banking licenses are granted by the Minister of Finance on the recommendation of the Central Bank, which has supervisory powers over both domestic and offshore banks. With regard to the offshore banks, the supervisory role of the Central Bank is restricted to the licensee's operations in Belize. The Central Bank has no access to information regarding a customer, depositor or transaction, except in case of large credit exposures.

Offshore trusts are governed under the Belize Trust Act, 1992, and are also prevalent in Belize. Registration with a regulatory body is not required. Although the Central Bank is the supervisory authority with regard to money laundering, there are no legal requirements to provide account information or activity regarding trusts to the Central Bank. While the GOB maintains that trusts are well regulated, it is important to note that the authorities do not know how many trusts are in operation and that no additional measures are being contemplated to thwart the potential misuse of charitable and/or non-profit entities, such as charitable trusts, that can be used as conduits for the financing of terrorism.

Under Belizean law all assets related to money laundering may be forfeited. This includes vessels, vehicles, aircraft and other means of transportation or communication. It also includes property tangible or intangible that may be related to money laundering. There are no limitations to the kinds of property that may be seized, but there are no specific provisions allowing for sharing of seized assets between cooperating foreign authorities.

Money Laundering and Financial Crimes

Belizean authorities have assisted foreign authorities with money laundering investigations. Belize's Police Department (BPD) has assigned five persons to investigate money laundering cases. This unit will serve as the Financial Intelligence Unit. An office space, separate from the police department, has been designated for this unit.

Belize has criminalized terrorist financing with amendments to its anti-money laundering legislation, the Money Laundering Prevention Act. Belize authorities have the power to identify, freeze, and seize terrorist finance assets. Authorities have also circulated to all financial institutions lists of persons alleged to be involved with terrorist financing. None of those on the list have been reported to be engaged in financial transactions in Belize, and no assets belonging to persons alleged to be engaged in terrorist financing have been identified in Belize.

The MLPA provides for the provision of legal assistance to a foreign country when there is bilateral or multilateral treaty in force providing for mutual legal assistance. Whenever possible, the Belize authorities have cooperated with U.S. Government agencies—most specifically with the FBI, Securities and Exchange Commission, U.S. Commodities Futures Trading Commission, and various state and regulated agencies. However, because the MLAT between Belize and the United States is not yet in force, in 2001, a court in Belize ordered that no legal assistance could be provided in a money laundering case. No arrests or prosecutions pertaining to money laundering or terrorist financing have occurred in Belize since January 2002.

Belize is a party to the 1988 UN Drug Convention. Belize has signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism. Belize is a member of the Caribbean Financial Action Task Force and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Belize signed a Mutual Legal Assistance Treaty (MLAT) with the United States. Belize has ratified the MLAT and the United States is expected to do so in 2003. Belize also has bilateral agreements with the United Kingdom and Canada.

The GOB will remain vulnerable to money launderers as long as IBCs can issue bearer shares without disclosure of the beneficial owner. The GOB should also increase its monitoring to ensure that charitable trusts are not vulnerable to abuse by terrorists. The GOB should monitor the Internet and casino gaming industry and require suspicious activity reporting to prevent potential money launderers from using these sectors to launder funds. Additionally, the GOB should provide the Financial Intelligence Unit sufficient resources and staff needed to receive, analyze, and disseminate suspicious transaction reports.

Benin. Benin is not a major financial center. However, Government of Benin (GOB) officials believe narcotics traffickers use Benin to launder proceeds. Although the exact nature of money laundering is unknown, GOB officials suspect that the primary methods are through the purchase of assets such as real estate, the wholesale shipment of vehicles or items for resale, and front companies. In addition, some laundering seems to occur through the banking system.

A 1997 counternarcotics law criminalizes narcotics-related money laundering, and provides penalties of up to 20 years in prison as well as substantial fines. The law requires that all financial institutions report transactions above a certain threshold, although compliance with this provision of the law is believed to be low. Cross-border currency reporting requirements exist, but are not enforced.

The GOB has the legal authority to seize narcotics-related assets, but no seizures have been made. Law enforcement authorities lack the training and resources to investigate money laundering cases.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA) based in Dakar, Senegal. In November 2002 GIABA hosted an anti-money laundering seminar for representatives of 14 ECOWAS members, including Benin.

Benin is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Benin's

National Assembly ratified the UN International Convention for the Suppression of the Financing of Terrorism on October 28, 2002.

Benin should criminalize terrorist financing and money laundering related to all serious crimes. Benin should also develop and enforce a viable anti-money laundering regime.

Bermuda. Bermuda, an overseas territory of the United Kingdom (UK), is considered a major offshore financial center and has a reputation, among offshore financial centers, for the integrity of its financial regulatory system. The government of Bermuda (GOB) has been cooperating with the United States and the international community in its money laundering and counter-terrorism efforts.

In 1997, the GOB enacted the Proceeds of Crime Act (PCA). The PCA applies money laundering controls to financial institutions such as banks, deposit companies, trust companies, and investment businesses, including broker-dealers and investment managers. Insurance companies are covered to the extent that they are doing higher risk business. Amendments in 2000, effective June 1, 2001, extended the scope of the legislation beyond the laundering of drug-related moneys to cover the proceeds of all indictable offenses, including tax evasion, corruption, fraud, counterfeiting, theft and forgery. It is likely that when the PCA is amended, which is expected to occur in 2003, the law will be expanded to address terrorist-related assets and to cover gatekeepers, such as attorneys and accountants.

One shortcoming of the current law is that it does not provide measures to detect/monitor cross-border transportation of cash. However, if there are reasonable grounds for suspicion, HM Customs is authorized to seize cash and instruments, and monies can also be seized if travelers fail to report the transportation of cash in excess of \$10,000. The GOB is consulting with industry groups on proposals to enact remedial legislation to govern the transportation of cash.

In addition to the PCA, which has encountered virtually no objections from the financial sector and has not resulted in a decline in deposits, other Bermuda statutes address money laundering. The Criminal Justice (International Co-Operation) (Bermuda) Act 1994, as amended in 1996, provides assistance upon requests from overseas agencies, including securing of evidence in Bermuda and overseas. It directs responsibility for the criminal aspects of financial crime to the Financial Investigation Unit, whereas tax offenses fall under the purview of the Attorney General.

The Investment Business Act 1998 authorizes the Bermuda Monetary Authority (BMA) to obtain any information deemed necessary by regulators to conduct their supervision of investment providers, who are fully subject to know-your-customer requirements under the PCA and its regulations. The BMA's supervision of investment providers includes specific on-site testing of their systems and controls, including their compliance with anti-money laundering requirements. The GOB will propose a new Investment Business Bill in 2003 to enhance its regulatory powers, including revisions expanding the BMA's authority to cooperate with foreign regulatory bodies. There will be no change in the anti-money laundering provisions or in the BMA's compliance testing regime.

As of January 1, 2000, the Banks and Deposit Companies Act 1999 implements the Basel Committee's "Core Principles for Effective Banking Supervision." The BMA is the designated entity for licensing and supervision of deposit-taking institutions, including the worldwide operations of Bermudian banks. As part of its oversight responsibilities, the BMA conducts on-site reviews and detailed compliance testing of banks' anti-money laundering controls. In 2001, the BMA was not required to employ its formal enforcement powers to investigate suspicions of illegal deposit-taking. The BMA may require reports from auditors, accountants or other persons with relevant professional skills on matters pertinent to the authority's responsibilities. Banks and other financial institutions must retain records for a minimum of five years. Bankers and others are protected by law with respect to their cooperation with law enforcement officials. Bermuda has not adopted bank secrecy laws, but does have banker negligence laws. Bearer shares are not permitted in Bermuda.

Bermuda's Trusts (Regulation of Trust Business) Act 2001, effective January 1, 2002, invests the BMA with full licensing, supervision and enforcement powers relating to persons who conduct trust business in

Money Laundering and Financial Crimes

or from Bermuda. The BMA routinely conducts on-site review visits to determine, among other things, compliance with anti-money laundering laws and regulations. Regulatory oversight of Bermuda's insurance industry is undertaken by the BMA.

New legislation to give the BMA a full set of regulatory powers with respect to collective investment schemes is in the early stages of development. In the meantime, collective investment schemes are regulated pursuant to regulations under the Bermuda Monetary Authority Act. In December 2002, Parliament passed the Bermuda Monetary Authority Amendment Act 2002, expanding the authority of the BMA to detect and prevent financial crime. Provision is also made authorizing the BMA to collect fees directly from financial service providers, an indication of its independence from the GOB. In order to implement provisions of UN anti-terrorism Security Council Resolutions, the Act also provides for the manner in which the Minister of Finance may delegate powers to the BMA for blocking accounts.

Although Bermuda is considered an offshore financial center, all financial institutions in Bermuda are subject to the PCA, as amended, which, as noted above, includes know-your-customer requirement and provides for the monitoring of accounts for suspicious activity. The vetting process is undertaken when an entity is incorporated. The BMA requires that a personal declaration form be submitted for principals (beneficial owners) of international businesses prior to licensing. Similar requirements apply to proposals to transfer shares. Additionally, a company must detail its business plan and maintain a register of shareholders at its registered office.

Offshore banking is not permitted in Bermuda, nor are nominee (anonymous) directors allowed. However, the BMA reports that some overseas banks have established operations on the island to provide other forms of financial services, such as licensed trust operations. In such instances, the BMA liaises with the home regulatory body to enhance combined supervision. Neither casinos nor Internet gaming sites are allowed in Bermuda.

International business forms the basis of Bermuda's economy. The BMA licenses and regulates international business in the same manner as it does domestic companies. As of June 30, 2002, the Registrar of Companies recorded 13,020 international businesses registered in Bermuda, compared to 2,772 domestic companies. Of the international businesses, there were 11,806 exempt companies, 557 exempt partnerships, 638 non-resident international companies (incorporated elsewhere to do business in Bermuda), and 19 non-resident insurance companies. The BMA's Report and Accounts records the following breakdown for 2001: 1,641 insurance companies, 1,301 mutual fund companies, and 120 unit trust companies.

The majority of Bermuda's exempt companies are shell companies with no physical presence on the island. Local directors are designated (generally a local lawyer and secretary) who manage corporate affairs in Bermuda. The owners and controllers are vetted by the BMA before they can be established or any shares transferred between non-residents. The register of members is open to public inspection. The GOB regulates offshore companies and domestic companies equally from a prudential standpoint. The difference between the two is the ownership restriction. Domestic companies, which must be at least 60 percent Bermudian-owned, are permitted to do business within Bermuda. Exempted companies are exempt from the 60 percent ownership restriction and in fact can be up to 100 percent foreign-owned, but they are prohibited from doing business locally. The GOB agreed to remove some minor distinctions between the two categories as part of its advance commitment to the OECD.

The Financial Investigation Unit (FIU), within the Bermuda Police Service, serves as Bermuda's Financial Intelligence Unit; The FIU has been a member of the Egmont Group, an organization of Financial Intelligence Units, since 1999. The majority of suspicious transaction reports (STR) have related primarily to conversion of suspected local drug profits to U.S. dollars via the island's Western Union money transmission service, which closed as of October 31, 2002. Because Bermuda law requires money transmission services to be conducted in association with a licensed deposit-taker, conversion of funds is subject to bank reporting standards.

In 2001, there were 2,827 STRs filed with the Financial Investigation Unit of the Bermuda Police Service. The figures were similar in 2002, with 1,742 STRs logged in and another 800 still to be entered into the system. Bank fraud cases, including STRs, totaled 3,556 in 2001 and about 3,800 in 2002. In 2001, there were two arrests but no prosecutions for money laundering. In 2002, there were eight arrests representing three cases, of which two are ongoing investigations and the third is in the hands of the Director of Public Prosecutions.

The PCA, as amended, establishes procedures for identifying, tracing, and freezing the proceeds of drug trafficking and other indictable offenses, including money laundering, tax evasion, corruption, fraud, counterfeiting, stealing and forgery. Additionally, the PCA provides for forfeiture upon criminal conviction if it is proven that benefit was gained from a criminal act. Under the PCA, there is no provision for seizure of physical assets unless intercepted leaving the island. However, the Supreme Court may issue a confiscation order pursuant to which the convicted must satisfy a monetary obligation. The amount paid is placed into the Confiscated Assets Fund and may be shared with other jurisdictions at the direction of the Minister of Finance. If the convicted fails to satisfy the confiscation order, the onus is on the prosecution to apply to the court for appointment of a receiver. Under the Misuse of Drugs Act, physical assets can be seized if used at the time the offense was committed.

The GOB enforces the existing drug-related asset seizure/forfeiture laws. It is the responsibility of the police and the court system to trace/seize assets. Although Bermuda cooperates with the United States and other countries to trace/seize assets and uses tips from other countries, it does not—as an overseas territory—engage in negotiations with other governments to enter into treaty obligations with respect to asset tracing and seizure. This role rests with the United Kingdom. Banks are legally obligated to cooperate in the tracing/seizure of assets. The GOB issued no confiscation orders in 2000, one for approximately \$62,000 in 2001, and none in 2002, although several are being processed. Inexperience by the GOB is perhaps the major impediment in implementing asset forfeiture and seizure legislation.

Bermuda has not formally criminalized terrorist financing, but it is subject by extension to the UK Terrorism (United Nations Measures) (Overseas Territories) Order 2001. That order creates the offense of collecting and making funds available for terrorist purposes and provides for identification and freezing of terrorist-related funds. Nevertheless, Bermuda recognizes the need for domestic terrorism legislation and in 2003 is expected to propose amendments to expand the definition of “serious crimes” under the PCA to include terrorism-related offenses, consistent with FATF guidelines, as well as relevant changes to Bermuda’s criminal code. Meanwhile, the BMA has requested that financial institutions treat suspect terrorist financing as if covered by PCA and to report accordingly. Financial institutions have been given the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 (on terrorist financing) and the UN 1267 Sanctions Committee consolidated list, but no matches have been found.

Bermuda is subject to the US/UK Extradition Treaty. Bermuda is a member of the Caribbean Financial Action Task Force (CFATF), and through the UK, is also a party to the 1988 UN Drug Convention. Bermuda is also a party by extension from the UK to the UN International Convention for the Suppression of the Financing of Terrorism. Bermuda is also a member of the Offshore Group of Banking Supervisors.

Bermuda should modify its domestic legislation to ensure that it implements the FATF Special Eight Recommendations on Terrorist Financing and should consider enacting measures to detect/monitor cross-border transportation of cash. Bermuda should also consider devoting additional resources toward investigative efforts to combat money laundering to more thoroughly deter international criminals and follow through on its plans for additional training in areas such as asset forfeiture.

Bolivia. Most money laundering in Bolivia is related to public corruption, contraband smuggling, and narcotics-trafficking. Bolivia’s long tradition of banking secrecy facilitates the laundering of the profits of organized crime and drug trafficking, the evasion of taxes, and laundering of other illegally obtained earnings.

Money Laundering and Financial Crimes

The Government of Bolivia (GOB) has criminalized money laundering related to narcotics-trafficking, organized criminal activities, and public corruption. Law 1768 also created a financial investigations unit, the Unidad de Investigaciones Financieras (UIF), within the Office of the Superintendency of Banks and Financial Institutions. The UIF is responsible for implementing anti-money laundering controls. 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 transactions 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 new government, the UIF is now fully operational however, there is still weak political support within the government, and confusion over the UIF's legal role. Its primary responsibility is to analyze information and transactions, and detect irregularities in the banking system. The UIF is obligated to report all detected criminal activity to the Public Ministry, the office responsible for prosecuting money laundering. In 2002, a Financial Investigative Unit, Grupo de Investigaciones y Analisis Financiamiento (GIAF) within Bolivia's Special Counternarcotics Force (FELCN) was created to work in coordination with the UIF. Agreements have been established for the formal exchange of bank secrecy information between the two units.

New agreements have also served to strengthen Bolivia's anti-money laundering regime. On June 27, 2002, two new agreements were signed. The first was signed by the Public Ministry, the National Police, and the Ministry of Justice, and allows for the implementation of investigations under the Code of Criminal Procedures (CCP). This agreement commits all entities to the CCP principle that grants prosecutors a broader responsibility over investigations and the work of investigative police. The second agreement defines the correct procedures for handling money laundering cases. The Superintendency of Banks' UIF, the Public Ministry, the National Police and FELCN are parties to this agreement, which establishes mechanisms for exchange and coordination of information, including formal exchange of bank secrecy information.

In spite of advancements in combating money laundering, there are still many weaknesses in the GOB's anti-money laundering system. The controls on the Bolivian banking system to regulate money laundering activities are lacking, and there is little legal support for money laundering investigations carried out by law enforcement officials. In order to prosecute a money laundering case, the crime of money laundering must 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. In spite of this, it is encouraging to note that the first sentence for money laundering, related to public corruption, in August 2002, was handed out.

The GOB lacks significant legislation regarding terrorist financing. Although Bolivia is a party to the UN International Convention for the Suppression of the Financing of Terrorism and signed the OAS Inter-American Convention Against Terrorism, there are no domestic laws that criminalize the financing of terrorism or grant the GOB the authority to identify, seize, or freeze terrorist assets.

Traditional asset seizure continues to be employed by CN authorities, however the forfeiture continues to be 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 Criminal Code further permitted the government to sell certain kinds of property, with or without the consent of the accused, when the property might lose value if stored, cost too much to maintain, etc.

In 1998, the United States Government (USG) suspended its support of the Directorate of Seized Assets, which is responsible for confiscating, maintaining and disposing of the property of persons accused of violating Bolivia's narcotics laws. The two principal problems were first, the Directorate's inability to account for the property in its inventories, and second, its inability to work with the judicial branch. This resulted in judges routinely returning seized property to narcotics defendants before trial, refusing to

authorize the Directorate to conduct sales as permitted by the decree or, when they did, to retain the proceeds. The USG resumed support of the Directorate of Seized Assets in 2001 in an effort to revitalize and reform this important office, to date with limited success.

Bolivia is a party to the 1988 UN Drug Convention, and in December 2000, signed the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Bolivia is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Bolivia is a member of the South America Financial Action Task Force (GAFISUD) and underwent a mutual evaluation by GAFISUD in October 2002. Bolivia's UIF is also a member of the Egmont Group. The GOB and the United States in June of 1995 signed an extradition treaty, which entered into force in November of 1996.

The GOB must continue to strengthen its anti-money laundering regime by improving Bolivia's current money laundering legislation so that it conforms to FATF and GAFISUD standards. The GOB should adopt new laws making money laundering a separate offense without connection to other illicit activities, expanding the list of predicate offenses, criminalizing terrorist financing and expeditiously blocking terrorist assets. The authority of the UIF must also be expanded to cover reporting by non-banking financial institutions. The GOB should continue to strengthen the relationships and cooperation between all government entities involved in the fight against money laundering.

Bosnia and Herzegovina. Bosnia is not a regional financial center. Laundering the proceeds of criminal activity through financial institutions is widespread. However, narcotics proceeds tend to be diverted outside Bosnia. Bosnia has not criminalized money laundering, although it is an offense in the civil code.

Regulatory supervision of the banking sector is largely vested at the local rather than the federal level through two separate but roughly parallel banking agencies. In 2001, the international community established a working group that plans to centralize banking supervision within the Central Bank in 2003. Although legislation generally reflects the Basel Committee's "Core Principles for Effective Banking Supervision", including suspicious transaction reporting and due diligence requirements, in practice banking standards do not conform to international norms. Asset seizure and forfeiture statutes exist, but implementation is rare. Some safe harbor protection has now been afforded to banking officials in fulfilling anti-money laundering compliance requirements. However, Bosnia's laws remain an unwieldy combination of communist-era statutes and internationally imposed reforms. Enforcement is tenuous at best in this cash-based, largely unregulated economy, thereby creating widespread potential for financial crime and the financing of terrorism.

In addition, ambiguous lines of responsibility among investigative and regulatory agencies have aggravated already rampant political interference in investigations and direct intimidation of officials.

On October 21, 2002, at the initiative of the United Nations High Representative Paddy Ashdown, the existing banking laws were amended. The amendments prohibit terrorist financing and provide regulatory authorities with the ability to freeze assets of suspected terrorists.

Bosnia is a party to the 1988 UN Drug Convention, and on April, 24, 2002, Bosnia ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Bosnia has signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism.

Bosnia should implement existing laws and banking regulations. Furthermore, Bosnia should criminalize money laundering for all serious crimes, centralize regulatory and law enforcement authority, establish a Financial Intelligence Unit, and require suspicious transaction reporting.

Botswana. Botswana is a developing regional financial center, and therefore, is vulnerable to money laundering. Botswana has a relatively well-developed banking sector.

Section 14 of the Proceeds of Serious Crime Act of 1990 criminalizes money laundering related to all serious crimes. The Bank of Botswana requires financial institutions to report any transaction in which

Money Laundering and Financial Crimes

Pula 100,000 (\$17,800) or more is transferred. The Bank of Botswana has the discretion to provide information on large currency transactions to law enforcement agencies. In 2001, Botswana amended the Proceeds of Serious Crimes Act to require identification of financial bodies and owners of corporations and accounts.

In 2001, the Government of Botswana began drafting regulations that would require banks to file Suspicious Activity Reports (SARs) with the Bank of Botswana. While the Bank of Botswana has not yet implemented these regulations, banks have already begun filing SARs in anticipation of the regulations.

Botswana is in the early stages of developing an offshore financial center; and consequently, licenses offshore banks and businesses. Background checks are performed on applicants for offshore banking and business licenses, as well as on their directors and senior management. The bank supervisory standards applied to domestic banks are applicable to offshore banks as well. One offshore bank has been licensed in Botswana, but it was not operational as of December 2002. Bank and business directors are subject to the “fit and proper test” required by Section 29 of the Banking Act of 1995. Anonymous directors are not allowed. Offshore trusts are prohibited in Botswana. There are no known offshore international business companies, exempt companies, or shell companies operating in the Botswana offshore financial center.

Terrorist financing is not criminalized as a specific offense in Botswana. However, acts of terrorism and related offenses, such as aiding and abetting, can be prosecuted under the Penal Code and under the Arms and Ammunitions Act. The Bank of Botswana has circulated to financial institutions the names of suspected terrorist individuals and groups on the UN 1267/1390 consolidated list, as well as lists provided by the United States Government and the European Union.

In 2001, an International Law Enforcement Academy (ILEA) opened in Gaborone. The ILEA provides training in money laundering and other law enforcement areas to countries in the southern region of Africa.

Botswana is a party to both the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. Botswana is also a party to the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Botswana should criminalize terrorist financing and implement SAR regulations. Botswana should also establish a Financial Intelligence Unit (FIU) that would receive SARs and would be capable of sharing information with other FIUs and law enforcement agencies internationally. Botswana should also join the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) by signing ESAAMLG’s Memorandum of Understanding.

Brazil. Despite the important regulatory and investigative steps the Government of Brazil (GOB) has taken, the laundering of proceeds from narcotics-trafficking, illegal gambling, white-collar crime, corruption, trade in contraband, and other crimes remains a problem in Brazil. A highly developed financial sector and a problem with local drug consumption and trafficking have made Brazil a money laundering center.

The GOB has a comprehensive anti-money laundering regulatory regime in place. Law 9,613 of March 3, 1998, criminalizes money laundering related to drug trafficking and other offenses, 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 \$4,000) in cash, checks or traveler’s checks across the Brazilian border must fill out a customs declaration that is sent to the Central Bank. Financial institutions remitting more than 10,000 reais also must make a declaration to the Central Bank.

On June 11, 2002, President Cardoso signed Law 10,467, which modified Law 9,613. The new law put into effect Decree 3,678 of November 30, 2000, which penalizes 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.

The 1998 Anti-Money Laundering law also created a Financial Intelligence Unit, the Council for the Control of Financial Activities (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 28, comprised of 18 analysts, two international organizations specialists and support staff; they have also recently hired a counter-terrorism specialist.

In 1999, the COAF issued eight sets of regulations that addressed real estate, factoring companies, gaming and lotteries, dealers in jewelry and precious metals, bingo, credit cards, commodities trading, and dealers in art and antiques. The regulations require customer identification, record keeping, and reporting of suspicious transactions directly to the COAF. In 2000, the COAF issued Regulation No. 9, slightly amending the bingo, lotteries, and gaming regulations. In November 2001, the COAF issued Regulation No. 10, which imposes additional requirements for money remittance businesses.

In 1999, the GOB's other regulatory bodies, the Central Bank, the Securities Commission (CVM), the Private Insurance Superintendency (SUSEP), and the Office of Supplemental Pension Plans (PC), issued parallel regulations to covered institutions that spell out requirements for customer identification and reporting of suspicious transactions. All of these regulations include a list of guidelines that help institutions identify suspicious transactions. In January 2002, SUSEP introduced Circular No. 181, which specified the insurance entities required to comply with Law No. 9,613 and required these entities to report to SUSEP any cash transactions equal to or higher than 30,000 reals (now approximately \$12,000).

The Central Bank has established the Departamento de Combate a Ilícitos Cambiais e Financeiros; Department to Combat Exchange and Financial Crimes (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. Until January 2001, bank secrecy protected the name of the bank and the account number, and transaction details. While the Central Bank had access to the information, other government agencies—except for congressional investigative committees—required a court order to access detailed bank account information. The GOB addressed this problem by enacting Complementary Law No. 105 and its implementing Decree No. 3,724 in January 2001. These allow for complete bank transaction information to be provided to government authorities, including the COAF, without a court order. On January 11, 2002, President Cardoso signed Brazil's new omnibus drug legislation, which allows for the suspension of bank secrecy during drug trafficking investigations. The president vetoed Chapter III of this law, which would have reduced the penalty for money laundering from the previous legislation's three to ten years, to one to two years, plus fines.

In 2002 COAF received 89 foreign requests for information on money laundering investigations, as well as 257 domestic requests from law enforcement, the Public Ministry, government agencies and the judiciary branch. Since 1998 the COAF has identified 321 cases that show evidence of money laundering. Subsequent investigations have led to the indictments of 149 persons.

Brazil has only a limited ability to employ advanced law enforcement techniques such as undercover operations, controlled delivery, 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. Indeed, there has only been one known money laundering conviction since 1998. This occurred in 2002 as a result of the investigation of Judge Nicolau dos Santos Neto, who was arrested in December 2000 for embezzling 169 million reals (then approximately \$85 million dollars in funds earmarked for construction of a city courthouse. Nicolau allegedly used a system of front companies in offshore havens to transfer money and buy property abroad, including the United States. In June 2002, Judge Nicolau, who was charged with embezzlement, corruption, tax evasion and money laundering, was sentenced to eight years in prison. Some of the embezzled funds have been traced to banks in Paraguay and Panama.

Money Laundering and Financial Crimes

Money laundering in Brazil is primarily related to drugs, corruption and trade in contraband. In 2002 COAF also began investigating instances of money laundering linked to the sale and purchase of luxury automobiles. This market is currently an unregulated sector in Brazil. Other schemes involve the purchase of winning lottery tickets to justify the increase of funds. Under Brazil's anti-money laundering law, 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.

Since September 11, 2001, the COAF has responded to U.S. Government efforts to identify and block terrorist-related funds. As a member of the South American Financial Action Task Force (GAFISUD) and the Financial Action Task Force (FATF), Brazil has sought to comply with the Eight Special Recommendations on Terrorist Financing. The GOB has signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism and the OAS Inter-American Convention on Terrorism.

Since September 11, 2001, COAF ran inquiries on over 700 individuals and entities, including searching its financial records for entities and individuals on the UN 1267 Sanctions Committee's consolidated list. None of the individuals and entities on the consolidated list, however, were found to be operating or executing financial transactions in Brazil.

According to Mr. Alberto Mendes Cardoso, Brazil's delegate to the OAS Inter-American Committee Against Terrorism (CICTE), "There is an undeniable link between certain forms of organized crime and terrorism. In a speech during the opening debate of the 56th United Nations General Assembly, in November 2001, President Fernando Henrique Cardoso stressed that 'throughout the world, problems of public safety, drug trafficking and consumption, and arms smuggling are evils associated with terrorism, which we must stamp out.' Thus, drug consumption, a scourge that affects all our countries, can contribute to the flourishing of terrorism, through the laundering of the funds used to purchase drugs." This is of concern because of the frequency of money laundering around the region of Foz de Iguacu, near the tri-border area with Paraguay and Argentina. This is an area with high occurrences of intellectual property violations and illicit commerce, and it is believed to be a haven for smuggling and arms trafficking. And again according to Brazil's representative to CICTE, "Brazil is ready to investigate any report that reaches us about the presence of terrorists or their activities not only along the Triple Frontier but also at any other point within Brazil." However, in spite of the problems in the tri-border area, and the recent conviction of a terrorist financier for income tax evasion in the region, the GOB insists there is no evidence of terrorist financing in the area.

Brazil has no legislation that criminalizes the financing of terrorism. There is legislation pending in the Brazilian Congress that would update Brazil's 1983 law penalizing acts of terrorism. The Brazilian congress is also considering draft legislation that would make terrorism a predicate offense under the money laundering law. Even in the absence of such provisions, Brazilian authorities maintain that the money laundering law and presidential decrees implementing UN Security Council resolutions give the government the authority to search for and if necessary block terrorist financial assets, but these internal security provisions have never been used in this context, nor have they been tested this way in court. In any event there is no domestic legislation that specifies which government agency has the responsibility to monitor the compliance of these resolutions and decrees.

The COAF is a member of the Egmont Group. In June 2000, Brazil became a full member of FATF. In 2000 Brazil also became a founding member of GAFISUD. 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. In February 2001, the Mutual Legal Assistance Treaty between Brazil and the United States entered into force. Brazil is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime, which is not yet in force internationally. The GOB has bilateral information exchange agreements with Belgium, France, Paraguay, Portugal, and Spain, as well as memoranda of understanding with the financial intelligence units of Belgium, Bolivia, Colombia,

Spain, France, Guatemala, Panama, Paraguay, Portugal, and Russia. FinCEN and COAF cooperate with one another on a case-by-case basis.

In order to successfully combat money laundering and other financial crimes, Brazil should develop legislation to regulate the sectors in which money laundering is an emerging issue. Brazil should also adopt new laws that, in compliance with international standards, criminalize the financing of terrorism and define terrorism as a predicate crime for money laundering. Brazil should also consider 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. In addition, the GOB and the 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 an U.K. Caribbean overseas territory of the United Kingdom (UK). The BVI is vulnerable to money laundering due to its financial services industry. Tourism and financial services account for approximately 50 percent of the economy. The offshore sector offers incorporation and management of offshore companies, and provision of offshore financial and corporate services. The BVI has 13 banks (four of which are commercial), and approximately 1800 mutual funds, 140 captive insurance companies, 1000 registered vessels, 90 licensed general trust companies, and approximately 360,000 active international business companies (IBCs). The BVI underwent an evaluation of its financial regulations in 2000, co-sponsored by the local and British governments.

According to the International Business Companies Act of 1984, BVI-registered IBCs 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. BVI has approximately 90 registered agents that are licensed by the Financial Services Commission (FSC), which was established December 7, 2001. Registered agents must verify the identities of their clients. The process for registering banks, trust companies, and insurers is governed by legislation that requires more detailed documentation, such as a business plan and vetting by the appropriate supervisor within the FSC. The law transfers responsibility for regulatory oversight of the financial services sector from a government body, the Financial Services Department, to an autonomous regulatory body, the FSC.

In 2000, the Information Assistance (Financial Services) Act (IAFSA) was enacted to increase the scope of cooperation between BVI's regulators and regulators from other countries. On December 29, 2000, the Anti-Money Laundering Code of Practice (AMLCP) of 1999 entered into force. The AMLCP established procedures to identify and report 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 Proceeds of Criminal Conduct Act of 1997 expanded predicate offenses for money laundering to all criminal conduct, and allows the BVI Court to grant confiscation orders against those convicted of an offense and who have benefited from criminal conduct. The law also created a Financial Intelligence Unit (FIU) referred to as the Reporting Authority-Financial Services Inspectorate. The Reporting Authority-Financial Services Inspectorate is an administrative Financial Intelligence Unit (FIU) responsible for the collection of suspicious activity reports. The Reporting Authority reviews approximately 30 suspicious transaction reports annually. Reports requiring investigation are given to the Police Financial Investigations Units. Only one money laundering case has been prosecuted in the BVI.

The BVI has proposed the Code of Conduct (Service Providers) Act (CCSPA) that would encourage professionalism, enhance measures to deter criminal activity, promote ethical conduct, and encourage greater self-regulation in the financial sector. The CCSPA also would establish the Council of Service Providers, a body that would regulate the conduct of individuals within the financial services industry. Additionally, the CCSPA would formulate policy, procedures, and other measures to regulate the industry, advise the government on legislation and policy matters, and monitor compliance within the industry.

Money Laundering and Financial Crimes

The Joint Anti-Money Laundering Coordinating Committee (JAMLCC) was established in 1999 to coordinate all anti-money laundering initiatives in the 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.

The BVI is a member of the Caribbean Financial Action Task Force, and is subject to the 1988 UN Drug Convention. Application of the U.S./U.K. Mutual Legal Assistance Treaty concerning the Cayman Islands was extended to the BVI in 1990. The Reporting Authority-Financial Services Inspectorate is a member of the Egmont Group.

The BVI should criminalize the financing of terrorists and terrorism and take measures necessary to implement the FATF Special Eight Recommendations on Terrorist Financing. The BVI should continue to strengthen its anti-money laundering regime by implementing legislation that would regulate the conduct of individuals within the financial sector.

Brunei. The Government of Brunei adopted anti-money laundering legislation, the Money Laundering Order, in 2000. Also in 2000, Brunei implemented an asset seizure and forfeiture law, the Criminal Conduct (Recovery of Proceeds) Order. This legislation applies both domestically and to the offshore sector. In 2002, Brunei enacted the Drug Trafficking Recovery of Proceeds Act and the Anti-Terrorism Financial and other Measures Orders.

In 2001, Brunei actuated its plans to become an offshore financial center. The Brunei Darussalam brought into effect a series of laws that established the Brunei International Financial Center (BIFC). The relevant laws are: the International Business Companies Order 2000; the International Banking Order 2000; the Registered Agents and Trustees Licensing Order 2000; the International Trusts Order 2000; the International Limited Partnerships Order 2000; the Mutual Fund Order 2000, the Securities Order 2000 and the International Insurance and Takaful Order 2000. The BIFC launched a virtual Stock Exchange in 2002. The BIFC offers banking, Islamic banking, insurance, international business companies (IBCs), trusts (including asset protection trusts) mutual funds, and securities services. Bearer shares are not permitted, but nominee shareholders are allowed for IBCs. Brunei residents are allowed to become shareholders of IBCs. At present 370 companies are on the Brunei International Financial Center database. The Government also recently established the Brunei Economic Development Board (BEDB) to attract more foreign direct investment. There are no exchange controls.

Brunei has no Central Bank. The Authority, a segregated unit of the Ministry of Finance, acting through the Financial Institutions Division and the Head of Supervision, oversees the BIFC. This unit combines both regulatory and marketing responsibilities. The Authority is a multi-disciplinary unit with individuals with banking, insurance, corporate and trust supervisory skills.

Brunei is a party to the 1988 UN Drug Convention and, in December 2002, acceded to the UN International Convention for the Suppression of the Financing of Terrorism. On November 5, 2001, Brunei signed the Association of Southeast Asian Nations (ASEAN) Declaration on Joint Action to Counter Terrorism, and on November 3, 2002 Brunei joined the other ASEAN countries in adopting a Declaration on Terrorism by the 8th ASEAN Summit. On August 1, 2002, Brunei, on behalf of the other ASEAN countries, signed the non-binding ASEAN-United States of America Joint Declaration for Cooperation to Combat International Terrorism. Brunei is an observer jurisdiction to the Asia/Pacific Group on Money Laundering (APG). Brunei is applying to join the APG in 2003 and has undertaken compliance with the APG's Terms of Reference, which include a commitment to adopt the international standards contained in the Financial Action Task Force Forty Recommendations on Money Laundering and to the procedures for the evaluation of the effectiveness of its anti-money laundering systems.

Brunei should continue to enhance its anti-money laundering regime by separating the regulatory and marketing functions of the Authority to avoid potential conflict of interest. Additionally, Brunei should adequately regulate its offshore sector to reduce its vulnerability to misuse by terrorist organizations and their supporters. For all IBCs, Brunei should provide for identification of all beneficial owners. If its Anti-

Terrorism Financial and other Measures Orders does not explicitly do so, Brunei should also criminalize the financing and support of terrorism.

Bulgaria. Bulgaria is not considered an important regional financial center. Bulgaria's financial system is vulnerable to money laundering related to narcotics-trafficking and financial crimes such as bank and corporate fraud, embezzlement, tax evasion, and tax fraud. The proceeds of smuggling, vehicle theft, alien smuggling, prostitution, and extortion also are laundered in Bulgaria. The sources and destinations for much of the illicit funds include Eastern Europe, the former Soviet Union, Turkey, and the Middle East. The presence of organized criminal groups and official corruption contribute to Bulgaria's money laundering problem. Combating corruption and organized crime have been policy priorities for the government.

Bulgarian anti-crime legislation includes a 1998 money laundering law criminalizing money laundering. The legislation takes an "all-crimes" approach, as opposed to a list approach, meaning that any crime may serve as a predicate crime for money laundering. Other provisions include customer identification and record keeping requirements, suspicious transactions reporting (STR), and internal rules for financial institutions on implementation of an anti-money laundering program. Banks, securities brokers, auditors, accountants, insurance companies, investment companies, and other businesses are subject to these reporting requirements. Penalties for these crimes are not addressed in this legislation, but fall within the penal code. All penalties for every crime fall within the penal code rather than the criminalizing legislation itself. Money laundering was criminalized within the Penal Code in 1997 via Articles 253 and 253(a). In 2001, the code was amended to add a 30-year prison penalty if the money laundering is linked with narcotics-trafficking.

During the fall of 2002, Parliament passed, through three committees, two readings of draft legislation further strengthening anti-money laundering measures. The legislation extends the types of obligated institutions and groups to include lawyers, and will introduce a currency transaction reporting requirement of 30,000 leva, (\$15,000), thus bringing Bulgaria into line with the EU standard. However, this requirement will not become effective until 2004, because Bulgaria's Bureau of Financial Intelligence (BFI) is currently not technologically capable of processing these reports. The legislation also changes the name of the BFI, Bulgaria's Financial Intelligence Unit, into the Financial Intelligence Agency (FIA), commensurate with BFI's status as a full agency within the Ministry of Finance rather than a bureau. It further institutionalizes and guarantees functional independence of the unit's director. The legislation (with the single named exception) will enter into force at the beginning of 2003.

Since its establishment in 1998, the BFI has received over 1,200 suspicious transaction reports. The various obligated institutions submitted over 95 percent of them. Eighty percent of cases are closed. By the end of October 2002, BFI's 37 staff members forwarded 191 cases to the Supreme Prosecutor's Office and the Ministry of Interior. In effect, the first ten months of 2002 saw twice as many cases reported to the Prosecutor's Office—a total of \$180 million—as in previous years. However, some of these cases represent the backlog of previous years. Notwithstanding the increase in activity, BFI remains handicapped technologically, but is working on improving its database and its management to make it more efficient for the analysts' use by being able to track across targets and years.

The National Investigative Service is the only agency authorized to investigate money laundering, and it does so at the behest of the Prosecutor's Office. However, BFI has the authority to close cases, and to pursue cases via appeal that have been closed by the Prosecutor's Office. Although money laundering has been pursued in court cases, there has never been a conviction for the crime. Prosecutors and investigators do not train for or specialize in money laundering, especially at the district level, so there may well be some confusion on their part with regard to pursuing money laundering cases.

The Government of Bulgaria (GOB) is still considering legislation addressing actual forfeiture and seizure of criminal assets, indictment of entities on money laundering charges, and prohibiting the use of funds of dubious or criminal origin in acquiring banks and businesses during privatization.

Money Laundering and Financial Crimes

The GOB recently enacted the Measures against the Financing of Terrorism, that criminalizes the financing of terrorism and links financial intelligence with other anti-terrorist measures in place. The law therefore legislates a link between BFI and the STRs it receives, and terrorism financing, and authorizes the agency to use its financial intelligence to that end as well as in fighting money laundering. In April 2002, Bulgaria became a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Bulgaria is a member of the Council of Europe (COE) and participates in the COE's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, PC-R-EV). The BFI is a member of the Egmont Group and participates actively in information sharing with foreign counterparts. In June 2001, Bulgaria was judged by the Technical Consultation Group of the European Commission to be in full compliance with Chapter 4 of the pre-accession negotiations with respect to preventive legislation in the area of counteraction of money laundering.

Bulgaria is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Bulgaria has signed and ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Currently, the BFI has bilateral memoranda of understanding regarding information exchange relating to money laundering with Belgium, the Czech Republic, Latvia, the Russian Federation, and Slovenia.

The GOB should approve and implement proposed measures that will address forfeiture and seizure of criminal assets, the indictment of entities on money laundering charges, as well as prohibiting the use of dubious or criminal-origin funds to acquire banks and businesses during privatization. BFI should continue to increase its staff to full capacity and work on its technological improvements for the analysts. The BFI should also continue to work with the police, Prosecutor's Office, National Investigative Service, and Appeals Office to improve the prosecutorial effectiveness in money laundering cases.

Burkina Faso. Burkina Faso is not a regional financial center. Although the economy is primarily cash-based, there are seven banks in Burkina Faso. Only an estimated six percent of the population have bank accounts.

Burkina Faso lacks laws and regulations specifically designed to fight money laundering or financial crimes. Neither money laundering nor terrorist financing is a criminal offense.

The Central Bank of West African States (BCEAO), based in Dakar, Senegal, is the central bank for the countries in the West African Economic and Monetary Union (WAEMU): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal, and Togo, all of which use the French-backed CFA franc currency. All bank deposits over approximately \$7,700 made in BCEAO member countries must be reported to the BCEAO, along with customer identification information.

In September 2002, the WAEMU Council of Ministers, which oversees the BCEAO, approved an anti-money laundering regulation applicable to banks and other financial institutions, casinos, travel agencies, art dealers, gem dealers, accountants, attorneys, and real estate agents. The regulation is subject to review by member countries, which would be responsible for implementing many provisions of the regulation. The regulation is expected to go into effect in early 2003.

Under the WAEMU regulation, financial institutions would be required to verify and record the identity of their customers before establishing any business relationship. The regulation would require financial institutions to maintain customer identification and transaction records for ten years. The regulation would also impose certain customer identification and record maintenance requirements on casinos.

All financial institutions, businesses, and professionals under the scope of the WAEMU regulation would be required to report suspicious transactions. The regulation calls for each member country to establish a National Office for Financial Information Process (CENTIF), which would be responsible for collecting suspicious transactions and would have the authority to share information with other CENTIFs within the WAEMU as well as with the financial intelligence units of non-WAEMU countries.

The WAEMU Council of Ministers issued another directive in September 2002 requesting member countries to pass legislation requiring banks to freeze the accounts of any persons or organizations targeted by the UNSCR 1267/1390 consolidated lists.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA), based in Dakar, Senegal. In November 2002 GIABA hosted an anti-money laundering seminar for representatives of 14 ECOWAS members, including Burkina Faso. In July 2002 Togo participated in the 2002 West African Joint Operation Conference (WAJO) that promotes regional law enforcement cooperation against narcotics-trafficking, terrorism, and money laundering.

On May 15, 2002, Burkina Faso ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Burkina Faso is a party to the 1988 UN Drug Convention.

Burkina Faso should criminalize money laundering and terrorist financing as part of a viable anti-money laundering regime.

Burma. Renamed the Union of Myanmar by the ruling junta, Burma has a mixed economy with private activity dominant in agriculture, light industry, and transport, and with substantial state-controlled activity, mainly in energy, heavy industry, and the rice trade. Burma's economy continues to be vulnerable to drug money laundering due to its under-regulated financial system, weak anti-money laundering regime, and policies that facilitate the funneling of drug money into commercial enterprises and infrastructure investment.

In June 2001, the Financial Action Task Force (FATF) identified Burma as non-cooperative in international efforts to fight money laundering (NCCT). This designation was based on Burma's lack of basic anti-money laundering provisions. Money laundering had not been criminalized for crimes other than narcotics-trafficking, and there were no record keeping or reporting requirements. Additionally, oversight of the banking sector was weak, and there were obstacles to international cooperation. Subsequent to the FATF's naming of Burma as NCCT, the U.S. Treasury Department issued an advisory to U.S. financial institutions, warning them to give enhanced scrutiny to all financial transactions relating to Burma. Both actions remain in force.

The Control of Money Laundering Law (The State Peace and Development Council Law No. 6/2002) was passed on June 17, 2002. There are ten predicate offenses listed in Chapter III of this legislation. The Psychotropics Substances Law of 1993 only criminalized narcotics money laundering. The 2002 legislation goes beyond narcotics money laundering and includes human and arms trafficking, smuggling, cybercrime, illegally operating a financial institution, hijacking, and "offenses committed by acts of terrorism" as predicate offenses. The legislation does require suspicious transaction reporting, but does not include a specific timetable for required submission of suspicious transaction reports (STRs), beyond "without delay." Chapter VIII requires financial institutions to maintain records for at least five years. Money laundering is punishable by imprisonment.

Chapter IV allows for the formation of the Central Control Board on Money Laundering, the Burmese Financial Intelligence Unit (FIU), which may conduct an investigation into a money laundering case based on a STR, and which is responsible for establishing the reporting thresholds. The Central Control Board, chaired by the Home Minister, will enforce the legislation. The Board will set policy, direct the Investigation Body (that performs money laundering investigations and conducts seizures), direct the Preliminary Scrutiny Body (that ensures due process and finalizes the case), cooperate with other international money laundering groups, and organize investigation teams. The legislation provides full access to all financial records for investigators from the FIU. The first investigations under this law began in July, resulting in the seizure of several hundred thousand dollars in assets. The first prosecutions should take place within the next several months.

Burma is an observer jurisdiction to the Asia/Pacific Group on Money Laundering and a party to the 1988 UN Drug Convention. Over the past several years, the Government of Burma (GOB) has

significantly extended its counternarcotics cooperation with other states. The GOB has bilateral drug control agreements with India, Bangladesh, Vietnam, Russia, Laos, the Philippines, China and Thailand. It is not known whether these agreements cover cooperation on money laundering issues. In 2001-2002, Burma joined with China in joint operations in northern and eastern Shan State that resulted in the destruction of several major drug-trafficking rings. Burma has signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism. Burma has not signed or ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Currently, Burma does not provide significant mutual legal assistance or cooperation to overseas jurisdictions in the investigation and prosecution of serious crimes. The GOB is planning to couple the anti-money laundering legislation with proposed mutual assistance legislation to facilitate judicial cooperation between Burma and other states.

Burma must increase the regulation and oversight of its banking system, and end policies that facilitate the investment of drug money in the legitimate economy. Burma should set the reporting thresholds required under its new anti-money laundering legislation and create the institutions and the environment conducive to establishing a viable anti-money laundering regime. The GOB should also criminalize the financing and support of terrorism. Burma should provide the necessary resources to the administrative and judicial authorities that supervise the financial sector and enforce the financial regulations to successfully fight money laundering.

Cambodia. Cambodia is not an important regional financial center. It is vulnerable to money laundering. Cambodia is a transit country for heroin-trafficking from the Golden Triangle. It has a cash-based economy (heavily dollarized), little control over its borders, and has widespread corruption. Cambodia has a significant black market for smuggled goods and commodities, but there is no indication the market is funded by narcotics proceeds. The black market exists due to high taxes and tariffs and the corresponding massive profits to be made by skirting official duties.

Cambodia's banking sector is small, with 13 general commercial banks and four specialized commercial banks. The National Bank of Cambodia (NBC) maintains strict control over the banking sector and, with a relatively small number of deposits in the system, feels it exercises good oversight over transactions. Casinos dot Cambodia's border with Thailand, most notably at Poipet. The NBC has no authority over these casinos and no knowledge of their financial holdings or transactions. The lack of oversight represents a significant money laundering vulnerability.

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 and includes setting a threshold for reporting currency transactions valued at \$10,000 or above and requires the maintenance of records for a ten-year period. The NBC regularly audits individual banks to ensure compliance with laws and regulations. The 1996 and 1999 laws include provisions for customer identification, suspicious transaction reporting, and the creation of the Anti-Money Laundering Commission (AMLC) under the Prime Minister's Office. The composition and functions of the AMLC have not been fully promulgated. In addition to the NBC, the Ministries of Economy and Finance, Interior and Justice also are involved in anti-money laundering matters.

Cambodia does not have any laws that specifically address terrorism financing. It does circulate to financial institutions the list of individuals and organizations designated by UN 1267 Sanctions Committee. To date, there have been no known reports of terrorist financing 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. Cambodia has signed, but has not become a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

Reportedly the Cambodian government plans to incorporate any new draft laws related to terrorism financing and money laundering into its financial roadmap as developed in cooperation with the Asian Development Bank. In the interim, the Royal Government of Cambodia should fully implement its existing anti-money laundering legislation and regulations and work towards new legislation that fully complies with world standards governing money laundering and terrorist financing.

Cameroon. Cameroon is not a regional financial center. Funds generated from the transit of illicit drugs through Cameroon, and the absence of any anti-money laundering legislation, make Cameroon vulnerable to money laundering. The Bank of Central African States (BEAC) supervises Cameroon's banking system. BEAC is a regional central bank that serves six countries of Central Africa.

On November 20, 2002, the BEAC Board of Directors approved draft anti-money laundering and counter-terrorist financing regulations that would apply to banks, exchange houses, stock brokerages, casinos, insurance companies, and intermediaries such as lawyers and accountants in all six member countries. The BEAC intends to submit the draft regulations to the Ministerial Committee of the Central African Economic and Monetary Community (CEMAC) for approval in January 2003.

If approved, the BEAC regulations would treat money laundering and terrorist financing as criminal offenses. The regulations would also require banks to record and report the identity of customers engaging in large transactions. The threshold for reporting large transactions would be set at a later date by the CEMAC Ministerial Committee at levels appropriate to each country's economic situation. Financial institutions would have to maintain records of large transactions for five years.

The regulations would require financial institutions to report suspicious transactions. Under the regulations, each country would establish a National Agency for Financial Investigation (NAFI), which would be responsible for collecting suspicious transaction reports. Bankers and other individuals responsible for submitting suspicious transaction reports would be protected by law with respect to their cooperation with law enforcement entities. If a NAFI investigation were to confirm suspicions of terrorist financing, the Cameroonian government could freeze and seize the related assets. The NAFI could cooperate with counterpart agencies in other countries, although this cooperation would be limited by privacy legislation.

Cameroon is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Cameroon should work with the BEAC to establish a viable anti-money laundering and counter-terrorist financing regime. Cameroon should also criminalize terrorist financing and money laundering.

Canada. Canada remains vulnerable to money laundering and terrorist financing because of its advanced financial services sector and heavy cross-border flow of currency and monetary instruments. The United States and Canada comprise the world's largest trade partnership and share a border that sees over \$1 billion dollars in trade a day. Both the U.S. and Canadian governments are particularly concerned about the criminal abuse of cross-border movements of currency. Canada's financial institutions are vulnerable to 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.

In 2000, the Government of Canada (GOC) passed the Proceeds of Crime (Money Laundering) Act to assist in the detection and deterrence of money laundering and facilitate the investigation and prosecution of money laundering offenses and to expand the list of predicate money laundering to cover serious crimes. The Act created a mandatory reporting system for suspicious financial transactions and cross-border movements of currency or monetary instruments. The Act also provided for the creation of a Financial Intelligence Unit (FIU), the Financial Transaction and Reports Analysis Centre of Canada (FINTRAC), which reports to the Minister of Finance and receives and analyzes reports from financial institutions and other financial intermediaries.

With the passage of the Anti-Terrorism Act in December 2001, the Proceeds of Crime (Money Laundering) Act, which was re-named as the Proceeds of Crime (Money Laundering) and Terrorist

Money Laundering and Financial Crimes

Financing Act, was amended to criminalize terrorist financing and require the reporting of suspicious transactions related to terrorist financing. Under the law, FINTRAC's mandate was expanded to include anti-terrorist financing and to allow disclosure of information to the Canadian Security Intelligence Service related to financial transactions that would be relevant to threats to the security of Canada. The Anti-Terrorism Act also enables Canadian authorities to deter, disable, identify, prosecute, convict and punish terrorist groups. No prosecutions took place in 2002. (Note: One financial institution reported that as of December, some \$200,000 were frozen in 29 separate accounts pending further investigation.)

In November 2001, FINTRAC became operational and regulations came into effect that require reporting entities to report all suspicious transactions when there are reasonable grounds to suspect that the transaction is related to the commission of a money laundering offense. In addition to banks and other financial institutions, money service businesses, casinos, lawyers, accountants, and real estate agents handling third-party transactions are required to file suspicious transaction reports (STRs). FINTRAC receives and analyzes the STRs and determines which suspicious transactions merit further investigation. A second set of regulations related to internal compliance regimes, the reporting of large cash transactions and large international electronic funds transfers, record keeping and client identification were published in May 2002 with certain requirements coming into effect in June 2002 and other requirements being phased in early 2003. A further set of regulations concerning the reporting of cross-border movements of currency and monetary instruments will come into effect in January 2003.

In June 2002, FINTRAC became a member of the Egmont Group. FINTRAC has the authority to negotiate information exchange agreements with foreign counterparts, and has completed discussions with several countries and is pursuing discussions with other countries, including the United States. However, Canada's privacy protection provisions can inhibit the timely and effective exchange of information on suspected criminals, including possible terrorists.

Canada is a member of the FATF and the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Canada also participates with the Caribbean Financial Action Task Force (CFATF) as a Cooperating and Supporting Nation, and as an observer jurisdiction to the Asia/Pacific Group on Money Laundering (APG).

Canada is a party to the OAS Inter-American Convention on Mutual Assistance in Criminal Matters. Canada has long-standing agreements with the United States on law enforcement cooperation including treaties on extradition and mutual legal assistance. Canada is a party to the 1988 UN Drug Convention, and in May 2002, ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Canada is a party to the UN International Convention for the Suppression of the Financing of Terrorism. It has signed all 12 UN terrorism conventions and protocols and has searched financial records for groups and individuals on the UNSCR 1267/1390 consolidated list.

Canada should continue to staff and develop FINTRAC and accelerate its efforts to sign MOUs that will allow for meaningful information exchange. The government of Canada should also continue its efforts to ensure that privacy protection does not inhibit the timely sharing of financial information that may be critical to international terrorist financing or major money laundering investigations.

Cayman Islands. The Cayman Islands, a United Kingdom (UK) Caribbean overseas territory, has made significant strides in its counter-money laundering program, though it is still vulnerable to money laundering due to its significant offshore sector. With a population of approximately 40,000, the Cayman Islands is home to a well-developed offshore financial center that provides a wide range of services such as private banking, brokerage services, mutual funds, and various types of trusts, as well as company formation and company management. Cayman Islands authorities report that approximately 580 banks and trust companies, 3,178 mutual funds, and 517 captive insurance companies are licensed in the Cayman Islands. In addition, approximately 45,000 offshore companies are registered in the Cayman Islands, including many formed by the Enron Corporation.

In June 2000, the Financial Action Task Force (FATF) placed the Cayman on the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering. The FATF in its report cited several concerns, including (1) lack of customer identification and record keeping requirements, (2) lack of access to customer identity records by supervisory authorities, (3) lack of mandatory reporting of suspicious transactions, and (4) lack of supervision of a large class of management companies.

In July 2000, the U.S. Treasury Department issued an advisory to U.S. financial institutions warning them to pay special attention and to give enhanced scrutiny for certain transactions or banking relationships involving the Cayman Islands.

Following the FATF designation and the U.S. Treasury Advisory, the Cayman Islands enacted and implemented comprehensive anti-money laundering laws and regulations to address the major identified deficiencies. Money laundering regulations that entered into force in September 2000 specify record keeping and customer identification requirements for financial institutions and certain financial services providers; the regulations specifically cover individuals who establish a new business relationship, engage in a one-time transaction over Cayman Islands (CI) \$15,000 (approximately \$ 18,000), or who may be engaging in money laundering. Amendments to the Proceeds of Criminal Conduct Law (PCCL) make failure to report a suspicious transaction a criminal offense that could result in fines or imprisonment. A provision of the Banks and Trust Companies Law (2001 Revisions) grants the Cayman Islands Monetary Authority (CIMA) the power to request “any information” from “any person” when there are “reasonable grounds to believe” that that person is carrying on a banking or trust business in contravention of the licensing provisions of the law, and grants CIMA access to audited account information from licensees who are incorporated under the Companies Law (2001 Second Revision).

The Monetary Authority Law (2001 Revision), was enacted in December 2002. It grants CIMA independence with respect to the licensing and enforcement powers over financial institutions. Previously these were vested directly in the government. The law grants CIMA, consistent with its regulatory authority, the power to obtain information “as it may reasonably require” from a person covered by the PCCL and its money laundering regulations of the Cayman Islands, a connected person, or a person reasonably believed to have information relevant to an inquiry by CIMA. The 2001 revisions to the Monetary Authority Law, unlike prior versions of the law, contain no requirement that CIMA obtain a court order before accessing account ownership and identification information. Amendments to the Companies Management Law (2001 Revision) expand regulatory supervision and licensing to management companies that were previously exempted, while the Companies Law (2001 Second Revision) institutes a custodial system in order to immobilize bearer shares.

A 2001 amendment to the PCCL revises the legal definition of Financial Intelligence Unit to adopt the Egmont Group definition, thereby paving the way for the Cayman Islands Financial Reporting Unit to become a member of the Egmont Group of Financial Intelligence Units in June 2001 and facilitating information exchange with its international counterparts. The Office of the Attorney General has also established an international division to respond to international requests for judicial cooperation.

Since the FATF issued its June 2000 report, the Cayman Islands has also passed and/or amended various other laws, including the Money Services Law (2000), Building Societies Law (2001 Revision), Cooperative Societies Law (2001 Revision), Insurance Law (2001 Revision), and the Mutual Funds Law (2001 Revision). The FATF recognized in June 2001 that the Cayman Islands had remedied the serious deficiencies in its anti-money laundering regime, and decided to remove the Cayman Islands from the NCCT list. Similarly, the U.S. Treasury Department withdrew its Advisory against the Cayman Islands in June 2001.

The Cayman Islands has been cooperative with criminal law enforcement authorities in the United States. The Cayman Islands is subject to the 1988 UN Drug Convention and the Treaty concerning the Cayman Islands relating to Mutual Legal Assistance in Criminal Matters. Also, it is a member of the Caribbean Financial Action Task Force (CFATF) and the Offshore Group of Banking Supervisors.

Money Laundering and Financial Crimes

The Cayman Islands has made significant progress toward addressing the serious systemic problems that characterized its counter-money laundering regime less than two years ago. The government should continue with its anti-money laundering implementation plans and international cooperation.

Chad. Chad is not an important financial center. Chad has a large informal sector that could be used to launder the proceeds of crime. The Bank of Central African States (BEAC), which supervises Chad's banking system, is a regional Central Bank that serves six countries of the Central African Economic and Monetary Community (CEMAC). The Chadian Central Bank is under the direction of the BEAC.

Money laundering is a criminal offense, and Chadian law holds individual bankers liable if their institutions launder money. Financial institutions are required to report suspicious transactions to the Chadian Central Bank. Banks must report monthly any domestic currency transactions over 500,000 CFA francs (about \$770) to the Central Bank. In addition, all currency transfers above 100,000 CFA francs (about \$154) from Chad to a non-CEMAC country or to Chad from a non-CEMAC country must be reported to both the Central Bank and the Ministry of Finance on a monthly basis. Banks are required to maintain records for two to 30 years, depending on the type of transaction. Banks must make customer information available to bank supervisors, the judiciary, the customs service, and tax authorities on request.

The Government of Chad (GOC) has the authority to freeze terrorist finance assets. In November 2001, the Ministry of Finance issued a directive to the Chadian Central Bank to freeze all accounts suspected of belonging to terrorist groups. The Central Bank has forwarded to Chadian banks the UN 1267/1390 consolidated list and the U.S. Government list of suspected terrorist individuals and organizations. As of the end of 2002, no suspect accounts had been identified.

On November 20, 2002, the BEAC Board of Directors approved draft anti-money laundering and counter-terrorist financing regulations that would apply to banks, exchange houses, stock brokerages, casinos, insurance companies, and intermediaries such as lawyers and accountants in all six member countries. The BEAC intends to submit the draft regulations to the Ministerial Committee of the Central African Economic and Monetary Community (CEMAC) for approval in January 2003.

If approved, the BEAC regulations would treat money laundering and terrorist financing as criminal offenses. The regulations would also require banks to record and report the identity of customers engaging in large transactions. The threshold for reporting large transactions would be set at a later date by the CEMAC Ministerial Committee at levels appropriate to each country's economic situation. Financial institutions would have to maintain records of large transactions for five years.

The regulations would require financial institutions to report suspicious transactions. Under the regulations, each country would establish a National Agency for Financial Investigation (NAFI) responsible for collecting suspicious transaction reports. Bankers and other individuals responsible for submitting suspicious transaction reports would be protected by law with respect to their cooperation with law enforcement entities. If a NAFI investigation were to confirm suspicions of terrorist financing, the Chadian government could freeze the related assets. The NAFI could cooperate with counterpart agencies in other countries.

Chad is a party to the 1988 UN Drug Convention.

Chad should criminalize terrorist financing and money laundering. Chad should also work with the BEAC to strengthen the region's anti-money laundering and counter-terrorist financing regime.

Chile. Chile has a sound modern financial sector, but is not considered a major regional financial center. There are approximately 27 financial institutions, including 16 foreign banks, nine private domestic banks, one state-owned bank, and one financial corporation. The financial sector, particularly the banks, commodities brokerages, and currency exchange houses, remains highly vulnerable to money laundering, due to the absence of comprehensive and effective anti-money laundering laws, and strict privacy laws.

Although Chile does not appear to have a significant money laundering problem, Chilean law in this area is underdeveloped. Money laundering offenses in Chile are limited only to the direct proceeds of narcotics

offenses. Chilean law also does not require a suspected money launderer to establish the legitimate source of suspicious funds. The lack of a Financial Intelligence Unit (FIU) with a full scope of authorities, the lack of reporting requirements for suspicious transactions and strict bank secrecy laws compound the investigative problem for law enforcement authorities. In addition, Chile's ports are also vulnerable to money laundering as indicated by reports and arrests related to narcotics-trafficking in these areas.

Chile's current anti-money laundering program is based on the 1995 Counter-Narcotics Law No. 19.366, which criminalized narcotics-related money laundering activities. The law allows banks to voluntarily report suspicious or unusual financial transactions. However, this law offers no "safe harbor" provisions protecting banks from civil liability, and as a result the reporting of such transactions continues to be extremely low. Law 19.366 only gives the Council for the Defense of the State (CDE) authority to conduct narcotics-related money laundering investigations. The Department for the Control of Illicit Drugs (Departamento de Control de Trafico Ilicito de Estupefacientes) within the CDE carries out this investigative function. It presently functions as Chile's Financial Intelligence Unit, and is a member of the Egmont Group. However, as a result of an ongoing reform to the criminal judicial system, a Public Ministry was established that has been gradually absorbing from the CDE the authority to carry out money laundering investigations. The transition into the new system is being done by region.

To further enhance its ability to prevent and combat money laundering, in June 2002, the Government of Chile (GOC) introduced proposed modifications to the Penal Code that include (in addition to illicit narcotics-trafficking) terrorism, illegal arms trafficking, child prostitution and pornography, and adult prostitution, as predicate offenses for money laundering. This bill, currently under consideration by the Chilean Senate's Constitutional Reform Committee, proposes creation of a financial analysis unit within the Ministry of Finance that would ultimately replace the one currently functioning with limited legal abilities within the CDE. The bill proposes mandatory reporting of suspicious transactions by banks, currency exchange houses, issuers and operators of credit cards, chambers of commerce, securities brokers, insurance companies, mutual funds administrators, remitters and transporters of funds and other valuables, casinos and horse racetracks, notaries, the Foreign Investments Committee, and the Central Bank.

Further, the bill requires the reporting of cash transactions of more than \$10,000 and imposes record keeping requirements (five years), as well as provides "safe harbor" provisions from liability to those complying with the reporting requirements. The bill also requires defendants to provide proof of the source of income in cases of illicit enrichment. The new FIU would receive and analyze the reports of suspicious financial activities and forward those deemed appropriate for further investigation to the Public Ministry. A separate bill to strengthen the Counter-Narcotics Law, particularly in the area of asset freezing and sharing, continues under separate review.

GOC officials had predicted passage of the new law by the end of 2002, but it now appears that approval will be delayed at least until early 2003. Despite the improvements in the proposed legislation, the bill still provides no mechanism for the seizure or forfeiture of suspicious assets. The United States has offered assistance to Chile on these issues, including technical assistance on asset seizure and forfeiture.

Chile is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. In November 2001, the GOC became a party to the UN International Convention for the Suppression of the Financing of Terrorism. Chile is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Chile is a member and currently holds the chair of the South American Financial Action Task Force on Money Laundering (GAFISUD) and has pledged to come into compliance with the organization's recommendations.

On August 2000, the GOC and U.S. Government (USG) signed a new letter of agreement, based under which the USG is providing counternarcotics and anticrime assistance to Chile. Although the GOC strongly supports the international coalition against terrorists, and acknowledged the USG request for assistance in identifying and freezing terrorist-related assets, it does not have the authority to issue a freeze

order. The Banking and Financial Institution Supervisory Agency provided the UNSCR 1267/1390 list and instructed them to check for accounts. However, the entities that regulate the financial system do not have legal authority to freeze bank accounts suspected of being associated with the financing of terrorists or terrorism, nor can the Executive Branch unilaterally freeze accounts. Essentially assets may be frozen only in narcotics cases. The GOC is aware of these limitations and has begun to address them.

The GOC should pass the proposed amendments to the Penal Code, criminalize the financing of terrorists and terrorism and promptly establish an effective FIU that meets the Egmont Group's standards. It should also continue efforts aimed at the passage of laws that would strengthen its ability to block, freeze and share seized assets. The GOC should also take steps to ensure that money launderers do not abuse its economically successful ports.

China, People's Republic of. Money laundering remains a major concern as the People's Republic of China (PRC) restructures its economy. Most money laundering cases now under investigation involve corruption and bribery. Narcotics-trafficking, smuggling, alien smuggling, counterfeiting, and fraud and other financial crimes remain major sources of laundered funds. Proceeds of tax evasion, recycled through offshore companies, return to the PRC disguised as foreign investment, and as such, receive tax benefits. Hong Kong-registered companies figure prominently in schemes to transfer corruption proceeds and in tax evasion recycling schemes.

After having studied how to strengthen the PRC's anti-money laundering regime over the past few years, the People's Bank of China (PBOC) and the State Administration of Foreign Exchange (SAFE) have 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.

Proposed regulations include: Rules on Management of Payment Transaction Reports and Interim Regulations on Reports of Financial Institutions Concerning Large and Suspicious Foreign Exchange Funds. Other regulatory agencies such as the China Securities Regulatory Commission and the China Regulatory Insurance Commission are preparing and implementing similar regulations for their respective financial sectors. Elements of these regulations require commercial banks to have systems, by January 2003, to monitor suspected money laundering transactions, develop anti-money laundering programs, and report large cash and suspicious transactions to the anti-money laundering department within the PBOC.

The existing and proposed measures complement the PRC's 1997 Criminal Code, which criminalizes money laundering under Article 191 for three predicate offenses—narcotics-trafficking, organized crime, and smuggling. Additionally, Article 312 criminalizes complicity in concealing the proceeds of criminal activity, and Article 174 criminalizes the establishment of an unauthorized financial institution.

The PRC is considering expanding the list of predicate offenses for money laundering, reflecting its experience in conducting investigations connected to fraud, embezzlement, and corruption. Widening the definition of money laundering will assist in international information sharing and heighten public awareness of the money laundering threat. PRC anti-money laundering efforts are hampered by the prevalence of counterfeit identity documents and cash transactions conducted by underground banks. Another structural impediment is the absence of a nationwide automated network to monitor banking transactions through the PBOC. Many inter-banking transactions from one region to another are conducted manually, which delays the PBOC's ability to prevent money laundering.

In July 2002, the PBOC set up an anti-money laundering team tasked with developing the legal and regulatory framework for countering money laundering in the banking sector. The team is chaired by the Vice Governor of the PBOC and composed of representatives of the PBOC's 15 functional departments. It also set up an office in the PBOC's Payment System and Technology Development Department to design a system for monitoring the movement of suspicious transactions through PBOC-licensed financial entities. In September 2002, SAFE adopted a new system to supervise foreign exchange accounts more

efficiently. The new system will allow for immediate electronic supervision of transactions, collection of statistical data, and reporting and analysis of transactions. The PRC has decided to establish or designate a Financial Intelligence Unit (FIU) in 2003 to enhance its anti-money laundering regime.

The United States and the PRC cooperate and discuss money laundering and other enforcement issues under the auspices of the US-PRC Joint Liaison Group's (JLG) subgroup on law enforcement cooperation. The JLG meetings are held periodically in either Washington, D.C., or Beijing.

The PRC supports international efforts to counter the financing of terrorism. Terrorist financing is now a criminal offense in the PRC 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, the PRC authorities began to actively participate in United States and international efforts to identify, track, and intercept terrorist finances, specifically through implementation of United Nations Security Council anti-terrorist financing resolutions.

While the PRC authorities have attempted to identify any terrorist assets in the PRC based on the UN 1267 Sanctions Committee's consolidated list, it was initially less cooperative relative to those named on lists issued by the United States. However, in late 2002, the PRC authorities subsequently determined that PRC law enforcement entities would grant equal legal weight to the U.S. lists and the UN consolidated list. Even so, as of November 2002, the PRC's Customs Service had not received from central government authorities copies of either the UN consolidated list or the additional U.S. lists for its use in its inspection activities. The PRC government has not identified, frozen or seized any confirmed terrorist assets to date.

The PRC signed the UN International Convention for the Suppression of the Financing of Terrorism on November 13, 2001. The United States, PRC, Afghanistan, and Kyrgyzstan jointly referred the Eastern Turkistan Islamic Movement, an al-Qaida linked terrorist organization that carries out activities in the PRC and Central Asia, to the UN 1267 Sanctions Committee for inclusion on its consolidated list. The United States and PRC 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. A high-level FATF mission visited the PRC in May 2002 for discussions on FATF membership and PRC anti-money laundering efforts, including counter-terrorist financing. The PRC expressed its willingness to participate in the work of FATF on both a political and an operational basis.

The PRC has signed mutual legal assistance treaties with 24 countries. The United States and the PRC 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 can provide a basis for exchanging records in connection with narcotics and other criminal investigations and proceedings. The FBI-staffed legal attaché office opened at the U.S. Embassy in Beijing in October 2002. The PRC is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

The PRC should continue to build upon the substantive actions taken in 2002 to develop a viable anti-money laundering regime consonant with international standards. Important steps include expanding its list of predicate crimes to include all serious crimes, continuing to develop a regulatory and law enforcement environment designed to prevent and deter money laundering, and establishing an FIU capable of sharing information with foreign law enforcement and regulatory agencies.

Colombia. The Government of Colombia (GOC) is a regional leader in the fight against money laundering. It has enacted comprehensive anti-money laundering legislation and continues to take significant measures to refine and improve its ability to combat financial crimes and money laundering. Nevertheless, drug money laundering from Colombia's lucrative cocaine and heroin trade continues to penetrate its economy and affect its financial institutions. Despite GOC efforts and funding and technical support from the United States, the magnitude of the money laundering threat combined with continued procedural difficulties in legal proceedings and limited resources continue to make Colombia a major money laundering concern.

Money Laundering and Financial Crimes

In addition to pervasive narcotics-related money laundering, Colombia confronts a money laundering threat from corruption, commercial smuggling for tax and import duty avoidance, kidnapping for profit, arms-trafficking, and terrorism connected to violent paramilitary groups and guerrilla organizations. One of the prominent methods for money laundering in Colombia is the Black Market Peso Exchange (BMPE), 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 in Colombia. Other money laundering techniques include, bulk shipment and body smuggling of narcotics-related foreign currency, the use of debit cards drawn upon financial institutions outside of Colombia, the use of exchange houses to transfer funds into and out of Colombia by wire or for bulk cash deposit in Central America, and the use of shell companies.

Colombia has broadly criminalized money laundering. In 1995, Colombia established the “legalization and concealment” of criminal assets as a separate criminal offense and, in 1997, more generally criminalized the laundering of the proceeds of extortion, illicit enrichment, rebellion, and narcotics-trafficking. Effective in 2001, Colombia’s criminal code extends money laundering predicates to reach 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 serve as nominees for the acquisition of the proceeds of 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, among other offenses, is itself an offense punishable under the criminal code, with penalties increased in 2002 to imprisonment of two to five years.

Colombian law provides for both conviction-based and non-conviction-based in rem forfeiture, giving it some of the most expansive forfeiture legislation in Latin America. Colombia’s penal law includes a general criminal forfeiture provision for intentional crimes since the 1930s, and more specific forfeiture provisions in other statutes, such as Law 30 of 1986, Colombia’s principal anti-narcotics statute. Colombia added non-conviction-based forfeiture with the enactment of Law 333 of 1996, which established “extinction of domain” procedures to extinguish property rights for assets tainted by criminal activity. Despite this expansive legislative regime, procedural and other difficulties led to only limited forfeiture successes in the past, with substantial assets tied up in proceedings for years. However, in 2002 the Anti-Narcotics and Maritime Unit of the Prosecutor General’s office used Law 333 to successfully forfeit \$35 million of U.S. currency seized with the assistance of DEA in 2001.

In 2002, the GOC took additional forceful measures to remove practical obstacles to the effective use of forfeiture to combat crime. In September, the GOC issued a decree to suspend application of Law 333 and implement more streamlined procedures in forfeiture cases. These reforms were refined and formally adopted in December through the enactment of Law 793 of 2002. Among other things, Law 793 repeals Law 333 and establishes new procedures that eliminate interlocutory appeals, which prolonged and impeded forfeiture proceedings in the past, imposes strict time limits on proceedings, and places obligations on claimants to demonstrate their legitimate interest in property. In addition, Law 793 requires expedited consideration of forfeiture actions by judicial authorities, and establishes a fund for the administration of seized and forfeited assets.

Also in December, the GOC strengthened its ability to administer seized and forfeited assets by enacting Law 785 of 2002. This new 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. The Department of Administration of Property within the Prosecutor General’s office has responsibility for the administration of approximately 1.5 million seized assets, while the DNE manages an additional 300,000 assets. The DNE, with assistance from the United States Marshals Service, is developing a modern asset management and electronic inventory system for seized assets.

In 1996, the Prosecutor General's office established a specialized task force unit of agents and prosecutors to investigate and prosecute money laundering cases and forfeiture actions. In 2002, this unit initiated 297 money laundering investigations, an increase of 23 percent over 2001, and 180 asset forfeiture investigations, an increase of 42 percent. Nevertheless, final money laundering convictions and forfeitures remain limited in number. Recent development of a document organization and exploitation team and the streamlined procedures under Law 793 may increase the number of successful actions.

In 1993, Colombia established suspicious activity and currency transaction reporting for banking institutions, and barred the entities and their employees with such reporting obligations from informing their clients of their reports to Colombian law enforcement. Wire remitters also are required to file suspicious transaction reports, and currency transactions and cross-border movements of currency in excess of \$10,000 must also be reported. Exchange houses must file currency reports for transactions involving \$750 or more. The GOC has also extended suspicious activity reporting obligations to additional institutions such as those regulated by the Superintendency of Securities, which oversees Colombia's stock exchanges, and the Superintendency of Notaries. In addition, the Superintendency of Banks has instituted "know your customer" regulations for the entities it regulates, including banks, insurance companies, trust companies, insurance agents and brokers, and leasing companies. Among other things, the Superintendency of Banks also has authority to rescind licenses for wire remitters.

Colombia formally adopted legislation in 1999 to establish a unified central Financial Information and Analysis Unit (UIAF) within the Ministry of Finance and Public Credit with broad authority to access and analyze financial information from public and private entities in Colombia. The UIAF is a member of the Egmont Group of financial intelligence units and provides expertise in organizational design and operations to other Financial Intelligence Units in Central and South America. In 2002, the UIAF received 13,343 suspicious activity reports (SARs), and forwarded 2,427 of these to the Prosecutor General's office for further investigation or prosecution.

Colombia continued to play a role in multilateral efforts to combat money laundering in 2002. Colombia is a member of the South American Financial Action Task Force (GAFISUD), a regional anti-money laundering organization modeled after the G-8 Financial Action Task Force. In 2002, Colombia underwent a mutual evaluation by fellow GAFISUD members and has provided experts for the mutual legal evaluation of other GAFISUD countries. Colombia also participates in a multilateral initiative with the Governments of the United States, Venezuela, Panama, and Aruba designed to address the problem of trade-based money laundering through the BMPE. Colombia became a signatory to the UN International Convention for the Suppression of the Financing of Terrorism in October of 2001 but has not yet become a party to the Convention.

The United States and Colombia continue to enjoy successful bilateral cooperation in money laundering and forfeiture investigations. In 2002, 40 fugitives, mostly Colombian nationals, were extradited from Colombia to the United States, including 13 on money laundering charges. Coordination between Colombia's Tax and Customs Directorate (DIAN) and the United States Customs Service (USCS), resulted in the seizure of approximately \$10 million in undeclared U.S. currency entering Colombia in 2002 and the arrest of fifteen couriers on money laundering charges entering Colombia from Mexico and Central America with amounts varying from \$200,000 to nearly \$2 million. Cooperation between USCS and Colombian law enforcement authorities in two major undercover cases resulted in more than 35 arrests and the seizure of nearly \$17 million in 2002. Colombian Judicial Police (DIJIN) and USCS expect to expand joint financial investigations in money laundering, BMPE, and terrorist financing.

Colombia should take legislative action to strengthen forfeiture, procedural impediments and other aspects of money laundering enforcement. Colombia should also consider devoting additional resources to prosecutors and investigators.

Congo, Democratic Republic of. The Congo is not a regional financial center, although its porous borders, lack of a financially sound, well-regulated banking sector and functional judicial system, and inadequate enforcement resources make it susceptible to money laundering. Money laundering in the

Money Laundering and Financial Crimes

Congo more than likely involves smuggling proceeds, as smuggling is a widespread crime in the Congo. The eastern two-thirds of the country is under the control of rebel groups and is unanswerable to the Government of the Democratic Republic of the Congo (GDRC). Most economic activity in the Congo takes place in the informal sector. In 2000, the informal sector was estimated to be at least four times the size of the formal sector. Most transactions, even those of legitimate businesses, are carried out in cash. Rebel-controlled Congo operates on a cash-only basis.

There is no law in the Congo criminalizing money laundering. In 1997, the Bank of Zaire (now the Central Bank of Congo) issued anti-money laundering guidance to banks. The guidance required that banks adhere to international anti-money laundering standards and report transactions greater than \$500 to the Central Bank. However, the Central Bank abolished these guidelines in 2000. There are no legal restrictions in the Congo prohibiting the sharing of financial account information with foreign authorities.

While there is no law criminalizing terrorist financing, both the President and the courts have the legal authority to freeze assets of terrorist organizations.

The Congo has signed, but not yet ratified, both the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention.

The GDRC should criminalize money laundering and terrorist financing and develop a viable anti-money laundering regime.

Congo, Republic of. Congo is not a regional financial center, and money laundering is not thought to be a problem. The Bank of Central African States (BEAC) supervises Congo's banking system, which is still recovering from the looting and neglect it received during Congo's civil unrest in the 1990s. BEAC is a regional Central Bank that serves six countries of Central Africa.

On November 20, 2002, the BEAC Board of Directors approved draft anti-money laundering and counter-terrorist financing regulations that would apply to banks, exchange houses, stock brokerages, casinos, insurance companies, and intermediaries such as lawyers and accountants in all six member countries. The BEAC intends to submit the draft regulations to the Ministerial Committee of the Central African Economic and Monetary Community (CEMAC) for approval in January 2003.

If approved, the BEAC regulations would treat money laundering and terrorist financing as criminal offenses. The regulations would also require banks to record and report the identity of customers engaging in large transactions. The threshold for reporting large transactions would be set at a later date by the CEMAC Ministerial Committee at levels appropriate to each country's economic situation. Financial institutions would have to maintain records of large transactions for five years.

The regulations would require financial institutions to report suspicious transactions. Under the regulations, each country would establish a National Agency for Financial Investigation (NAFI) responsible for collecting suspicious transaction reports. Bankers and other individuals responsible for submitting suspicious transaction reports would be protected by law with respect to their cooperation with law enforcement entities. If a NAFI investigation were to confirm suspicions of terrorist financing, the Congolese government could freeze and seize the related assets. The NAFI could cooperate with counterpart agencies in other countries.

Congo has signed, but not yet ratified, both the UN Convention Against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism.

Congo should criminalize money laundering and terrorist financing, and should work with the BEAC to establish a viable anti-money laundering and counter-terrorist financing regime.

Cook Islands. The Cook Islands is a self-governing group of islands in the South Pacific that maintains a free association with New Zealand. Cook Islanders are citizens of New Zealand and are part of the British Commonwealth. The Cook Islands is vulnerable to money laundering because it has an offshore sector that offers banking, insurance, international trusts, and formation of international companies (the

equivalent of international business companies (IBCs)). Marketers of offshore services on the Internet promote the Cook Islands as a favored jurisdiction for establishing asset protection trusts.

The Cook Islands remain on the Financial Action Task Force (FATF) list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering. The FATF, in its June 2000 report, cited several concerns. In particular, the Government of the Cook Islands (GOCI) had no relevant information on approximately 1,200 international companies it had registered. The country also licensed seven offshore banks that took deposits from the public, yet were not required to identify customers, nor keep records. Excessive secrecy provisions guarded against the disclosure of bank records and relevant information about the international companies. A U.S. Treasury Department advisory to U.S. financial institutions, warning them to give enhanced scrutiny to all financial transactions originating in, or routed to or through, the Cook Islands remains in force.

The GOCI's regulatory scheme is susceptible to money laundering. The International Companies Act of 1981, amended in 1982, permits issuance of bearer shares and the marketing of shelf companies. The Act prohibits public access to registers of corporate directors or managers or the disclosure of beneficial owners. While corporate directors are not required to be residents, companies must maintain a registered office and company secretary in the Cook Islands. Companies must file annual reports, but are not required to have their accounts audited.

The Offshore Industry (Criminal Provisions) Act 1995-96 requires officers and employees of the Cook Islands' six trustee companies to report to the Cook Islands Commissioner for Offshore Financial Services (COFS) suspicious activities related to narcotics-trafficking or transactions where there is actual knowledge that a serious crime has been committed. Trustee companies must provide information to the COFS to substantiate their suspicions. The COFS can petition the High Court to rescind the license of, or strike from the corporate register, offshore entities found to be involved in such crimes. Moreover, the High Court also may dispose of the assets of the business entity.

The GOCI has enacted several legislative reforms to address the deficiencies identified by the FATF. In August 2000, the GOCI passed the Money Laundering Prevention Act 2000 (MLPA), that expands the predicate offenses for money laundering, creates a Financial Intelligence Unit (FIU), mandates the reporting of suspicious transactions by financial institutions, and defines records retention and customer identification requirements for financial institutions. The anti-money laundering measures in the financial area cover both the domestic and offshore sector. The Cook Islands passed the Money Laundering Prevention Regulations in January 2002. The regulations specify the documentation required for customer identification, the retention of relevant business records, suspicious transaction reporting requirements, and time limits for the submission of such reports.

The legislation established a Money Laundering Authority (MLA) that is comprised of the financial secretary, the commissioner for offshore financial services, and the commissioner of the police, and currently constitutes the country's FIU. The GOCI is in the process of making this FIU fully operational, with the assistance of a technical advisor provided by the Government of New Zealand. The MLA receives suspicious transactions reports, sends reports to the Solicitor General when money laundering is suspected, instructs financial institutions to cooperate with investigations, compiles statistics and records for use by domestic and foreign regulators and law enforcement, issues guidelines to financial institutions, and creates record keeping and reporting requirements for financial institutions. The MLA issued Guidance Notes on Money Laundering Prevention in April 2001.

The MLPA imposes certain reporting obligations on financial institutions such as banks, offshore banking businesses, offshore insurance businesses, casinos, and gambling services. Financial institutions are required to report transactions if there is reasonable cause to suspect that the transaction involves the proceeds of a crime. Financial institutions are required to maintain, for a minimum of five years, all records related to the opening of accounts and to business transactions that exceed NZ \$30,000 (approximately \$12,900). The records must include sufficient documentary evidence to prove the identity of the customer. In addition, financial institutions are required to develop and apply internal policies,

Money Laundering and Financial Crimes

procedures, and controls to combat money laundering, and to develop audit functions to evaluate such policies, procedures, and controls. Financial institutions must comply with any guidelines and training requirements issued by the MLA.

The MLPA also requires that individuals declare cross-border movements of currency or negotiable securities greater than the equivalent of NZ \$10,000 (approximately \$4,150) to a police, customs, or immigration officer. Failure to declare cross-border movements of currency or negotiable instruments can result in a maximum fine of NZ \$1,000 (approximately \$415) and a maximum prison sentence of one year.

The MLA is authorized to cooperate with foreign governments that have entered into bilateral or multilateral mutual assistance arrangements with the GOCI. In addition, Section 21 of the MLPA makes provision for ad hoc requests, granting the Minister of Finance the power to approve cooperation with a foreign government without an agreement in place. Money laundering is an extraditable offense.

The Cook Islands is not a party to the 1988 UN Drug Convention. It is a member of the Asia/Pacific Group on Money Laundering and participated in a mutual evaluation conducted by that Group and the Offshore Group of Banking Supervisors in October 2001. The Cook Islands has not signed the UN Convention against Transnational Organized Crime, which is not yet in force internationally. The Cook Islands signed the UN International Convention for the Suppression of the Financing of Terrorism on December 24, 2001. The GOCI is also finalizing regulations to give effect to UN Security Council Resolution 1373.

The GOCI has taken a number of steps toward addressing the deficiencies identified by FATF. However, the GOCI should aggressively implement and enforce the provisions of the MLPA and the Money Laundering Prevention Regulations 2002. Moreover, the GOCI should eliminate confidentiality provisions relating to the incorporation, registration and transactions of companies and other entities, and expand oversight of the offshore sector. The Cook Islands should also staff the relevant bodies to supervise the offshore sector, and review its offshore legislation, in order to address the remaining deficiencies identified by the FATF. The GOCI should also criminalize the financing of terrorism and terrorists.

Costa Rica. Costa Rica remains vulnerable to money laundering and other financial crimes, due to the narcotics-trafficking in the region. Costa Rica is a haven for Internet gaming companies, especially sports betting, with over 100 companies active in this area. Despite a December 2001 law that expanded the scope of anti-money laundering regulations, the offshore sector continues to be largely unregulated by the government.

Low taxes and strong secrecy laws have created a growing offshore sector in Costa Rica that offers banking, corporate, and trust formation services. These 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. Instead, these banks receive or transfer funds in foreign currency, generally using correspondent accounts in other countries, thus avoiding most of the financial rules and laws of Costa Rica.

To date, the licensing procedure for foreign-domiciled banks remains inadequate. The Central Bank approves applications for foreign-domiciled banks to operate in Costa Rica by relying on a foreign jurisdiction’s certificate of good standing, rather than conducting its own due diligence. While the jurisdiction submitting the certificate must be able to enter into supervision agreements with Costa Rica and be deemed as an “adequately regulated jurisdiction” by Costa Rican authorities, this process is extremely vulnerable to corruption and abuse.

Foreign-domiciled banks are required only to provide monthly balance statements and year-end audits to the General Superintendent of the Financial System (SUGEF). The SUGEF only has authority over the domestic activity of foreign-domiciled banks. All other activity of these offshore banks is beyond SUGEF supervision.

In December 2001, Costa Rica expanded the scope of Law 7786 to criminalize the laundering of proceeds from all serious crimes. The newly expanded law obligated domestic (not offshore) financial institutions

and other businesses (casinos, jewelry dealers, money exchangers, etc.) to identify their clients, report currency transactions over \$10,000, report suspicious transactions, keep financial records for at least five years, and identify the beneficial owners of accounts and transacted funds. However, Law 7786 does not grant SUGEF the authority to conduct on-site money laundering inspections or to incorporate money laundering compliance testing in other inspections, such as the prudential safety and soundness inspections that are carried out under Law 7558.

Law 7786 also created Costa Rica's Financial Intelligence Unit (FIU), the Centro de Inteligencia Conjunto Antidrogas/Unidad de Analisis Financiero (CICAD/UAF), which is a member of the Egmont Group of FIUs. However, reporting appears to be low and Costa Rica has not yet successfully prosecuted anyone under its current anti-money laundering law.

In addition, Costa Rican authorities lack the inability to block, seize or freeze property without prior judicial approval, and thus Costa Rica lacks the ability to expeditiously freeze assets connected to terrorists and terrorism. However, Costa Rica has given U.S. authorities significant forfeiture assistance in a pending fraud case out of the Northern District of Florida by seizing and freezing substantial assets which are alleged to be the proceeds of the fraud.

There appears to be a recent surge in illicit activity related to money laundering. Indeed, there is growing evidence of black market peso exchange through private banks in Costa Rica. These exchange schemes have allowed Colombian international credit card holders and currency exchange houses to carry large sums of declared currency (often between \$100,000 and \$300,000) to Costa Rican banks. The U.S. dollars are transferred to U.S. banks and then to Colombian banks, where account holders profit from arbitrage exchange rates. It is estimated that \$225 million has entered Costa Rica in this fashion since April 2001. No Costa Rican law is broken when the currency is declared at port of exit and entry. Costa Rican banks that apply "know your client" standards acknowledge that they are not certain of the source of the currency that they are allowing to be deposited. One private bank responded positively in November 2002 to inquiries from the U.S. Embassy and the Costa Rican Drug Institute and discontinued its business relationship with a Colombian currency exchange house that had been responsible for bringing approximately \$90 million into Costa Rica. However, the Costa Rican Private Bankers' Association reported in December 2002 that three other private banks had been solicited to do business with the same Colombian exchange house.

Costa Rica ratified the 1988 UN Drug Convention in 1990. It ratified the UN International Convention for the Suppression of the Financing of Terrorism in October 2002. On March 16, 2001 Costa Rica signed, but has not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. In 2002, Costa Rica signed the OAS Inter-American Convention on Mutual Assistance in Criminal Matters, to which the United States is a party, but Costa Rica has not yet ratified. Costa Rica is a member of the Caribbean Financial Action Task Force (CFATF). Additionally, Costa Rica has signed, but its parliament has not yet ratified, an agreement with the United States under which the International Law Enforcement Academy (ILEA) for the Latin American region would be located in Costa Rica. It is anticipated that the ILEA will provide anti-money laundering training to students from throughout the region.

Costa Rica should extend its anti-money laundering regime and strengthen its supervisory control over its offshore sector, including Internet gaming activities. It should strengthen its domestic inspection capability, criminalize the financing of terrorists and terrorism and enact measures to allow it to administratively block assets.

Côte d'Ivoire. Côte d'Ivoire is an important regional financial center in West Africa. Porous borders, an ongoing armed rebellion, and regional instability contribute to Côte d'Ivoire's vulnerability to money laundering from narcotics-trafficking, corruption, and arms-trafficking. Fraud is also a source of laundered funds. Criminal proceeds laundered in Côte d'Ivoire are reportedly derived mostly from regional criminal activity organized chiefly by nationals from Nigeria and the Democratic Republic of the Congo. Police recently have seen an increase in crimes related to credit card theft and foreign bank account fraud.

Money Laundering and Financial Crimes

The Central Bank of West African States (BCEAO), based in Dakar, Senegal, is the Central Bank for the countries in the West African Economic and Monetary Union (WAEMU): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal, and Togo, all of which use the French-backed CFA franc currency. All bank deposits over approximately \$7,700 made in BCEAO member countries must be reported to the BCEAO, along with customer identification information. Cote d'Ivoire's economy accounts for 40 percent of the GDP of the WAEMU region. In September 2002, the WAEMU Council of Ministers, which oversees the BCEAO, approved an anti-money laundering regulation applicable to banks and other financial institutions, casinos, travel agencies, art dealers, gem dealers, accountants, attorneys, and real estate agents. The regulation is subject to review by member countries, which would be responsible for implementing many provisions of the regulation. The regulation is expected to go into effect in early 2003.

Under the WAEMU regulation, financial institutions would be required to verify and record the identity of their customers before establishing any business relationship. The regulation would require financial institutions to maintain customer identification and transaction records for ten years. The regulation would also impose certain customer identification and record maintenance requirements on casinos.

All financial institutions, businesses, and professionals under the scope of the WAEMU regulation would be required to report suspicious transactions. The regulation calls for each member country to establish a National Office for Financial Information Process (CENTIF), which would be responsible for collecting suspicious transactions and would have the authority to share information with other CENTIFs within the WAEMU as well as with the Financial Intelligence Units of non-WAEMU countries.

The WAEMU Council of Ministers issued another directive in September 2002 requesting member countries to pass legislation requiring banks to freeze the accounts of any persons or organizations designated by UN 1267 Sanctions Committee. The Government of Côte d'Ivoire (GOCI) is preparing a law that would provide for the freezing and seizing of terrorist finance assets.

Laundering of money related to any criminal activity is a criminal offense. Banks are required to maintain the records necessary to reconstruct significant transactions through financial institutions. Law enforcement authorities can access these records to investigate financial crimes upon the request of a public prosecutor. There are no mandatory time limits for keeping records. Côte d'Ivoire enacted a banking secrecy law in 1996 that prevents disclosure of client and ownership information, but it does allow the banks to provide information to the court in legal proceedings or criminal cases. Banks are required to adhere to "due diligence" standards.

In 2002, a national of Saudi Arabia was indicted for money laundering in Côte d'Ivoire in relation to an attempted purchase of a hotel. The case was dropped after high-level political intervention.

Law 97/1997 regulates cross-border transport of currency. When traveling from Côte d'Ivoire to another WAEMU country, Ivorians and expatriate residents must declare the amount of currency being carried out of the country. When traveling from Côte d'Ivoire to a destination other than another WAEMU country, Ivorians and expatriate residents are prohibited from carrying an amount of currency greater than the equivalent of 500,000 CFA francs (approximately \$795) for tourists, and two million CFA francs (approximately \$3,180) for business operators. Carrying currency greater than those thresholds is only permissible with approval from the Department of External Finance of the Ministry of Economy and Finance.

Côte d'Ivoire's asset seizure and forfeiture law applies to both real and personal property, including bank accounts and businesses used as conduits for money laundering. The GOCI is the designated recipient of any narcotics-related asset seizures and forfeitures. It is not known whether legal loopholes exist to permit traffickers and others to shield assets. The law does not allow for the sharing of assets with other governments.

The GOCI is considering legislative proposals regarding the regulation of alternative remittance systems.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA), based in Dakar, Senegal. In November 2002, GIABA hosted an anti-money laundering seminar for representatives of 14 ECOWAS members, including Côte d'Ivoire. In July 2002 Côte d'Ivoire participated in the 2002 West African Joint Operation Conference (WAJO) that promotes regional law enforcement cooperation against drug trafficking, terrorism, and money laundering.

Côte d'Ivoire became a party to the UN International Convention for the Suppression of the Financing of Terrorism on March 13, 2002. Côte d'Ivoire is a party to the 1988 UN Drug Convention. Côte d'Ivoire has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Côte d'Ivoire should criminalize terrorist financing and enact legislation allowing for the freezing and seizing of terrorist assets.

Croatia. With a population of less than five million and a tourism industry serving 6.5 million people each year—Croatia's most lucrative industry—Croatia is neither a regional financial nor a money laundering center. Much of the money laundering that does occur is related to financial crimes such as tax evasion and business-related fraud, although there has been a recent rise in money laundering cases with drug trafficking as the predicate crime. The proceeds of narcotics-trafficking tend to be converted into real estate and luxury goods rather than laundered for re-integration into the financial system.

In 1996, Croatia passed legislation that amended its penal code to criminalize money laundering related to serious crimes. In 1997, Croatia passed its Law on the Prevention of Money Laundering requiring banks and non-bank financial institutions to report transactions that exceed approximately \$17,500, as well as any cash transactions that seem suspicious. It also authorized establishment of a Financial Intelligence Unit (FIU), known as the Ured za Sprječavanje Pranja Novca (Anti-Money Laundering Department) within the Ministry of Finance. Croatia's FIU is a member of the Egmont Group. In 2000, Croatia's Parliament strengthened the country's penal code to ensure that all those indicted can be charged with the money laundering offense where applicable. Prior to this change, a person could not be charged with money laundering if the predicate offense carried a maximum penalty of fewer than five years in prison.

In 2001, the GOC established a National Center for the Prevention of Corruption and Organized Crime within the State Prosecutor's Office. This office has the authority to freeze assets, including securities and real estate, for up to a year. The office also has enhanced powers to seek financial transaction information and to coordinate the investigation of financial crimes. However, to date the GOC has not yet been able to staff and equip this office to its capacity.

Croatia continued the development of its anti-money laundering regime throughout 2002. The Croatian Parliament enacted a variety of legislation related to the fight against money laundering, such as the Law on Penal Responsibility of Legal Persons, the Law on Suppression of Organized Crime and Corruption, and the Law on Banks, and amended the Law on Legal Proceedings. The Parliament is now drafting new money laundering laws as well, including the new Law on the Prevention of Money Laundering and the new Law on Foreign Exchange Transactions, which includes foreign investments. However, despite efforts, there was a small number of arrests and prosecutions for money laundering or terrorism financing during 2002. Weak interagency cooperation, the insufficient technical skills of the police and prosecutors, a general lack of knowledge of exactly what constitutes a money laundering offense, and a judicial backlog of over one million cases hinder Croatia's anti-money laundering efforts.

Croatia has criminalized terrorist financing. Authorities have the authority to identify and, with a court order, freeze and seize terrorist finance assets. Law enforcement has the authority to freeze the assets of those individuals or organizations named by the UN 1267 Sanctions Committee. Croatia has established an interministerial body to evaluate and improve the country's terrorist activity prevention and repression system, and it has been cooperative in checking all international lists of possible terrorists in the financial system. The AMLD has the authority to freeze assets in the short term very easily and with little basis, but

Money Laundering and Financial Crimes

for the long term, the Prosecutor's Office requires either an international instrument or a formal legal request for an asset freeze. This may prove detrimental in the long term, because if Croatia identifies assets of entities that have not been cited by the UN, the Prosecutor's Office will have a difficult time implementing a long term legal freeze. To date, no terrorist-linked assets have been seized in Croatia.

Croatia does not have limitations on providing and exchanging information with international law enforcement on money laundering investigations. There is also no specific legislation regulating the sharing of seized assets with foreign governments. Croatian officials advise that under current law, judges can authorize asset sharing with another country.

Throughout 2002, Croatia has been actively involved with its Balkan neighbors on law enforcement cooperation, especially in cooperating to fight money laundering, and this included the establishment of a regional working group to address the issue. This working group meets twice yearly. In addition, Croatia is working in concert with Bosnia-Herzegovina to stem cross-border money laundering and smuggling. The joint efforts include the participation by authorities from both countries as well as the use of new technology and computer programs developed specifically for this purpose. Croatia also intensified its cooperation with Austria, Germany, Italy, and Slovenia regarding border control and crime. As a member of the Council of Europe's Select Committee of Experts (Moneyval, formerly PC-R-EV), Croatia has participated in mutual evaluations with the other members, both by being evaluated, and by sending experts to evaluate other states' progress. Regionally, within the Egmont Group, Croatia has assisted and supported the creation of anti-money laundering legislation and the establishment of FIUs in Albania, Macedonia, Bosnia and Herzegovina and Yugoslavia.

Croatia has signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism. Croatia has signed the Council of Europe's European Convention on the Suppression of Terrorism. Croatia has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Croatia is a party to the 1988 UN Drug Convention.

The GOC should work to improve interagency cooperation on money laundering matters and should provide sufficient resources to law enforcement authorities and the judiciary to aid them against money laundering and terrorist financing.

Cuba. The Department of State has designated Cuba as a State Sponsor of Terrorism. Cuba is not an international financial center. The Government of Cuba (GOC) controls all financial institutions, and the Cuban peso is not a freely convertible currency.

The GOC is not known to have prosecuted any money laundering cases since the National Assembly passed legislation in 1999 that criminalized money laundering related to trafficking in drugs, arms, or persons. The Cuban central bank has issued regulations that encourage banks to identify their customers, investigate unusual transactions, and identify the source of funds for large transactions. Cuba also has cross-border currency reporting requirements. Cuba has solicited anti-money laundering training assistance from the United Kingdom, Canada, France, and Spain.

Cuba is a party to both the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. Cuba has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Cuba should criminalize terrorist financing.

Cyprus. The Republic of Cyprus is a major regional financial center with a robust offshore financial services industry, and as such, remains vulnerable to international money laundering activities. Fraud and, to some extent, narcotics-trafficking are the major sources of illicit proceeds laundered in Cyprus. Offshore casinos or Internet gaming sites are not permitted in the government-controlled area of Cyprus.

In 1996, the Government of Cyprus (GOC) passed the Prevention and Suppression of Money Laundering Activities Law. This law criminalizes non-drug related money laundering; provides for the confiscation of

proceeds from serious crimes; codifies actions that banks and non-bank financial institutions must take (including customer identification); and mandates the establishment of a Financial Intelligence Unit (FIU). The anti-money laundering law authorizes criminal (but not civil) seizure and forfeiture of assets. Previously enacted legislation criminalizes drug-related money laundering. A 1998 amendment to the 1996 legislation adds criminal offenses punishable by imprisonment exceeding one year to the list of predicate offenses. The amendment also addresses government corruption, and facilitates the exchange of financial information with other FIUs, as well as the sharing of assets with other governments.

A law passed in 1999 criminalizes counterfeiting bank instruments, such as certificates of deposit and notes. In November 2000, the GOC further amended its 1996 money laundering law by eliminating the separate list of predicate offenses. This amendment, coupled with the Central Bank's guidance note to commercial banks reminding them of the importance of reporting any suspicious transaction to the FIU, has contributed to a significant increase in the number of bank suspicious activity reports from 25 in 2000 to 72 in 2002.

The Unit for Combating Money Laundering (UCML), established in 1997, serves as the FIU and is comprised of representatives from the Attorney General's Office, Customs, law enforcement, and support staff. All banks and non-bank financial institutions—insurance companies, the stock exchange, cooperative banks, lawyers, accountants and other financial intermediaries—must report suspicious transactions to the UCML. The UCML evaluates evidence generated by its member organizations and other sources to determine if an investigation is necessary. The UCML also conducts anti-money laundering training for Cypriot police officers, bankers, accountants, and other financial professionals. In July 2002, the Cypriot Parliament approved the creation of eleven new positions for UCML, which will bring its total strength to 28, including three accountants.

From January to November 2002, the UCML opened 222 cases and closed 101. During the same period, the UCML issued 22 Information Disclosure Orders and 22 freezing orders, resulting in the freezing of U.S. \$1,102,597 in bank accounts, 15 plots of land, four apartments and one vehicle. Government actions to seize and forfeit assets have not been politically or publicly controversial, nor have there been retaliatory actions related to money laundering investigations, cooperation with the United States, or seizure of assets. There have been six convictions recorded under the 1996 Anti-Money Laundering law, while twelve cases are pending.

The GOC places restrictions on foreign ownership of property and transportation of currency and bullion across the border. Cypriot law requires declaration of all cash entering or leaving Cyprus in the amount of U.S. \$1,600 or greater. Declarations over U.S. \$10,000 are sent directly to the Investigations Section of Cypriot Customs and the Central Bank of Cyprus. Cypriot law protects reporting individuals with respect to their cooperation with law enforcement. Bank employees currently are required to report all suspicious transactions to the bank's compliance officer, who determines whether to forward the report to the UCML for investigation. Banks retain reports not forwarded to the UCML, 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 activity reports submitted to the compliance officer, and the number forwarded by the compliance officer to the UCML. By law, bank officials may be held personally liable if their institutions launder money.

The Central Bank took several steps during 2001 to improve suspicious activity reporting and the identification of beneficial owners of new accounts. The Central Bank amended its requirement that commercial banks report the opening and maintenance of accounts by banks incorporated in 19 jurisdictions, to include the Former Yugoslav Republic of Montenegro. The amendment also enhances the requirement to obtain Central Bank approval for cash deposits exceeding \$100,000 per year by requiring banks to apply the annual limit to the aggregate value of deposits from family members and business associates.

In 2000, the Financial Action Task Force (FATF), in a review of Cyprus' anti-money laundering regime, raised a concern regarding customer identification with respect to all forms of trusts. In 2001, the Central

Money Laundering and Financial Crimes

Bank issued rules addressing this concern, requiring banks to ascertain the identities of the natural persons who are the “principal/ultimate” beneficial owners of new corporate or trust accounts. This rule was extended to existing accounts in 2002. This requirement will be applied in stages. By the end of November 2002, banks had to report the number of accounts that lacked complete beneficial owner information and the value of the accounts. The Central Bank will use this information to establish deadlines for obtaining complete customer identification information on the beneficial owners of these accounts. Throughout this process, banks must also adhere to the Basel Committee on Banking Supervision’s October 2001 paper titled, “Customer Due Diligence for Banks.” This paper recommends that banks regularly review existing customer identification records, particularly when a transaction of significance takes place, when customer identification standards change substantially, or when there is a material change in the way the account is operated.

A substantial amount of money was illegally transferred out of Yugoslavia while former President Slobodan Milosevic was in office. Estimates range as high as four billion dollars, with some of these funds believed to have been transferred through Cyprus. By April 2001, the GOC had turned over documents to the international war crimes tribunal in The Hague concerning possible money laundering by Milosevic and his associates. Some 250 bank accounts have been identified as belonging to Serbian offshore companies based in Cyprus.

The development of the offshore financial sector in Cyprus has been facilitated by the island’s central location, a preferential tax regime, an extensive network of double tax treaties (particularly with Eastern European 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. Cyprus’s offshore sector includes 28 banks (May 2002 assets: U.S. \$9.6 billion), 15 licensed foreign insurance companies, 108 financial services companies, eight companies that manage collective investment schemes, and 12 offshore trustee companies.

Cyprus has put in place a comprehensive anti-money laundering legal framework that meets international standards. The GOC took several additional steps in 2002 to enhance its laws. Cyprus has implemented FATF’s Special Recommendations on Terrorist Financing. As described above, the Central Bank took steps to extend to existing accounts its rules requiring identification of the beneficial owners of bank accounts. The Central Bank also required compliance officers to file an annual report outlining measures taken to prevent money laundering and to comply with its guidance notes and relevant laws. The Investment Services Law, adopted in July, will extend supervision to cover all investment services in Cyprus, including some domestic businesses not previously covered. In addition to the Central Bank’s routine compliance reviews, the UCML is now authorized to conduct unannounced inspections of bank compliance records. The UCML also maintains an active outreach and education program targeted at compliance officers, lawyers and accountants. In July 2002, the 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.

The Central Bank has in place a regulatory framework aimed at preventing abuses within the offshore sector. Offshore banks are required to adhere to the same legal, administrative, and reporting requirements as domestic banks. The Central Bank requires prospective offshore banks to face a detailed vetting procedure to ensure that only banks from jurisdictions with proper supervision are allowed to operate in Cyprus. Offshore banks must have a physical presence in Cyprus and cannot be brass plate operations (shell banks). Once an offshore bank has registered in Cyprus, it is subject to a yearly on-site inspection by the Central Bank. Following the liberalization of existing exchange controls, international banking units may now accept foreign currency deposits and extend medium- and long-term foreign currency loans to residents. Cyprus does not permit bearer shares.

At the end of 2002, there were approximately 57,600 international business companies (IBCs) registered in Cyprus. Registrations of new IBCs fell approximately 20 percent in 2002. Approximately 14,000 of these remain active and about 1,100 have a physical presence in Cyprus. Russian IBCs constitute a “significant” share of the total number of active IBCs. The Central Bank began an intensive program in 2001 to identify inactive offshore companies and to delete them from the registry. Reportedly, as of November 2002, the Central Bank had deleted approximately 21,000 companies from the registry. The names of beneficial owners of IBCs can be released to law enforcement by court order.

A 2001 International Monetary Fund (IMF) assessment of the offshore sector in Cyprus concluded that, although lack of resources meant that onsite supervision was less than optimal, Cyprus’s supervision of the offshore sector was generally “effective and thorough.” The IMF characterized Cyprus’ anti-money laundering legislative framework, as well as measures imposed by the Central Bank and other regulatory authorities, as being adequate. The report noted that, as in other offshore jurisdictions, there was still room to improve the identification of beneficial owners and the reporting of suspicious transactions, particularly in the case of non-resident controlled companies.

Profits of Cypriot offshore companies had been taxed at a rate of only 4.25 percent. However, on July 15, 2002, the Cypriot Parliament enacted a new law that provides for a uniform corporation tax rate of 10 percent for both IBCs and local companies, thus erasing a major advantage of IBCs. There is still no tax on dividends, and IBCs may keep freely transferable currency accounts both abroad and in Cyprus. If an IBC is registered as an offshore partnership, profits are not taxed. The above major changes in the tax code in 2002, the repeal of most exchange controls, new rules governing disclosure of beneficial owners, and removal of restrictions on doing business with residents of Cyprus have effectively eliminated significant differences in the treatment of offshore and domestic companies.

On November 30, 2001, Cyprus ratified the UN International Convention for the Suppression of the Financing of Terrorism. The implementing legislation amended the anti-money laundering law to criminalize the financing of terrorism. The GOC created a sub-unit within the UCML to focus specifically on the financing of terrorism. The unit reinforces the UCML with additional staff. The UCML will coordinate with the new counter-terrorism task force under the authority of the Attorney General. The Central Bank also issued a series of orders requiring domestic and offshore banks to notify it of accounts held by any individuals or organizations associated with the financing of terrorist organizations, and to freeze assets held in those accounts. These orders are based on the identification of individuals and organizations named by the UN, the United States and the European Union. These requirements apply equally to domestic and offshore banks. No bank reported holding a matching account as of the end of 2002. At the request of the Central Bank, the lawyers’ and accountants’ associations asked their members to notify the associations of any work performed on behalf of certain terrorist organizations. Both associations are cooperating closely with the Central Bank. The GOC cooperates with the United States to investigate terrorist financing.

Reportedly, there is no evidence that alternative remittance systems such as hawala or black market exchanges are operating in Cyprus. The GOC believes that its existing legal structure is adequate to address money laundering through such alternative systems. The GOC licenses charitable organizations, which must file with the GOC copies of their organizing documents and annual statements of account. The majority of all charities registered in Cyprus are domestic organizations.

Cyprus 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, which is not yet in force internationally. Cyprus is a member of the Council of Europe’s Moneyval (formerly known as PC-R-EV), and is a member of the Offshore Group of Banking Supervisors. The UCML is a member of The Egmont Group and has signed MOUs with the FIUs of Belgium, France, the Czech Republic, Slovenia, and Israel. A Mutual Legal Assistance Treaty between Cyprus and the United States entered into force September 18, 2002. In 1997, the GOC entered into a bilateral agreement with Belgium for the exchange of information on money laundering.

Money Laundering and Financial Crimes

Cyprus has been divided since the Turkish military intervention of 1974, following a coup d'état directed from Greece. Since then, the southern part of the country has been under the control of the Government of the Republic of Cyprus. The northern part is controlled by a Turkish Cypriot administration that in 1983 proclaimed itself the "Turkish Republic of Northern Cyprus." The U.S. Government recognizes only the Government of the Republic of Cyprus.

It is more difficult to evaluate anti-money laundering efforts in the "Turkish Republic of Northern Cyprus" ("TRNC"), but there continues to be strong evidence of a growing trade in narcotics with Turkey and Britain, as well as of significant money laundering activities. "TRNC" officials believe that the 21 essentially unregulated, and primarily Turkish-mainland owned, casinos are the primary vehicles through which money laundering occurs. Currency generated by these casinos is reportedly transported directly to Turkey without entering the "TRNC" banking system.

In 1999, a money laundering law for northern Cyprus 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 U.S. \$10,000. Banks are required to report to the "central bank" any electronic transfers of funds in excess of U.S. \$100,000. Such reports must include information identifying the person transferring the money, the source of the money, and its destination. Furthermore the 1999 law also prohibits individuals entering or leaving the "TRNC" from transporting more than U.S. \$10,000 in currency. Banks, non-bank 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 transactions to a central multi-agency committee that will function as an FIU and have investigative powers.

There is an offshore sector, consisting of 32 banks and 54 IBCs. The offshore banks may not conduct business with "TRNC" residents and may not deal in cash. The offshore entities are not audited and their records are not publicly available. Reportedly, a new law will restrict the granting of new bank licenses to only those banks already having licenses in an OECD country. In spite of a growing awareness in the "TRNC" of the danger represented by money laundering, it is clear that "TRNC" regulations fail to provide effective protection against the risk of money laundering. The new law of the "TRNC" provides better banking regulations than were previously in force. The major weakness continues to be the "TRNC's" many casinos, where a lack of resources and expertise leave that area, for all intents and purposes, unregulated, and therefore especially vulnerable to money laundering abuse.

Although Cyprus has criminalized money laundering for all serious crime, and passed additional legislation necessary to construct a viable anti-money laundering regime, the GOC should take steps to ensure its implementation of these laws. Additionally, Cyprus should improve the identification of beneficial owners and the reporting of suspicious transactions by non-resident controlled companies in its offshore sector. The GOC also should adequately regulate its charitable and nonprofit entities. Unless it does so, Cyprus' financial institutions will remain vulnerable to abuse by organized crime and misuse by terrorist organizations and their supporters.

Czech Republic. Both geographic and economic factors render the Czech Republic vulnerable to money laundering. Slovakia, which separated from the Czech Republic less than a decade ago, and Poland are to the east, Germany to the west, and Austria to the south. Narcotics-trafficking, smuggling, auto theft, arms trafficking, tax fraud, embezzlement, racketeering, prostitution, and trafficking in illegal aliens are the major sources of funds that are laundered in the Czech Republic. Domestic and foreign organized crime groups target Czech financial institutions for laundering activity; banks, currency exchanges, casinos and other gaming establishments, investment companies, and real estate agencies have all been used to launder criminal proceeds.

Money laundering was technically criminalized in September 1995 through additions to the Czech 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 May 2001 revision of the Criminal Code facilitates the seizure and forfeiture of bank accounts. The Financial Action Task Force

(FATF) report of July 2001 on the Czech Republic noted that the country had some major weaknesses in its anti-money laundering regime. The Czech Government—partly in the context of conforming its legislation to EU requirements—has been working to draft new laws and regulations.

In July 2002, an amendment to the Criminal Code became effective. This amendment introduces 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.

Another amendment to the Anti-Money Laundering Act is currently in preparation. This will implement the Second EU Directive and streamline the legislation regarding the identification of beneficial owners. It will also extend the responsibilities of the Czech Republic’s Financial Intelligence Unit, known as the Financial Analytical Unit (FAU), to combat terrorism financing as well as money laundering. Obligated institutions will be required to report all transactions that are suspected of being linked to terrorist financing. This amendment will become effective July 1, 2003.

The number of suspicious transaction reports transmitted to the FAU has increased significantly, as has the number evaluated and forwarded to law enforcement, indicating an active participation of the mandated entities in the anti-money laundering regime. After clarifications to the reporting requirements in 1996, reporting rose from 95 unusual transactions per annum (1996) to 1,750 suspicious transactions in 2001 and 1,179 as of November 26, 2002. The number of reports forwarded to the police increased from none the first year to 101 in 2001 and 93 as of October 31, 2002.

For years, the Czech Republic had been criticized for allowing anonymous passbook accounts to exist within the banking system. Legislation adopted in 2000 prohibited new anonymous passbook accounts. In 2002, the Act on Banks was amended to abolish all existing bearer passbooks by December 31, 2002.

The Czech Government approved the National Action Plan of the Fight Against Terrorism in April 2002. This document covers themes ranging from police work and cooperation to protection of security interests, enhancement of security standards, and customs issues. The performance of the factors identified in the Action Plan is presently under analysis. The FAU currently is distributing “terrorist lists” to relevant financial and governmental bodies. While the Czechs do not have specific laws criminalizing terrorist financing, they do have legislation permitting rapid implementation of UN and EU financial sanctions, including action against accounts held by suspected terrorist entities or individuals. Czech authorities have been cooperative in the global effort to identify suspect accounts, but none have yet been found in Czech financial institutions. A new government body called the Clearinghouse was instituted in October 2002, under the FAU; its function is to streamline input from institutions in order to enhance cooperation and response to a terrorist threat. The Czech Republic became a signatory to the UN International Convention for the Suppression of the Financing of Terrorism in 2000, but has not yet ratified it.

The Czech Republic participates in the Council of Europe’s Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, formerly PC-R-EV), and in 2001 underwent a mutual evaluation by the Committee. The Czech Republic continues to implement changes to its anti-money laundering regime based on the results of the mutual evaluation.

The United States and the Czech Republic have a Mutual Legal Assistance Treaty, which entered into force on May 7, 2000. The Czech Republic is a party to the 1988 UN Drug Convention, and in December 2000 signed, but has not ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. The Czech Republic has signed memoranda of understanding (MOUs) on information exchange with Belgium, France, Italy, Croatia, Cyprus, Estonia, Latvia, Lithuania, Poland, Slovenia, Slovakia and Bulgaria. Formalization of an agreement between the Czech Republic and Europol, the European police office, also took place in 2002. The agreement allows an exchange of information about specific crimes and investigating methods, the prevention of crime, and the training of police. Among the most important crimes cited in the cooperation agreement are terrorism, drug dealing, and

Money Laundering and Financial Crimes

money laundering. The FAU is a member of the Egmont Group, and is authorized to cooperate with its foreign counterparts, including those not part of the Egmont Group.

The Czech Republic should continue to enhance its anti-money laundering regime by adopting the suggestions of the PC-R-EV mutual evaluation report. The Parliament should pass the new amendment to the anti-money laundering legislation to strengthen the requirements on identification of beneficial owners and to criminalize terrorism financing.

Denmark. Denmark is a regional financial center. Banking procedures in Denmark are transparent and are subject to government review, which discourages prospective money launderers and minimizes the likelihood of improper use of the banking system. Denmark's Office of the Public Prosecutor for Serious Economic Crime handles economic crime cases. The Office consists of both public prosecutors and police officers specially trained in fighting economic crime.

Money laundering is a criminal offense in Denmark, regardless of the predicate offense. The 1993 Act on Measures to Prevent Money Laundering covers customer identification and mandatory suspicious transaction reporting. Denmark also has the Gambling Casino Act of 1993, which specifically addresses casino money laundering issues and customer registration information. Recently enacted legislation requires that importation of any money exceeding 15,000 euros (approximately \$14,500) be reported to customs upon entry into Denmark. Banks and other financial institutions are required to know, record, and report the identity of customers engaging in significant transactions and maintain those records for an adequate amount of time. There are no secrecy laws in Denmark that prevent disclosure of financial information to competent authorities, and there are laws that protect bankers and others who cooperate with law enforcement authorities. Denmark has regulations in place that ensure the availability of adequate records in connection with narcotics investigations. Denmark's Financial Intelligence Unit (FIU), the Money Laundering Secretariat, within the Public Prosecutor's office, provides a central point for collection of all intelligence related to money laundering. The FIU is also responsible for receiving reports on suspicions of money laundering and terrorist financing. Denmark has cooperated fully with U.S. authorities with regards to money laundering investigations.

Legislation adopted on May 5, 2002, by the Danish Parliament, extends the Money Laundering Act so that if a transaction is suspected of ties to terrorism financing it must have the prior consent of the Money Laundering Secretariat before it can be carried out. In addition, the extended Money Laundering Act now includes lawyers, accountants, tax advisors, real estate agents, money transmitters, money exchange offices and transporters of money among those required to file Suspicious Transaction Reports with the FIU. The blocking of assets either belonging to, or at the disposal of, a suspect is covered under the Danish Administration of Justice Act. Asset blocking may take place concurrent with an investigation or when charges have been filed. Seizures or forfeitures of proceeds from a criminal act performed by a person found guilty are provided for under the Danish Penal Code.

In an effort to prevent any terrorist financing or transnational crime, Denmark signed an agreement in 1999 with Australia to combat money laundering and break up illegal networks. Denmark and the United States signed a Convention for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with Respect to Taxes on Income in March 2000. The treaty has provisions to exchange information for investigative purposes. In December 2002, Denmark helped negotiate, on behalf of the EU, a U.S.-Europol agreement on the exchange of personal data and related information that will aid in tracing financial transactions and, thereby, help combat crime for which these transactions provide the economic means.

Denmark passed comprehensive anti-terrorism legislation on June 4, 2002, specifically addressing terrorist financing and implementing UNSCR 1373, and ratified the UN International Convention for the Suppression of the Financing of Terrorism in August 2002.

Denmark initiated the "Framework Decision on Combating Corruption in the Private Sector" at the European Union Council in August 2002, in order to take action to prevent and prosecute transnational

corruption and to provide for uniformity in the application of the law. Denmark is a party to the 1988 UN Drug Convention, and in 1999, ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. It participates in European Union anti-money laundering efforts, and its Financial Intelligence Unit belongs to the Egmont Group. Denmark has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision." Denmark is also a member of the Financial Action Task Force.

Dominica. While the Government of the Commonwealth of Dominica (GCOD) has recently enacted considerable legislation to address many of the deficiencies in its anti-money laundering program, there have been shortcomings in the implementation of these reforms and in its international cooperation on these matters. Such implementation and cooperation remain vital to the country's ability to combat financial crime, money laundering and the potential threat of terrorist financing, particularly in its offshore sector. Like many Caribbean jurisdictions, Dominica had initially sought to attract offshore dollars by offering a wide range of financial services and promises of confidentiality, low fees and minimal government oversight.

Dominica's financial sector includes five domestic banks and two offshore banks (a reduction from nine in 2000), 17 credit unions, 1435 IBC's, four Internet gaming companies, 18 insurance agencies and one domestic insurance company. A rapid expansion of Dominica's offshore sector without proper supervision made Dominica attractive to international criminals, and therefore, vulnerable to official corruption prompting public criticism from FATF. An additional problem has been Dominica's ongoing economic citizenship program, under which individuals can purchase Dominican citizenship (and thus Dominican passports) as well as official name changes. Prior to July 2002, the price of economic citizenship was \$50,000 for a family of four and \$25,000 for an individual. In July, the price of participating in the program was increased to \$100,000 for an individual and \$150,000 for a family of up to four persons. This increase in fees proved unpopular, however, and no passports were issued at the new price levels. Dominica subsequently lowered the cost of purchasing citizenship to \$75,000 for an individual and \$100,000 for a family of up to four persons. The GCOD heavily advertised this reduction in fees (actually an increase from pre-July rates). Dominica's economic citizenship program does not appear to be 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 Canada without visas. Between 1996 and 2002, the GCOD granted 650 economic citizenships. Noting "growing concern over the practice of selling citizenship or passport-issuing irregularities", Canada instituted a visa requirement on holders of Dominican passports in December 2001.

In June 2000, the Financial Action Task Force (FATF) identified Dominica as a Non-Cooperative Country or Territory (NCCT) in its international efforts to combat money laundering. The FATF in its report of June 2000 cited several concerns: outdated anti-money laundering legislation, inadequate identification of corporate owners and bank customers, and a largely unregulated offshore sector. The U.S. Department of Treasury also issued an advisory to U.S. financial institutions in July 2000 warning them to "give enhanced scrutiny" to financial transactions involving Dominica. Dominica was removed from the NCCT list in October 2002 on the strength of its legislative reforms, but only with a strongly worded list of ongoing conditions. The U.S. Treasury advisory remains in effect.

The GCOD has neither signed nor ratified the UN International Convention for the Suppression of the Financing of Terrorism. Dominica is the only Caribbean country which did not sign the Inter-American Convention Against Terrorism last June during the Summit in Barbados and has not yet done so. The GCOD plans to introduce anti-terrorist financing legislation to the Parliament that will provide the authority to identify, freeze and seize terrorist assets. No known evidence of terrorist financing has been discovered in Dominica to date. The GCOD has not taken any specific initiatives focused on alternative remittance systems or the misuse of charitable and non-profit entities.

Money Laundering and Financial Crimes

In response to pressure from the international community, the GCOD enacted a number of reforms to address the deficiencies in its financial sector. In July 2000, the Finance Minister announced a comprehensive review of all offshore banks and the establishment of an Offshore Financial Services Council (OFSC). The OFSC's mandate is to advise the GCOD on policy matters relating to the offshore sector and to make recommendations with respect to applications by service providers for licenses.

Under common banking legislation enacted by its eight member jurisdictions, the Eastern Caribbean Central Bank (ECCB) acts as the primary supervisor and regulator of onshore banks in Dominica. An agreement between the OFSC and the ECCB in December 2000 placed Dominica's remaining offshore banks and trusts under the dual supervision of the ECCB and the GCOD's International Business Unit (IBU). 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. During 2002, the ECCB conducted on-site inspections for anti-money laundering compliance of all onshore and offshore banks in Dominica. The inspections of the offshore banks were conducted by the ECCB in collaboration with the IBU.

The IBU supervises and regulates all offshore entities, domestic insurance companies, and registered agents, as well as visiting international business companies to ensure their compliance with the money laundering law. The manager of the IBU is also an integral part of the Money Laundering Supervisory Authority (MLSA).

Dominica enacted anti-money laundering legislation in 2000. The Money Laundering (Prevention) Act (MLPA) No. 20 of December 2000 (effective January 2001) and its July 2001 amendments criminalize the laundering of proceeds from any indictable offense. The MLPA requires financial institutions to keep records of transactions for at least seven years. The MLPA established the Money Laundering Supervisory Authority (MLSA), which 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 MLPA authorizes the MLSA to inspect and supervise non-bank financial institutions and regulated businesses for compliance with the MLPA. The MLPA requires a wide range of financial institutions and businesses, including offshore institutions, to report suspicious transactions to the MLSA, which will then send the reports to Dominica's Financial Intelligence Unit (FIU). The MLSA is also responsible for developing anti-money laundering policies, issuing guidance notes and conducting training.

The MLPA requires the reporting of cross-border movements of currency that exceed \$10,000 to the FIU. The FIU will analyze these reports of suspicious transactions and cross-border currency transactions, forward appropriate information to the Director of Public Prosecutions and liaise with other jurisdictions on financial crime cases. The MLPA further authorizes the FIU to exchange information with foreign counterparts. A new Exchange of Information Act provides for information exchange between regulators. The FIU has five trained staff and has been operational since August 2001. As of December 2002, the FIU had received 64 suspicious transaction reports, of which 36 had been investigated.

The MLPA also 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; assets may be forfeited after a conviction. 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 customer identification, record keeping and suspicious transaction reporting procedures and require compliance officers and training programs for financial institutions. 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 to the MLSA.

The Offshore Banking (Amendment) Act No. 16 of 2000 prohibits the opening of anonymous accounts, prohibits International Business Companies (IBCs) from direct or indirect ownership of an offshore bank, requires all banks licensed in Dominica to have a physical presence in Dominica, and requires disclosure

of legal and beneficial owners and prior authorization to changes in beneficial ownership of banks. The International Business Companies (Amendment) Act No. 13 of 2000 (effective January 2001) requires that newly issued bearer shares be kept with an “approved fiduciary”, who is required to maintain a register with the beneficial owner name and address. An IBC’s books, records, accounts and minutes must be kept at its registered office and are subject to government inspection. The Act precludes IBC’s from engaging in licensed financial business or licensed management services. It empowers the IBU to “perform regulatory, investigative and enforcement functions” relative to IBC’s and facilitates cooperation by the Attorney General under mutual legal assistance treaties and other similar agreements entered into with other countries. Additional amendments to the Act in September 2001 require previously issued bearer shares to be registered.

In September 2001, Dominica amended its Money Laundering (Prevention) Regulations to require Dominican institutions, within one-year, to apply customer identification procedures for existing bank accounts. Dominica is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Dominica is a member of the Caribbean Financial Action Task Force (CFATF), although its attendance has been irregular. Dominica is scheduled for its Second Round Mutual Evaluation in September 2003.

In May 2000, a Mutual Legal Assistance Treaty and an Extradition Treaty with the United States entered into force. Dominica has not responded consistently in a comprehensive and rigorous manner to USG MLAT requests. Its record of cooperation with USG law enforcement officials on money laundering cases involving its offshore banks has been spotty. Dominica is a party to the 1988 UN Drug Convention. An amendment to its Mutual Assistance in Criminal Matters Act permits judicial cooperation between Dominica and any party to the 1988 UN Drug Convention.

The GCOD should fully implement and enforce the provisions of its recent legislation, provide additional resources for regulating offshore entities, continue to develop the FIU and enhance domestic regulatory and law enforcement cooperation. The GCOD should enact legislation to criminalize terrorist financing and become a party to the UN International Convention for the Suppression of the Financing of Terrorism. The GCOD should also establish a consistent record of better quality cooperation with foreign authorities on anti-money laundering and international criminal issues. Such measures will help protect Dominica’s financial system from further abuse by international criminals.

Dominican Republic. The Dominican Republic continues to be a key point for the transshipment of narcotics moving from South America into Puerto Rico and the United States. The Dominican Republic’s financial institutions 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 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 and money remittance companies facilitate the laundering of these illicit funds.

There have been notable legislative and regulatory efforts by the Government of the Dominican Republic (GODR) to combat drug trafficking, corruption, money laundering, and terrorism. Narcotics-related money laundering has been deemed a criminal offense since the enactment of Act 17 of December 1995 (the “1995 Narcotics Law”). The Act 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 confiscated, there have been only three successful money laundering prosecutions under the 1995 Narcotics Law.

One notable event occurred on September 5, 2001 when the Dominican Republic’s National Drug Control Directorate (DNCD) and the DEA brought to fruition a year long investigation, initiated by the DNCD, with the arrest of eight people in San Juan, Dominican Republic and Orlando, Florida. These eight individuals were part of an international organization engaged in the trafficking of multi-ton

Money Laundering and Financial Crimes

quantities of cocaine and the laundering of millions of U.S. dollars in drug proceeds as well as the arrest of ten members of a Colombian-Lebanese money laundering organization operating in Colombia, New York, Miami, West Palm Beach, and San Juan, Puerto Rico. The operation netted 43 arrests, the seizure of 2,899 kilograms of cocaine and \$2,511,285.

Under Decree No. 288-1996, the Superintendency 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 report suspicious financial transactions (SARs) to the Superintendency of Banks.

In 1997, a Financial Analysis Unit (FAU) was created within the Superintendency of Banks to receive, analyze, and disseminate SAR information. The FAU also refers SARs to the Financial Investigative Unit of the DNCD for follow up investigation. The FAU is a member of the Egmont Group, and is authorized to exchange information with other Financial Intelligence Units. In 1998, the GODR passed legislation that allows extradition of Dominican nationals on money laundering charges.

In June 2002, the GODR augmented its measures to prevent and combat money laundering, drug trafficking, and related activities, with the passage of Law No. 72-02. This law expanded the predicate offenses for money laundering beyond illicit trafficking in drugs and controlled substances, to include other serious crimes such as any act related to terrorism, illicit trafficking in human beings or human organs, arms trafficking, kidnapping, extortion related to recordings and electronic film made by physical or moral entities, theft of vehicles, counterfeiting of currency, fraud against the State, embezzlement, and extortion and bribery related to drug trafficking. It broadened the requirements for customer identification, record keeping of transactions, and reporting of SARs, to numerous other financial 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/debit card companies; funds 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.

Law No. 72-02 also requires the reporting of cash transactions greater than \$10,000 to the FAU; until now these needed only to be recorded internally by the financial institutions. 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 GODR responded to U.S. Government efforts to identify and block terrorist-related funds. Although no assets were frozen, efforts continue through orders and circulars issued by the Ministry of Finance and the Superintendency of Banks, instructing all financial institutions to continually monitor accounts. On November 15, 2001, the GODR signed, but has not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism. The Dominican Republic is the current president of the Caribbean Financial Action Task Force (CFATF), and is a member of the Organization of American States 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 and a signatory to the UN Convention against Transnational Organized Crime (December 2000), which is not yet in force internationally. Cooperation with USG law enforcement on fugitive and extradition matters remains strong.

Effective implementation of the newly expanded anti-money laundering law of June 2002 constitutes a priority for the Dominican Republic, as well as sustained anti-corruption efforts. The GODR should also remain vigilant concerning controls relating to its many free zones, which may represent vehicles to facilitate money laundering.

Ecuador. Drug trafficking organizations continue to exploit Ecuador's borders while money launderers benefit from the absence of an effective anti-money laundering program. Ecuador's dollarized economy also increases the attractiveness of Ecuador as a money laundering site. Considering the country's

proximity to Colombia and Peru, some drug money laundering and investment may be taking place through the real estate market and sales of businesses or commercial contraband.

The Narcotics and Psychotropic Substance Act of 1990 (Law 108) provides for the following money laundering crimes: illegal enrichment, (Article 76), conversion or transfer of assets (Article 76, 77), and prosecution of front men (figureheads) (Article 78), but only in connection with illicit drug trafficking. A draft revision of Law 108 recently completed by the National Drug Council (CONSEP) would criminalize the laundering of money from any illicit source. However, there is broad agreement that Law 108 itself is an inappropriate vehicle for provisions that extend beyond drug offenses. An interagency group is nearing completion of a draft of a stand-alone law criminalizing the laundering of proceeds of any crime. Both draft laws will be introduced in the new congress inaugurated in January 2003.

Regulations are in place (through Drug Law 108, 1994 Financial System Law, and 1996 Banking Superintendency Resolution) requiring financial institutions to report to the National Drug Council (CONSEP) any transaction in cash or stocks over \$5,000, as well as suspicious financial transactions. Mutual societies are required to report transactions of \$5,000 and above. Financial cooperatives must report transactions of \$2,000 and higher. Electronic reporting of this information was implemented in 1999. Banks operating in Ecuador are required to maintain financial transaction records for six years. There are no due diligence or banker negligence laws that hold individual bankers responsible if their institutions launder money. However, a bank's board of directors can be held legally responsible if money laundering occurs in their institution.

Some existing laws conflict with the goal to combat 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 Superintendency of Banks (Banking Superintendency). 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.

As a result of this contradictory legal framework, the National Police must seek and obtain a court order to be able to search for and obtain financial information from banks. However, private financial institutions and banks often refuse to honor such orders, claiming that banking regulations make them answerable only to the Superintendency of Banks. In turn, the Superintendency of Banks will not accept requests for information directly from the police, but instead requires that the request come via CONSEP and will only pass the information back to CONSEP, which may fail to share it with law enforcement agencies. The CONSEP has a financial monitoring unit, but it simply collects information and does not analyze or investigate the data received.

Cooperation between other Government of Ecuador (GOE) agencies and the police falls short of the level needed for effective enforcement of money laundering statutes. The Superintendency of Companies refuses to provide any information concerning private corporations to the police. The Ministry of Finance refuses to share with the police information on stock market transactions. Data on property and tax records held by individual municipalities are not generally shared with law enforcement agencies.

In addition the CONSEP has refused to share financial reporting such as suspicious financial transaction reports with the Central Bank or other financial regulatory agencies such as the Banking Superintendency. As a result, Superintendency auditors cannot verify if a bank is doing all of the mandatory reporting required under the money laundering statutes.

Other problems with Ecuador's anti-money laundering regime include the absence of regulations requiring financial institutions to exercise due, the lack of reporting requirements on large amounts of currency brought into or taken out of the country, and the weak regulation of currency exchange businesses (casas de cambio). (On Ecuador's border with Colombia, the U.S. dollar trades at less than the official rate, banks are open seven days a week, and some exchange houses never close.)

Money Laundering and Financial Crimes

As a result of these problems, during the past five years there have been no serious investigations of drug money laundering in Ecuador. Without solid financial intelligence, it is impossible to estimate accurately the extent and nature of the money laundering problem in Ecuador. It is not known to what extent money laundering may be related to narcotics proceeds, or may be generated by other crimes such as contraband smuggling, illegal migration, corruption, bank fraud, or terrorism. Private Ecuadorian bank officials have recently expressed interest in increasing their cooperation with USG experts in order to detect and control money laundering.

The GOE has taken some steps to combat money laundering. For example, the Banking Superintendency recently created a Financial Intelligence Unit. The National Counternarcotics Police have a financial investigations unit that has received some USG-funded training. Planning has begun towards establishing an interagency financial investigations unit (FIU) including police and prosecutors. The U.S. Embassy is working with the Superintendency to provide equipment and technical assistance to these new units. The UN Office on Drugs and Crime also has offered assistance. The Superintendency has also requested technical assistance from the Organization of American States.

Several Ecuadorian banks maintain offshore offices. The Superintendency 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 banking Superintendency. These private accounting firms perform the standard audits on offshore banks that would generally be undertaken by the Superintendency in Ecuador. Bearer shares are not permitted for banks or companies in Ecuador.

Terrorist financing has not been criminalized in Ecuador. The Banking Superintendency has cooperated with the USG in requesting financial institutions to report transactions involving known terrorists, as designated by the United States as Specially Designated Global Terrorists pursuant to E.O. 13224 (on terrorist financing) or by the UN 1267 Sanctions Committee. No terrorist finance assets have been identified to date in Ecuador. The Superintendency would have to obtain a court order to freeze or seize such assets in the event they were identified in Ecuador.

Ecuador has signed (September 6, 2000), but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism. There is no domestic legislation in force aimed at preventing terrorist financing. 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 non-profitable entities to finance terrorist activities.

Ecuador is a party to the 1988 UN Drug Convention and has ratified (September 17, 2002) the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Ecuador is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Ecuador is also a member of the South American Financial Action Task Force (GAFISUD). Ecuador and the United States have an Agreement for the Prevention and Control of Narcotic Related Money Laundering that entered into force in 1994 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 Government of Ecuador (GOE) and the U.S. to share information on currency transactions.

The GOE should enact reforms to criminalize money laundering from any illicit activity and take the necessary steps to construct a viable anti-money laundering regime, criminalize the financing of terrorists and terrorism, and create mechanisms to expeditiously block terrorist assets.

The Arab Republic of Egypt. Egypt is not a major regional financial center. Cumbersome financial regulations make it an unattractive place through which to move large amounts of money. The majority of

funds laundered in Egypt represent proceeds from drug trafficking, political corruption, bank loans and other frauds, and tax evasion. There have been cases where narcotics-related money laundering sometimes involves investment in real estate or business ventures. Because of widespread mistrust of banks and fear that banking records—despite Egypt’s secrecy laws—could provide authorities with incriminating evidence, it is believed money launderers rarely use the banking system.

During the last year, Egypt has taken a number of steps to meet international anti-money laundering standards. These actions come on the heels of Egypt’s being designated in June, 2001 by the Financial Action Task Force (FATF) as “non-cooperative” in international efforts to fight money laundering. Following the “non-cooperative” designation, the U.S. Department of Treasury’s Financial Crimes Enforcement Network (FinCEN) issued an Advisory which instructs all U.S. financial institutions to “give enhanced scrutiny” to all transactions involving Egypt. As a result, Egypt passed anti-money laundering legislation (Law No. 80-2002) in May 2002. The 2002 law criminalizes laundering the proceeds of a range of crimes, including narcotics offenses, hijacking, terrorism and terrorism financing, illegal arms trading, money stealing, fraud, debauchery, organized crime, and environmental crimes.

The 2002 law also requires the declaration of foreign currency imports of over \$20,000 or equivalent, but places no restriction on the export of cash currency. It provides for international exchange of information and judicial cooperation in money laundering, and allows for the freezing and seizing of assets involved in money laundering crimes. The law updated regulations issued in June 2001 by the Central Bank of Egypt (CBE), the Ministry of Economy and Foreign Trade, and the Ministry of Planning, which impose additional anti-money laundering obligations on banks, insurance companies, and companies operating in capital markets.

Among other provisions, the law calls for the creation of a competent authority (financial intelligence unit, FIU) within the CBE to combat money laundering, and mandates the reporting of suspicious transactions by all financial institutions. The law also requires all such institutions to know their customers and keep transaction records. The law provides for penalties of imprisonment of up to seven years for money laundering offenses, and imprisonment for failure to report suspicious transactions or keep necessary records.

The new law also gives Egypt a more efficient mechanism for responding to terrorist money flows. The CBE now has the legal authority to direct the Attorney General to freeze funds if he makes a determination that the funds are being used to support terrorist activity. Prior to the law, the governor was required to file a criminal case against non-UN-designated terrorists, and funds could be frozen only after the courts render a guilty verdict.

Notwithstanding the new legislation’s positive attributes, there is a significant flaw in Article 17 which states that the perpetrator of a money laundering crime shall be exempted from the principal penalty (imprisonment) if the perpetrator reports the crime to competent authorities prior to their otherwise gaining knowledge of the crime. So long as this provision remains, the law will be materially deficient in relation to international standards and will prevent further progress for Egypt in the FATF’s NCCT process.

Presidential Decree No. 164/2002, issued in June 2002, delineates the structure, functions, and procedures of the new Egyptian FIU. The head of the unit has recently been appointed. The unit will handle implementation of the new law, including publishing the executive directives. The unit will take direction from a five-member council, headed by the Assistant Minister of Justice for Legal Affairs. Other members include the chairman of the Capital Market Authority, Deputy Governor of the Central Bank of Egypt, and a representative from the Egyptian Banking Federation. The CBE is in the process of identifying other staff members and drafting an implementation work plan. Egypt plans to have the new money laundering regime up and running by early 2003.

The Egyptian Government has shown some willingness to cooperate with foreign authorities in criminal investigations. The Egyptian Government acted promptly on asset-freezing requests from the United

Money Laundering and Financial Crimes

States. Also, Egypt is monitoring operations of domestic non-governmental organizations and charities to forestall funding of terrorist groups abroad.

The United States and Egypt signed a Mutual Legal Assistance Treaty in May 1998. Egypt is a party to the 1988 UN Drug Convention. It is a signatory to the 1999 UN International Convention for the Suppression of the Financing of Terrorism. The Egyptian Government has signed legal and judicial cooperation agreements with the United Arab Emirates, Bahrain, Morocco, Hungary, Jordan, France, Kuwait, Tunisia, Iraq, and Algeria. It has signed other international agreements, including extradition agreements and mutual judicial recognition agreements, with Italy, Turkey, and Arab League countries.

As of January 2003, Egypt remains on the FATF's list of "Non-Cooperating Countries or Territories" (NCCT). Though the Egyptian Government has made some attempt to improve the country's domestic anti-money laundering program and to cooperate internationally with criminal investigations, serious deficiencies remain. Pending amendment of the money laundering law with respect to Article 17 and pending the issuance of secondary regulations, and full implementation and enforcement of legal and regulatory reforms, the Egyptian financial system remains vulnerable to misuse for money laundering and other illicit purposes.

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, composed of 13 banks, 2 pension funds, 18 insurance companies, and 16 securities trading companies. The most significant financial contacts are with neighboring Central American countries, as well as the United States, Mexico, and the Dominican Republic. The January 2001 adoption of the U.S. dollar as legal tender together with the size and growth rate of the financial sector make the country a potentially fertile ground for money laundering.

Most money laundering is related to narcotics-trafficking, and, to a lesser degree, kidnapping, corruption, counterfeiting, fraud, and contraband. Criminal proceeds laundered in El Salvador are primarily from domestic criminal activity. There is no significant black market for smuggled goods. Most money laundering occurs through fund transfers between local banks and banks in the United States, the Dominican Republic, and Europe. There is no evidence money laundering proceeds are controlled by narcotics-traffickers, organized crime, or terrorist groups.

The 1998 "Law Against Laundering of Money and Assets" criminalizes money laundering related to narcotics-trafficking and any other criminal activity. The Unidad de Investigación Financiera (UIFa Financial Intelligence Unit (FIU)), is located within the Attorney General's Office. Also the Policía Nacional Civil (PNC) and the Central Bank have their own anti-money laundering units.

By law, financial institutions and alternative remittance systems must identify their customers, maintain records for a minimum of five years, train personnel in identification of money and asset laundering, and establish internal auditing procedures. Also, the aforementioned institutions must report suspicious transactions and transactions that exceed 500,000 colones (approximately \$57,000) to the UIF. In addition, the law includes a safe harbor provision to protect all persons who report transactions and cooperate with law enforcement authorities and "banker negligence" provisions making individual bankers responsible for money laundering at their institutions. Bank secrecy laws do not apply to money laundering investigations.

El Salvador has signed several agreements of cooperation and understanding with 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.

The UIF has been operational since January 2000 and joined the Egmont Group in June 2001. The UIF presently has a staff of six. In 2001, the UIF investigated 137 financial crime cases, and 88 cases in 2002. During 2002, four persons were arrested on money laundering charges.

Salvadoran law does not require the FIU to sign agreements in order to share or provide information to other countries. The FIU is also legally authorized to access the databases of public or private entities. The Government of El Salvador (GOES) has cooperated with foreign governments in financial investigations

related to narcotics and money laundering. The FIU works closely with the U.S. Treasury's FinCEN and readily shares and provides information to the U.S. Government in investigations and proceedings relating to narcotics, terrorism, terrorism financing, and other serious crime investigations, including 16 investigations involving 429 persons or entities related to terrorist activities.

The UIF has proposed legal reforms to require all travelers entering and departing from El Salvador to report the value of goods or cash they are carrying in excess of 100,000 colones (approximately \$11,400). Currently, the law requires sworn declarations only from incoming travelers with more than 100,000 colones (approximately \$11,400), or its foreign equivalent in cash or securities.

The GOES has the authority to freeze and seize suspected assets associated with terrorists and terrorism. The GOES provided financial institutions with the names of the individuals and entities listed by the UNSCR 1267 Sanctions Committee, the U.S. Government, and the United Kingdom, as being linked to Usama Bin Ladin. These institutions have searched for but have not located any assets related to the individuals and entities on the above referenced lists, and therefore, have neither blocked nor seized any assets related to those on such lists.

The GOES has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related and other assets of serious crimes but has no legal mechanism to share seized assets with other countries. Salvadoran law provides only for the judicial forfeiture of assets upon conviction (criminal forfeiture). The current law does not provide for civil or administrative forfeiture, although a proposal to expand the law to include certain types of civil forfeiture is under consideration. The FIU and PNC have adequate police powers to trace and seize assets, but the PNC lacks the resources to do so.

Forfeited money laundering proceeds are deposited in a special fund used to support law enforcement, drug treatment and prevention, and other government programs. Funds forfeited as the result of other criminal activity are deposited into general government revenues. In 2002, \$3.85 million in assets was seized or forfeited; in 2001, \$508,712.14; in 2000, \$5,699.22; and in 1999, \$19,723.78.

El Salvador is also a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the OAS Inter-American Convention Against Terrorism. El Salvador hosted the third regular session of the OAS Inter-American Committee Against Terrorism in January 2003, and assumed leadership of the committee. The GOES has not signed the UN International Convention for the Suppression of the Financing of Terrorism. El Salvador is party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. El Salvador signed the OAS Inter-American Convention on Mutual Assistance in Criminal Matters, to which the United States is a party, in 2002, but has not yet ratified it. The United States and the GOES do not have a bilateral Mutual Legal Assistance Treaty (MLAT). 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 growth of El Salvador's financial sector, the increase in narcotics-trafficking, and the use of the U.S. dollar as legal tender make El Salvador vulnerable to money laundering. The GOES should continue its anti-money laundering policies and strengthen its ability to seize and share assets.

Eritrea. Eritrea is a small country that has a developing financial system with limited integration with international markets and financial institutions. Its economy remains largely cash-based. There is no indication that it is a significant haven for money laundering activities. However, due to its limited regulatory structure and its proximity to regions where terrorist and criminal organizations operate, Eritrea is vulnerable to money laundering related activities.

Currently, no foreign banks are authorized to operate in the country. Central bank regulations act as a disincentive for holders of foreign currency to exchange it into local currency through licensed and regulated exchange houses. As a result, unauthorized money changers are thought to process foreign

Money Laundering and Financial Crimes

exchange transactions. Much of this foreign currency is transported as cash by members of Eritrea's far-flung Diaspora who bring the money to support their relatives and invest in real estate.

Eritrea became a party to the 1988 UN Drug Convention on January 30, 2002.

As Eritrea's financial system becomes more integrated with international markets, the government should put a priority on implementing anti-money laundering legislation, criminalizing terrorist financing, signing the UN International Convention for the Suppression of the Financing of Terrorism, and becoming party to relevant international conventions.

Estonia. Estonia has one of the most developed banking systems of the former Soviet Union (FSU). Estonia permits credit institutions to participate in a variety of activities such as leasing, insurance, and securities. While Estonia ranks highest in "transparency" of all the FSU countries, suspicions persist that Estonian financial institutions are used for laundering illegal proceeds for organized crime.

In 1999, Estonia implemented anti-money laundering legislation, and established the Information Bureau (IB), Estonia's Financial Intelligence Unit, and a separate police unit to fight money laundering. Estonia's legislation requires financial institutions to report suspicious or unusual transactions to the IB. The reporting thresholds are: the equivalent of approximately \$11,000 for non-currency transactions, and the equivalent of approximately \$5,500 for currency transactions.

Beginning in January 2002, the Financial Supervisory Authority (FSA) was established and activated. The FSA is responsible for monitoring and directing credit and financial institutions. It monitors compliance with reporting requirements and can apply administrative remedies for non-compliance. Client confidentiality may not be invoked against a request for information from the IB.

In the 1999 Money Laundering Prevention Act (MLPA), money laundering is not tied to a particular predicate crime, nor does a conviction for a predicate offense seem to be required. The Government of Estonia (GOE), however, anticipates modifying the MLPA specifically to include terrorism financing according to FATF Special Recommendations on Terrorist Financing. In the meantime, in cooperation with the FSA and commercial banks, the Bank of Estonia has elaborated several procedures and recommendations for the prevention of money laundering and combating terrorism financing. In June 2002 the FSA approved a new guideline, "Additional Measures to Prevent Money Laundering in the Credit and Financial Institutions." This guideline conforms to FATF's "Guidance for Financial Institutions in Detecting Terrorist Financing Activities." The Estonian Banking Association (EBA) has also issued more detailed instructions regarding information and documentation when opening an account or performing a transaction; the documents and data required in relations with foreign legal persons, with special attention to those founded in offshore regions; and a listing of red flags useful when opening an account, performing transactions, and analyzing transactions. Reportedly, the GOE has initiated an amendment to the existing MLPA. This draft legislation harmonizes the second EU Directive with the MLPA and further criminalizes the financing of terrorism.

Estonia is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, formerly known as PC-R-EV). The IB is a member of the Egmont Group and may exchange information with its counterparts, provided the information is used for investigative purposes only. Bank secrecy-protected information, that is to be used as evidence in court, may only be shared when a mutual assistance agreement is in place. A Mutual Legal Assistance Treaty is in force between the United States and Estonia. GOE is a party to the 1988 UN Drug Convention, and in August 2000, ratified the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. In October 2001, the GOE signed a cooperation agreement with Europol, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Estonia has signed, and in May 2002, ratified the UN International Convention for the Suppression of the Financing of Terrorism.

The GOE has been active in establishing agencies, amending current laws, and drafting new ones in its effort to strengthen its anti-money laundering regime. Estonia should criminalize terrorist financing. Every endeavor should be made to enforce best practices within its financial community.

Ethiopia. Ethiopia's location within the Horn of Africa region make it vulnerable to money laundering related activities perpetrated by transnational criminal organizations, terrorists, and narcotics-trafficking organizations. Sources of illegal proceeds include narcotics-trafficking, smuggling, trafficking in persons, arms trafficking, trafficking of animal products, and corruption. Reports indicate that alternative remittance systems are widely used by immigrant communities living within the country.

Money laundering is not a crime in Ethiopia. The country has an underdeveloped financial infrastructure, containing approximately six small private banks as well as three government banks. Currently, there are no foreign banks that operate within the country. The Central Bank has mandated that banks report suspicious transactions but the supervision capability is limited as most records and communications are not yet computerized. Foreign exchange controls limit possession of foreign currency, and the government controls the exchange of foreign currency into local currency. These restrictions encourage the use of alternative systems to remit funds and the hawala system is widespread.

As of February 2003, the Government of Ethiopia has proposed draft terrorist finance legislation, which is under preliminary review in Parliament.

Ethiopia is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Ethiopia should pass anti-money laundering legislation, criminalize terrorist financing and sign the UN International Convention for the Suppression of the Financing of Terrorism.

Fiji. Money laundering does not appear to be a significant problem in Fiji, although Fiji may be used as a drug transshipment point.

Money laundering is criminalized under the Proceeds of Crime Act of 1997. In addition, the Reserve Bank of Fiji (RBF) has issued anti-money laundering guidelines for licensed financial institutions. These guidelines require licensed financial institutions to develop customer identification procedures, keep transaction and other account records for seven years, and report suspicious financial transactions to both the RBF and the anti-money laundering unit in the Fiji Police Force's Criminal Investigation Department. These guidelines went into effect in January 2001. In the first ten months of 2002, financial institutions filed approximately 130 suspicious transaction reports. In 2002, the Fiji Police, with input from the RBF and the Association of Banks in Fiji, issued a standardized suspicious transaction reporting form.

The Permanent Secretary for Justice, along with senior representatives from the Attorney General's Office, the Office of the Director of Public Prosecutions, the Office of the Commissioner of Police, the RBF, and the Fiji Revenue and Customs Authority compose the Anti-Money Laundering Officials Committee, which meets once a month to discuss the implementation of anti-money laundering measures in Fiji. The Anti-Money Laundering Officials Committee is considering the establishment of a Financial Intelligence Unit.

Fiji is a member of the Asia/Pacific Group on Money Laundering, a FATF-style regional body. In February 2002, the APG conducted a mutual evaluation of Fiji.

Fiji is a party to the 1988 UN Drug Convention.

Fiji should criminalize terrorist financing and continue to develop its anti-money laundering regime. Fiji should also sign the UN International Convention for the Suppression of the Financing of Terrorism. Fiji should also establish a Financial Intelligence Unit.

Finland. Finland is not a regional financial or money laundering center. A "Corruption Perceptions Index" survey taken in 2002, which compiles the perception of corruption rather than actual statistics, listed Finland in first place as the country perceived to be the least corrupt. However, Finnish authorities

Money Laundering and Financial Crimes

are concerned about possible money laundering by Russian organized crime, as well as money laundering arising from fraud or other economic crimes.

In 1994, Finland enacted legislation criminalizing money laundering related to all serious crimes. Legislation enacted in 1998 compels credit and financial institutions, investment and fund management companies, insurance brokers and companies, real estate agents, pawn shops, betting services, casinos, and most non-bank financial institutions (excluding accountants and lawyers) to report suspicious transactions. Management companies and custodians of mutual funds were added in the Money Laundering Act in 1999.

Proposals submitted to the Parliament in October 2002 are under consideration for amendments concerning the Financial Action Task Force's (FATF) Eight Special Recommendations on Terrorist Financing, the obligations in the UN International Convention for the Suppression of the Financing of Terrorism; and the amendments to the EU Directive on Money Laundering. Under the proposals, terrorism and terrorist financing would be specifically included in the anti-money laundering regime. Another proposal submitted to Parliament was that the class of those obligated to report suspicious transactions be widened to include accountants, dealers and agents of valuable goods, auctioneers, and practitioners of legal professions (excluding those who act as counsel or attorneys in court trials).

The number of suspicious transactions reports (STRs) Finnish police have investigated has increased in the past three calendar years: 348 STRs in 1999, 1,109 in 2000, and 2,700 in 2001. The significant increase in STR filings may be attributed to attempts to launder funds as Finland transitioned from the markka in 1999 to the euro on January 1, 2002. The conversion rate was 1 euro = 5.9 Finnish markka, and approximately 225 million banknotes were printed by January 2002 for the Finnish transition. Trafficking in narcotics was the predicate offense for 40 percent of money laundering convictions in 2001. Money laundering represents about 10 percent of all financial crime in Finland, and approximately 75 percent of those cases have links to other countries.

In an effort to prevent avoidance and evasion of income taxes, Finland signed a tax treaty with the United States in September 1989, replacing the previous treaty signed in 1970. The current treaty has provisions to exchange information for investigative purposes.

In 1998, Finland established a Financial Intelligence Unit, the Money Laundering Clearing House (MLCH), to receive, record, and investigate suspicious transaction reports from obligated reporting institutions. The MLCH is a member of the Egmont Group.

Finland is a member of the FATF and the Council of Europe. Finland also co-operates with the European Union, the United Nations, the Baltic Sea Task Force, the Organization for Economic Co-operation and Development, and other international agencies designed to combat organized crime. Finland is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Finland is also a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of Proceeds from Crime. Finland became a party to the UN International Convention for the Suppression of the Financing of Terrorism on June 28, 2002.

Finland should criminalize terrorist financing.

France. France remains an attractive venue for money laundering because of its sizable economy, political stability, and sophisticated financial system. Common methods of laundering money in France include the use of bank deposits, foreign currency and gold bullion transactions, corporate transactions, and purchases of real estate, hotels, and works of art. A 2002 Parliamentary Report states that, increasingly, Russian and Italian organized crime networks are using the French Riviera to launder (or invest previously laundered assets) by buying up real estate, "a welcoming ground for foreign capital of criminal origin." The report estimates that between 7 and 60 billion Euros (about \$7-60 billion) of dirty money has already been channeled through the Riviera. France has enacted legislation that codifies the Financial Action Task Force (FATF) Forty Recommendations concerning customer identification, record keeping requirements,

suspicious transaction reporting, internal anti-money laundering procedures, and training for financial institutions.

France first criminalized money laundering related to narcotics-trafficking in 1987. In 1996 that criminalization was expanded to cover the proceeds of all crimes. Even though the Act made money laundering in itself a general offense, some French courts do not allow joint prosecution of individuals on both money laundering charges and the underlying predicate offense, on the grounds that they constitute the same offense.

Decree No. 2002-770 of May 3, 2002, addresses the functioning of France's Liaison Committee against the Laundering of the Proceeds of Crime. This committee will be co-chaired by the French Financial Intelligence Unit (FIU), TRACFIN (the unit for Treatment of Information and Action Against Clandestine Financial Circuits) and the Justice Ministry. It will comprise representatives from reporting professions and institutions, regulators, and law enforcement authorities.

TRACFIN is responsible for analyzing suspicious transaction reports that are filed by French financial institutions and non-financial professions. TRACFIN is a part of FINATER, a cell created within the French Ministry of the Economy, Finance, and Industry in September 2001, in order to gather information to fight terrorist financing.

TRACFIN is a member of the Egmont Group and represents the European Union FIUs at the Egmont Committee created on June 5, 2002. The French FIU may exchange information with foreign counterparts that observe similar rules regarding reciprocity and confidentiality of information.

As a member of the European Union, France is subject to the revised Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering (Directive 2001/97/EC) that will be enacted into domestic French legislation in 2003. France is a member of the FATF and a Cooperating and Supporting Nation to the Caribbean Financial Action Task Force. France is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. France ratified, in January 2002, the UN International Convention for the Suppression of the Financing of Terrorism. In October 2002 France ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. The United States and France have entered into a Mutual Legal Assistance Treaty (MLAT), which was ratified by the French Parliament and 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.

Since 1986, French anti-terrorist 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 15 November 2001 introduced several new characterizations of offenses, specifically including the financing of terrorism. The offense of financing terrorist activities (art. 41-2-2 of the Penal Code) is defined according to the UN International Convention for the Suppression of the Financing of Terrorism and is subject to 10 years' imprisonment and a fine of FF 1.5 million. The Act also includes as an offense money laundering in connection with terrorist activity (article 421-1-6 Penal Code), punishable by 10 years' imprisonment and a fine of FF 5 million. An additional penalty of confiscation of the total assets of the terrorist offender has also been introduced. Accounts and financial assets can be frozen through both administrative and judicial measures.

French authorities moved rapidly to freeze financial assets of organizations associated with al-Qaida and the Taliban, and took the initiative to put the two groups on the UN 1267 Sanctions Committee consolidated asset freeze list. France takes actions against non-Taliban and non-al-Qaida-related groups in the context of the EU-wide "clearinghouse" procedure. Within the G-8, 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. On the operational level, French law enforcement cooperation targeting terrorist financing continues to be excellent.

Money Laundering and Financial Crimes

TRACFIN has information-sharing agreements with FIUs in Australia, Italy, the United States, Belgium, Monaco, Spain, the United Kingdom, Mexico, the Czech Republic, Portugal, Finland, Luxembourg, Cyprus, Brazil, Colombia, Greece, Guernsey, Panama, Argentina, and Andorra.

France has established a comprehensive anti-money laundering regime. The Government of France should build upon this regime by expanding suspicious transaction reporting requirements to auditors and attorneys, in line with the revised EU Directive on money laundering.

Gabon. Gabon is not a regional financial center. The Bank of Central African States (BEAC) supervises Gabon's banking system. BEAC is a regional Central Bank that serves six countries of Central Africa.

On November 20, 2002, the BEAC Board of Directors approved draft anti-money laundering and counter-terrorist financing regulations that would apply to banks, exchange houses, stock brokerages, casinos, insurance companies, and intermediaries such as lawyers and accountants in all six member countries. The BEAC intends to submit the draft regulations to the Ministerial Committee of the Central African Economic and Monetary Community (CEMAC) for approval in January 2003.

If approved, the BEAC regulations would treat money laundering and terrorist financing as criminal offenses. The regulations would also require banks to record and report the identity of customers engaging in large transactions. The threshold for reporting large transactions would be set at a later date by the CEMAC Ministerial Committee at levels appropriate to each country's economic situation. Financial institutions would have to maintain records of large transactions for five years.

The regulations would require financial institutions to report suspicious transactions. Under the regulations, each country would establish a National Agency for Financial Investigation (NAFI) responsible for collecting suspicious transaction reports. Bankers and other individuals responsible for submitting suspicious transaction reports would be protected by law with respect to their cooperation with law enforcement entities. If a NAFI investigation were to confirm suspicions of terrorist financing, the Gabonese government could freeze and seize the related assets. The NAFI could cooperate with counterpart agencies in other countries.

Gabon has signed, but not yet ratified, both the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism.

Gabon should work with the BEAC to establish a viable anti-money laundering and counter-terrorist financing regime.

The Gambia. The Gambia is not a regional financial center, although it is a regional re-export center. Goods and capital are freely and legally traded in the Gambia, and, as is the case in other re-export centers, smuggling of goods occurs.

Banks in the Gambia are supervised by the Central Bank. The Central Bank receives weekly activity reports from all in-country financial institutions, and these reports must include information on any suspicious transactions. Banks and other financial institutions are required to know, record, and report the identities of customers engaging in transactions over the equivalent of \$10,000, and records of these transactions must be kept for two years. Central Bank officials perform on-site examinations of all banks and trust companies operating in the Gambia on a yearly basis. If necessary, Central Bank officials can examine a bank or trust company more than once a year. Money laundering is not a criminal offense, and the Government of the Gambia (GOG) lacks specific legal authority to freeze illicit funds.

In October 2002, the Finance Ministry and the Central Bank submitted a draft law—designed to modernize the banking and financial sector—to the IMF for review. While the text of the draft law has not been made public, the GOG has stated that the law contains provisions to combat money laundering and terrorist financing. The GOG expects to present the draft law to the National Assembly in early 2003.

The Central Bank has circulated the U.S. Government list of terrorists designated under E.O. 13224 among banks and other financial institutions in the Gambia. As of December 2002, no suspect accounts

had been identified. The GOG lacks specific legal authority to freeze accounts with suspected links to terrorists.

The Gambia is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. In July 2002, the Gambia participated in the 2002 West African Joint Operation Conference (WAJO) that promotes regional law enforcement cooperation against drug trafficking, terrorism, and money laundering.

The Gambia should enact comprehensive anti-money laundering legislation including provisions that would criminalize terrorist financing, provide legal authority for the freezing of criminal proceeds and funds linked to terrorist financing, and establish a Financial Intelligence Unit. The Gambia should also examine its re-export sector to determine whether or not it is being used to launder criminal proceeds.

Georgia. Georgia has a small economy and is not a regional financial center. The scope of money laundering in Georgia involves small-scale schemes with proceeds from various illegal activities. Contraband, which is a large part of the “shadow economy” in Georgia, generates substantial revenues. Estimates of the “shadow economy” are in the range of 60 percent of GDP. Reportedly, some commercial banks have become involved in laundering funds generated by the smuggling of alcohol and cigarettes, but these proceeds are generally held in dollars outside the banking system. Most financial transactions in Georgia are conducted in cash. Only between three to five percent of the population currently maintain a personal bank account, as following independence there was a mushrooming of banking institutions, the majority of which collapsed, causing bank customers serious losses. Corruption also remains an issue in Georgia. Overall, Georgia is very vulnerable to money laundering, as there are serious deficiencies in the anti-money laundering system in all areas—legal, financial and law enforcement.

Legislation to combat both terrorism financing and money laundering is minimal and those laws that do exist are not enforced. Georgia’s criminal code of June 2000 does not criminalize money laundering, but makes it a crime to “transform illegal money into legal income” or to conceal the source, location or owner of property acquired illegally. Violators of this law are subject to imprisonment. The criminal code does not make any provisions for suspicious transaction reporting, and there are no legal safeguards to protect banks and other financial institutions that cooperate with law enforcement agencies. There are no laws that allow for any of the Ministries or the National Bank of Georgia to monitor bank accounts and collect information on depositors and the source of investments. Georgia has strict banking secrecy regulations. Currently, there are no controls on the amount of money that may be brought into the country. The money laundering controls that do exist are not applied to non-bank financial institutions.

Currently, the National Bank of Georgia (the Central Bank) has been charged with preparing relevant legislative changes. It has prepared a draft law on the prevention of money laundering. Reportedly, the draft meets the recommendations of the Financial Action Task Force on Money Laundering, with a clear commitment of the banking and financial authorities to fight money laundering. The draft is being circulated among the Ministries and to the National Bank of Georgia for comments and proposals, and is expected to be considered by the Georgian parliament during the first quarter of 2003. The draft legislation contains provisions on recording large currency transactions and the source, destination and ownership of funds.

The National Bank of Georgia plays a growing role in regulating the banking industry. Current banking legislation, including the “Law on the National Bank of Georgia,” does not allow a banking institution to trace the routing of money through a bank account or multiple bank accounts.

The U.S. Government provides technical assistance and training to the Georgian tax inspectorate in support of improvements in tax policy and regulation, which could enable the tax inspectorate to identify underreporting of income, including questionable gains from illegal sources.

There are no laws that deal with prosecuting individuals who raise funds for terrorist activities, or who are involved in terrorist acts in other countries. There are no provisions that make it a crime to handle money,

but not be directly involved in a terrorist act. There are no laws concerning charitable organizations' funding sources.

The lead on complying with UN Security Council Resolutions 1267/1390/1373 has been taken by the Ministry of Finance and the National Bank of Georgia on an ad hoc basis in support of the Global War on Terror, but it is unclear how this fits into the Georgian legal system. The Supreme Court of Georgia has ruled that the freezing, confiscation and forfeiture of illegal proceeds is unconstitutional, which may present a barrier to the implementation of the draft legislation. The National Bank of Georgia and the Ministries of Finance and Foreign Affairs have been provided by the Embassy with relevant information concerning the UN 1267 Sanctions Committee's Consolidated List.

Georgia has passed 10 of the 12 UN conventions relating to terrorism. Georgia is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. On July 7, 2002 Georgia ratified the UN International Convention for the Suppression of the Financing of Terrorism.

Georgia should adopt appropriate legislation to explicitly criminalize money laundering and the support and financing of terrorism. Provisions for suspicious activity reporting, record keeping and identification of account holders should be enacted and should be applied to banks and non-bank financial institutions. Georgia should adequately regulate alternative remittance systems and non-governmental organizations, including charities, to ensure they are not used for terrorist or other criminal ends. Georgia should establish government mechanisms to regulate and monitor currency movements and financial transactions and to enforce its laws. Until it does so, Georgia's financial institutions will remain vulnerable to abuse by organized crime and as well as to terrorist organizations and their supporters.

Germany. Germany has the largest economy in Europe and a well-developed financial services industry. Russian organized crime groups, the Italian Mafia, and Albanian and Kurdish narcotics-trafficking groups launder money through German banks, currency exchange houses, business investments, and real estate.

The Money Laundering Act, which was 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, and imposes due diligence and reporting requirements on financial institutions. Under the current law, financial institutions are required to obtain customer identification for transactions exceeding 15,000 euros (approximately \$15,000) that are conducted in cash or precious metals. Germany has had this requirement for some time (in DM), but the information was only used for statistical purposes; only recently has the information been used in money laundering investigations.

In May 2002, the banking, securities, and insurance industry regulators were merged into a single financial sector regulator known as BaFIN. Also in 2002, Germany established a single, central, federal Financial Intelligence Unit (FIU) within the Bundeskriminalamt (National Police Office). The FIU functions as an administrative unit and will be staffed with financial market supervision, customs, and legal experts. Though not yet fully operational, the FIU will be responsible for developing money laundering cases before they go to prosecutors for formal investigation. It will also exchange information with its counterparts in other countries.

The amendments also brought German laws into line with the first and second European Union money laundering directives (Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering, as revised by Directive 2001/97/EC). These include the mandate that member states standardize and expand "suspicious activity" reporting requirements to include information from notaries, accountants, tax consultants, casinos, luxury item retailers, and attorneys. Since 1998, the Federal Banking Supervisory Office has licensed and supervised money transmitters, and has issued anti-money laundering guidelines to the industry. Germany also has a law, entered into force in 1998, that gives border officials the authority to compel individuals to declare imported currency above a certain threshold (formerly DM 30,000).

The new anti-money laundering package also requires the country's banking supervisory authority to compile a central register of all bank accounts, including 300 million deposit accounts. Banks will use computers to analyze their customers and their financial dealings to identify suspicious activity. The legislation also calls for stiffer checks on the background of owners of financial institutions and tighter rules for credit card companies. Banks that have suspicions of money laundering must report their suspicions to the FIU as well as to the Staatsanwaltschaft (State Attorney), and then they may freeze the account.

Regulations for freezing assets are in place and the Ministry of Finance is considering amending the Banking Act further to increase the ability to freeze accounts. The Government of Germany (GOG) has established procedures to enforce its asset seizure and forfeiture law. The number of asset seizures and forfeitures remains low because of the high burden of proof that prosecutors must meet in such cases. German law requires a direct link to narcotics-trafficking before seizures are allowed. German authorities cooperate with U.S. efforts to trace and seize assets to the extent that German law allows, and the GOG investigates leads from other nations. However, German law does not allow for sharing forfeited assets with other countries.

The GOG moved quickly after the September 11, 2001, terrorist attacks in the United States, to identify weaknesses in Germany's laws that permitted at least some of the terrorists to live and study in Germany, unobserved and unnoticed, prior to September 11. Germany's cabinet has submitted, and the Bundestag has passed, two packages of legislation to modify existing laws. The first package closes large loopholes in German law that have permitted members of foreign terrorist organizations to live and raise money in Germany, and have allowed extremists to advocate violence in the name of religion under "religious privilege" protections. The second package went into effect January 1, 2002. It enhances the capabilities of federal law enforcement agencies, and improves the ability of intelligence and law enforcement authorities to coordinate their efforts and share important information, as they attempt to identify terrorists residing and operating in Germany. Germany's internal intelligence service is provided access to information from banks and financial institutions, postal service providers, airlines, telecommunication and Internet service providers.

The Wirtschaftsministerium (Ministry of Economics) receives the international lists of suspected terrorists and distributes the lists as separately issued regulations to the industries. Banks are directed to freeze the accounts of individuals and groups on the list and report them to the FIU independent of the standard regulations. In 2002, the Bundestag added terrorism and terrorism financing to the predicate offenses for money laundering as defined by Penal Code 161.

Germany's strict data privacy laws have made it difficult for authorities to monitor and take action against financial accounts and transfers used by terrorist networks. The situation is changing rapidly in the aftermath of the attacks on the United States. The GOG responded quickly to freeze over 30 accounts of entities associated with terrorists. New measures introduced in the second security package require financial institutions to make more data on suspicious transactions available to authorities. Although Germany signed the UN International Convention for the Suppression of the Financing of Terrorism in 2000, it has not yet ratified the Convention.

The GOG cooperates fully with the United States on anti-money laundering initiatives, though it does not have a Mutual Legal Assistance Treaty (MLAT) with the United States. The GOG exchanges information with the United States through bilateral law enforcement agreements and other informal mechanisms. Germany has MLATs with numerous countries, and German law enforcement authorities cooperate closely at the EU level, such as through Europol.

Germany is a member of the Financial Action Task Force (FATF), the European Union, and the Council of Europe. The head of BaFIN, Jochen Sanio, is the outgoing President of FATF. Germany 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, which is not yet in force internationally.

Money Laundering and Financial Crimes

Recently, the GOG put forward a number of important proposals to further strengthen its anti-money laundering regime. The GOG's new anti-money laundering package reflects Germany's commitment to combat money laundering, and to cooperate with international governments. Germany's cooperation will be strengthened with the implementation of its Financial Intelligence Unit. The GOG should continue to enhance its anti-money laundering regime and its active participation in the international fora.

Ghana. Ghana is not a regional financial center. However, non-bank financial institutions such as foreign exchange bureaus are suspected of being used to launder the proceeds of drug trafficking. In addition, donations to religious institutions allegedly have been used as a vehicle to launder money. There have also been increases in the amount of "advanced fee" scam letters intercepted that originated in Ghana.

Ghana has criminalized money laundering related to drug trafficking and other serious crimes. Law enforcement can compel disclosure of bank records for drug-related offenses, and bank officials are given protection from liability when they cooperate with law enforcement investigations. Ghana has cross-border currency reporting requirements. In December 2001, the Bank of Ghana began drafting money laundering legislation designed to increase the government's financial oversight capabilities.

The Narcotic Drug Law of 1990 provides for the forfeiture of assets upon conviction of a money laundering offense. The Government of Ghana in 2002 made no arrests or prosecutions related to money laundering.

In August and September 2002, the Narcotics Control Board in collaboration with the Ghana Police Service, Ghana Immigration Service, Bureau of National Investigations, Aviation Security, and Customs, Excise and Preventive Service conducted an interdiction exercise at Ghanaian airports. Through this exercise, currency worth \$200,000 was seized on suspicion of money laundering.

Ghana participated in the formation of the Inter-Governmental Action Group Against Money Laundering (GIABA) at the December 2001 meeting of the Economic Community of West African States in Dakar. In July 2002, Ghana also hosted the 2002 West African Joint Operation Conference (WAJO) that promotes regional law enforcement cooperation against drug trafficking, terrorism, and money laundering.

Ghana is a party to the 1988 UN Drug Convention. Ghana ratified the UN International Convention for the Suppression of the Financing of Terrorism on September 6, 2002. Ghana has endorsed the Basel Committee's "Core Principles" for Effective Banking Supervision. Ghana has bilateral agreements for the exchange of money laundering-related information with the United Kingdom, Germany, Brazil, and Italy.

Ghana should criminalize terrorist financing and should take steps to develop an anti-money laundering regime in accordance with international standards.

Gibraltar. Gibraltar is a largely self-governing overseas territory of the United Kingdom, which assumes responsibility for Gibraltar's defense and international affairs. As part of the European Union, Gibraltar is required to transpose all relevant EU directives, including those relating to anti-money laundering.

The Financial Services Commission (FSC) is responsible for regulating and supervising Gibraltar's financial services industry. It is required by statute to match UK supervisory standards. Both onshore and offshore banks are subject to the same legal and supervisory requirements. Gibraltar has 19 banks, ten of which are incorporated in Gibraltar, and all except one are subsidiaries of major international financial institutions. The FSC also licenses and regulates the activities of trust and company management activities insurance companies, and collective investment schemes. There were 8620 international business companies (IBCs) registered in Gibraltar in 2002. Bearer shares are permitted. Internet gaming is permitted by the Government of Gibraltar (GOG) and is subject to a licensing regime.

The Drug Offences Ordinance (DOO) of 1995 and Criminal Justice Ordinance of 1995 criminalize money laundering related to all crimes and mandate reporting of suspicious transactions by any person whose suspicions of money laundering are aroused and includes such entities as 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.

Gibraltar was one of the first jurisdictions to introduce and implement money laundering legislation that covered all crimes. The Gibraltar Criminal Justice Ordinance to combat money laundering, which related to all crimes, entered into effect in January 1996. Comprehensive anti-money laundering Guidance Notes (which have the force of law) were also issued to clarify the obligations of Gibraltar's financial service providers.

Also in 1996, Gibraltar established the Gibraltar Coordinating Centre for Criminal Intelligence and Drugs (GCID) to receive, analyze, and disseminate information on financial disclosures filed by institutions covered by the provisions of Gibraltar's anti-money laundering legislation. The GCID incorporates the Gibraltar Financial Intelligence Unit (GFIU), and is a sub-unit of the Gibraltar Criminal Intelligence Department. The GFIU consists mainly of police and customs officers, but is independent of law enforcement. The GFIU has applied to join the Egmont Group of FIUs.

In 2000, the Financial Action Task Force (FATF) conducted a review of Gibraltar's anti-money laundering program against the 25 Criteria employed in the Non-Cooperative Countries and Territories (NCCT) exercise. While Gibraltar was not placed on the NCCT list, the FATF noted a number of concerns, particularly with regard to suspicious transaction reporting and customer identification and verification.

In response to the issues raised by the FATF, the GOG is currently drafting amendments to their anti-money laundering legislation. The amendments will provide direct reporting requirements of suspicious transactions, and extend the provisions of the anti-money laundering legislation to cover company formation agents and trust services providers.

The FSC redrafted the anti-money laundering guidance notes (in July 2002) to abolish the present system for introducer certificates and to require institutions to review all accounts opened prior to April 1, 1995 to ensure that they are in compliance with the new "know your customer" (KYC) procedures. The FSC also took this opportunity to introduce new guidelines related to correspondent banking, politically exposed persons, and bearer securities as well as clearer and more defined KYC procedures. Gibraltar has adopted and implemented the European Union (EU) Money Laundering Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering. The United Kingdom has not extended the application of the 1988 UN Drug Convention to Gibraltar. The Mutual Legal Assistance Treaty between the United States and the United Kingdom also has not been extended to Gibraltar. However, application of 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. Also, the DOO of 1995 provides for mutual legal assistance with foreign jurisdictions on matters related to narcotics-trafficking and related proceeds. Gibraltar has indicated its commitment, as part of the EU decision on its participation in certain parts of the Schengen arrangements, to update mutual legal assistance arrangements with the EU and Council of Europe partners.

Gibraltar is a member of the Offshore Group of Banking Supervisors (OGBS). The FATF (under the aegis of the OGBS) conducted an on-site evaluation of Gibraltar in April 2001 against the FATF 40 Recommendations on Money Laundering. The report on Gibraltar found that "Gibraltar has in place a robust arsenal of legislation, regulations and administrative practices to counter money laundering," adding: "The authorities clearly demonstrate the political will to ensure that their financial institutions and associated professionals maximize their defenses against money laundering, and cooperate effectively in international investigations into criminal funds. Gibraltar is close to complete adherence with the FATF 40 Recommendations".

The Government of Gibraltar also invited the International Monetary Fund (IMF) to perform an assessment in May 2001 of the extent to which Gibraltar's supervisory arrangements for the offshore

financial sector complied with certain internationally accepted standards. The assessment was carried out on the basis of the “Module 2” assessment in accordance with the procedures agreed by the IMF’s Executive Board in July 2000. The evaluation found that “...supervision is generally effective and thorough and that Gibraltar ranks as a well-developed supervisor.” Gibraltar was found to be fully compliant or partially compliant with all but one of the 67 international standards of supervision in the areas of banking, insurance and securities. The standard that was found not to be met was in relation to on-site visits to insurance companies. This has been fully addressed by the FSC.

Gibraltar has also worked towards implementing the FATF Eight Special Recommendations on Terrorist Financing and giving effect to the relevant UN resolutions on the same issue. Arrangements are presently being made to introduce a licensing and supervisory regime in relation to money transmission services.

Gibraltar should take steps to ensure that Internet marketers of financial services offered by the GOG do not engage in false advertising that can harm Gibraltar’s reputation as a well-regulated offshore financial center.

Greece. While not a major financial center, Greece is vulnerable to money laundering related to drug trafficking, trafficking in women and children, arms smuggling, blackmail, and illicit gambling activities conducted predominantly by Russian and Albanian criminal organizations. Capital disclosure requirements for prospective foreign investors are weak. As a result, Greece’s five private and two state-owned casinos are susceptible to money laundering. The cross-border movement of illicit currency and monetary instruments is a continuing problem. During 2002, the cross-border transport of foreign currency into Greece increased, with the money often being deposited temporarily in Greek banks and then transported abroad.

The Government of Greece (GOG) criminalized money laundering derived from all crimes in 1995. The 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 non-bank financial institutions file suspicious transaction reports (STRs). New legislation passed in March 2001 targeted organized crime by making money laundering a criminal offense when the property holdings being laundered are obtained through criminal activity or cooperation in criminal activity.

The 1995 law also established the Competent Committee (CC) to receive and analyze STRs and to function as Greece’s Financial Intelligence Unit (FIU). The CC is chaired by a senior judge and includes representatives from the Central Bank, various government ministries, and the stock exchange. If the CC believes that an STR warrants further investigation, it forwards the STR to the Financial Crimes Enforcement Unit (SDOE), a multi-agency group that functions as the CC’s investigative arm. The CC is also responsible for preparing money laundering cases on behalf of the Public Prosecutor’s office.

The Bank of Greece (through its Banking Supervision Department), the Ministry of National Economy and Finance (which supervises the Capital Market Commission), and the Ministry of Development (through its Directorate of Insurance Companies) supervise Greek credit and financial institutions. Supervision includes the issuance of guidelines and circulars, as well as on-site examinations aimed at checking 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 are required to send to the Bank of Greece a monthly report on their daily purchases and sales of foreign currency. All persons entering or leaving Greece must declare to the authorities any amount they are carrying over 2,000 euros (\$2,017). Reportedly, however, cross border currency reporting requirements are not uniformly enforced at all border checkpoints.

Banks in Greece must demand customer identification information when opening an account or conducting transactions that exceed 15,000 euros (\$15,130). Greek citizens must provide a tax registration number if they conduct foreign currency exchanges of 1,000 euros (\$1,008) or more, and proof of compliance with tax laws in order to conduct exchanges of 10,000 euros (\$10,087) or more. Banks and

financial institutions are required to 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. Reporting individuals are protected by law.

Greece's Central Bank stepped up measures to counter money laundering, as part of its effort to cooperate with an investigation by authorities in Belgrade into the illegal transfer of funds abroad during the rule of former Yugoslav President Slobodan Milosevic, an alleged war criminal. There have been several arrests for money laundering since January 2002. These involve the Greek owners (and their spouses) of vessels transporting cocaine from Colombia and other Western Hemisphere countries. The guilty parties received five-year sentences. Legitimate businesses can be seized if used to launder drug money. The government recently seized a hotel that was used as a cutting mill and storage facility for drugs. As Greece is becoming a major gateway for illegal narcotics to the Balkans, Western Europe and the United States, the amount of assets seized has steadily increased.

Last year, the GOG seized an estimated \$20 million in assets for narcotics-related crimes. There have been no objections from banking and political groups to the GOG's policies and laws regarding money laundering.

The Ministry of Justice unveiled legislation on combating terrorism, organized crime, money laundering, and corruption in March 2001; Parliament passed the legislation in July 2002. Regarding the freezing of accounts and assets, Greece is committed to incorporating in its internal regulations the EU Council Framework Decision on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime, and the EU Council regulation on combating financing of terrorism, and the freezing of funds or other financial assets. Within the first six months of 2003, Greece is expected to adopt internal legislation criminalizing terrorist financing by amending its 1995 anti-money laundering law to include terrorism financing as a predicate offense.

The Bank of Greece and the Ministry of Economy and Finance have the authority to identify, freeze, and seize terrorist assets. The Bank of Greece has circulated to all financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list. Suspect accounts (of small amounts) have been identified and frozen. On June 8, 2000, Greece signed, but has not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism.

Illegal immigrants or individuals without valid residence permits are known to send remittances to Albania and other destinations in the form of gold and precious metals, which are often smuggled across the border in trucks and buses. As of December 2002, there were no legislative initiatives regarding the regulation of alternative remittance systems. Charitable and non-government organizations are closely monitored by the financial and economic crimes police as well as tax authorities; there is no evidence that such organizations are being used as conduits for the financing of terrorism.

Greece is a member of the Financial Action Task Force, the European Union, 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, which is not yet in force internationally. Greece has signed bilateral police cooperation agreements with Egypt, Albania, Armenia, France, the United States, Iran, Israel, Italy, China, Croatia, Cyprus, Lithuania, Hungary, Former Yugoslav Republic of Macedonia, Poland, Romania, Russia, Tunisia, Turkey and Ukraine. It also has a trilateral police cooperation agreement with Bulgaria and Romania. Greece exchanges information on money laundering through its MLAT with the United States, which entered into force November 20, 2001.

The GOG should extend and implement suspicious transaction reporting requirements for gaming and stock market transactions, and should to adopt more rigorous standards for casino ownership or investments. Additionally, Greece should ensure uniform enforcement of its cross-border currency reporting requirements. If Greece has not already done so, it should criminalize the financing and support of terrorists and terrorism.

Grenada. There has been improvement in Grenada's anti-money laundering regime and its supervision of its financial sector. Grenada also has demonstrated consistently good cooperation with the U.S. Government (USG) by responding rapidly to requests for information involving money laundering cases. Like those of many other Caribbean jurisdictions, the Government of Grenada (GOG) raises revenue from the offshore sector by imposing licensing and annual fees upon offshore entities. As of December 2002, Grenada had 13 offshore bank and five trust companies; all are under some type of GOG regulatory or liquidator control. There was one international insurance company, two company managers and 2,775 IBCs. Grenada's domestic financial sector includes six commercial banks, 15 registered domestic insurance companies, 22 credit unions and two money remitters. In December 2002, the GOG began revoking legislation that had allowed foreigners to buy economic citizenship, and thus Grenadian passports. This economic citizenship program had been inadequately regulated and had been abused by international criminals.

The collapse of the First International Bank of Grenada (FIBG) in 2000 highlighted the serious deficiencies in Grenada's existing counter-money laundering regime, but it also prompted the GOG to accelerate legislative reforms concerning anti-money laundering and financial sector regulation and to begin revoking the licenses of suspicious offshore banks. A U.S. citizen founded the offshore bank FIBG by using a purchased Grenadian passport, assets from a Nauruan bank, and fictitious documents to document his purported financial worth. A liquidator's report issued in March 2001 estimated FIBG's liabilities at \$206 million and assets at \$46 million, and indicated that FIBG had transferred funds to accounts in Grenada, St. Vincent, Jersey and Uganda. The liquidator found FIBG's deposit insurance program a "sham" and concluded that since its inception, the business of FIBG had been carried on "with the intent to mislead depositors and creditors."

In September 2001, the Financial Action Task Force (FATF) placed Grenada on the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering. The FATF in its report cited several concerns: inadequate access by Grenadian supervisory authorities to customer account information; inadequate authority by Grenadian supervisory authorities to cooperate with foreign counterparts; and inadequate qualification requirements for owners of financial institutions.

In April 2002, the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) issued an Advisory advising banks and other financial institutions operating in the United States to give enhanced scrutiny to all financial transactions originating in or routed to or through Grenada, or involving entities organized or domiciled, or persons maintaining accounts, in Grenada. FinCEN cited the legal, supervisory, and regulatory systems of Grenada as creating significant opportunities and tools for the laundering and protection of the proceeds of crime.

As a result of the international scandal caused by the FIBG collapse and the FATF/NCCT listing, the GOG embarked on a concerted effort to put its financial sector in order. Grenada's Money Laundering Prevention Act (MLPA) of 1999, which came into force in 2000, criminalized money laundering related to offenses under the Drug Abuse (Prevention and Control) Act whether occurring within or outside of Grenada, or other offense occurring within or outside of Grenada, punishable by death or at least five years imprisonment in Grenada.

The MLPA also established a Supervisory Authority (SA) to receive, review and forward to local authorities suspicious activity reports from obliged institutions and imposed customer identification requirements on banking and other financial institutions. The Supervisory Authority also issues anti-money laundering guidelines pursuant to section 12(g) of the MLPA that direct financial institutions to maintain records, train staff, identify suspicious activities, and designate reporting officers. The guidelines also provide examples to assist bankers to recognize and report suspicious transactions. Financial institutions must report Suspicious Activity Reports (SARs) to the SA within 14 days of the date that the transaction was determined to be suspicious. A financial institution or an employee who willfully fails to file a SAR or makes a false report will be liable to criminal penalties that include imprisonment or fines up to EC\$250,000, and possibly revocation of the financial institution's license to operate.

Financial sector legislation was strengthened and the Grenada International Financial Services Authority (GIFSA), which monitors and regulates offshore banking, was brought under stricter management. An amendment to the GIFSA Act (No. 13 of 2001) eliminated the regulator's role in marketing the offshore sector. Currently GIFSA has a staff of 12. GIFSA makes written recommendations to the Minister of Finance in regards to the revocation of offshore entities' licenses and also issues certificates of incorporation to international business companies.

International business companies are regulated under the International Companies Act. The Act requires registered agents to maintain records of the names and addresses of directors and beneficial owners of all shares, as well as the date the person's name was entered or deleted on the share register. Currently, there are seven registered agents licensed by the GIFSA. There is a \$30,000 penalty and possible revocation of the registered agent's license for failure to maintain records. The International Companies Act also gives GIFSA the authority to conduct onsite inspections to ensure that the records are being maintained on IBCs and bearer shares. GIFSA began conducting inspections in August 2002. Under the MLPA, the SA also has power to conduct money laundering inspections.

The International Financial Services (Miscellaneous Amendments) Act 2002 required all offshore financial institutions to recall and cancel any issued bearer shares and to replace them with registered shares. The holders of bearer shares in non-financial institutions must lodge their bearer share certificates with a licensed registered agent. These agents are required by Grenada law to verify the identity of the beneficial owners of all shares and to maintain this information for seven years. GIFSA was given the authority to access the records and information maintained by the registered agents and can share this information with regulatory, supervisory and administrative agencies.

The Minister of Finance has signed a memorandum of understanding (MOU) with the Eastern Caribbean Central Bank (ECCB). The MOU grants the ECCB oversight of the offshore banking sector in Grenada. Currently, legislation is being drafted that would incorporate the ECCB's new role into the offshore banking legislation. The ECCB will have the authority to share bank and customer information with foreign authorities. The ECCB already provides similar regulation and supervision to Grenada's domestic banking sector.

In 2001 and 2002, the GOG passed further substantial legislation to improve its structure: the Offshore Banking (Amendment) Act No. 10 of 2001, the Company Management (Amendment) Act No. 11 of 2001, the International Companies (Amendment) Act of 2001, the Grenada International Financial Services Authority (Amendment) Act No. 13 of 2001, the Money Laundering (Prevention)(Amendment) Act No. 19 of 2001, the Proceeds of Crime (Amendment) Act No. 20 of 2001, the International Trusts (Amendment) Act No. 21 of 2001, and the International Financial Services (Miscellaneous Amendments) Act No. 02 of 2002.

Grenada's legal framework now effectively enables GIFSA to obtain customer account records from an offshore financial institution upon request and to share the customer account information with other regulatory, supervisory and administrative bodies. GIFSA also has the ability to access auditors' working papers, and can share this information as well as examination reports with relevant authorities.

Although Grenada remains on the NCCT list, Grenada's efforts to put into place the legislation and regulations necessary for adequate supervision of Grenada's offshore sector prompted the FATF to move Grenada to the implementation stage in the NCCT de-listing process and the FATF/NCCT Americas Review Group to conduct an on-site assessment visit to Grenada in December 2002. In June 2001, the GOG established a Financial Intelligence Unit (FIU) that is headed by a police inspector and staffed by five officers and two support personnel. The FIU, which operates within the police force but is assigned to the SA, is charged with receiving suspicious activity reports from the SA and with investigating alleged money laundering offenses. The United States contributed computers, furniture, and equipment for the FIU office, and the U.S. and the Caribbean Anti-Money Laundering Program, a program funded jointly by the United States, the United Kingdom and the European Union, are providing on-going mentoring in FIU management and asset seizure techniques.

Money Laundering and Financial Crimes

The GOG should pass anti-terrorist financing legislation that will provide the authority to identify, freeze and seize terrorist assets. There has not yet been any known identified evidence of terrorist financing in Grenada. GOG has not taken any specific initiatives focused on alternative remittance systems or the misuse of charitable and non-profit entities.

A Mutual Legal Assistance Treaty and an Extradition Treaty have been in force between Grenada and the United States since 1999. Grenada's cooperation under the MLAT recently has been excellent. Grenada is an active member of the Caribbean Financial Action Task Force (CFATF), underwent a CFATF mutual evaluation in November 1999 and will undergo a Second Round evaluation in March 2004. Grenada is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and is a party to the 1988 UN Drug Convention.

Although Grenada has significantly strengthened its regulation and oversight of its financial sector in 2001 and 2002, it must remain alert to potential abuses and steadfastly implement the laws and regulations it has adopted. The GOG should pass anti-terrorist legislation that criminalizes the financing of terrorists and terrorism and that will provide the authority to identify, freeze and seize terrorist assets. The GOG should continue to expose GIFSA, SA and FIU staff to available training opportunities. The GOG should also continue to enhance its information sharing, particularly with other Caribbean jurisdictions.

Guatemala. Guatemala's location on a major drug transit route and its historic lack of a broad-based anti-money laundering regime make the country vulnerable to money laundering. Officials of the Government of Guatemala (GOG) believe that criminals deposit their illegal proceeds in bank accounts and subsequently invest the funds in real estate or large commercial projects. Some law enforcement sources believe that the laundering of proceeds from kidnapping, tax evasion, vehicle theft, and corruption is on the rise. Guatemala remains on the Financial Action Task Force's (FATF) list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering.

The Guatemalan financial services industry is comprised of 32 commercial banks, approximately 13 offshore banks, seven money exchangers, 18 insurance companies, 21 financial societies (bank institutions that act as financial intermediaries specializing in investment operations), 32 bonded warehouses, five wire remitters, and 160 cooperatives (similar to credit unions) and 13 fianzas (financial guarantors). The Superintendency of Banks (SIB), which operates under the general direction of the Monetary Board, has oversight and inspection authority over the 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.

In June 2001, the Financial Action Task Force (FATF) placed Guatemala on the NCCT list. In its report, the FATF noted: (1) Secrecy provisions in Guatemalan law constitute a significant obstacle to administrative authorities' anti-money laundering efforts, (2) Guatemalan law fails to provide for the sharing of information between Guatemalan administrative authorities and their foreign counterparts, (3) Guatemala's laws criminalize money laundering only in relation to drug offenses and not for all serious crimes, and (4) Guatemala's suspicious transaction reporting system does not prohibit "tipping off" the person involved in the transaction.

Since the FATF designation, the GOG has taken important steps to reform its anti-money laundering program in accordance with international standards. On April 25, 2001, the Guatemalan Monetary Board issued Resolution JM-191, approving the "Regulation to Prevent and Detect the Laundering of Assets" (RPDLA) submitted by the Superintendency of Banks. The RPDLA, effective May 1, 2001, requires all financial institutions under the oversight and inspection of the Superintendency of Banks to establish counter-money laundering measures, and introduces requirements for transaction reporting and record keeping. Obligated institutions must establish money laundering detection units, designate compliance officers, and train personnel. Also, obligated institutions must identify all customers opening new accounts, and must report customers conducting transactions (cash or other types) of \$5,000 or more a day (or national currency equivalent) to the bank's manager. Accounts opened prior to May 1, 2001, are not subject to the customer identification requirements of the RPDLA. If, however, a customer performs

a cash transaction for more than \$5,000, the bank must fully identify the customer and the customer must submit the information regardless of when the account was opened. The regulation also requires obligated entities to monitor, record, and report transactions considered “unusual” or “suspicious” to the Superintendency of Banks within ten days of detection.

In November 2001, Guatemala enacted Decree 67-2001, “Law Against Money and Asset Laundering” (LAMAL), to address several of the deficiencies identified by the FATF. Article 2 of the LAMAL expands the range of predicate offenses for money laundering from drug offenses to any crime. Individuals convicted of money or asset laundering are subject to a non-commutable 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.

The LAMAL also adds new record keeping and transaction reporting requirements to those already in place as a result of the RPDLA. These new requirements apply to all entities under the oversight of the Superintendency of Banks, as well as several other entities including credit card issuers and operators, check cashers, sellers or purchasers of travelers checks or postal money orders, and currency exchangers. The requirements also apply to off-shore entities that are described by the LAMAL as “foreign domiciled entities” that operate in Guatemala but are registered under the laws of another jurisdiction.

Among other things, the LAMAL prohibits obligated institutions from maintaining anonymous accounts or accounts that appear under fictitious or inexact names. Covered institutions 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, the leasing of safety deposit boxes, or the execution of cash transactions exceeding \$10,000 (or national currency equivalent). For cash transactions in excess of \$10,000, the LAMAL requires obligated institutions to maintain a daily registry of the transactions. Obligated institutions also must adopt measures to obtain, update, and store information regarding the beneficial owners of accounts where there is doubt as to their true identity. The LAMAL obligates individuals and legal entities to report cross-border movements of currency in excess of \$10,000 (or national currency equivalent) with the competent authorities. Under the LAMAL, obligated entities must maintain records of these registries and transactions for five years.

Bearer shares are permitted by non-banks and there is banking secrecy. However, since the passage of the 2001 money laundering legislation, confidentiality or banking secrecy cannot be used to prevent law enforcement officials from obtaining information related to bearer shares or any other financial instruments. It is unclear how the issuers of bear shares will meet the requirements for customer identification under the LAMAL.

The LAMAL obligates offshore or foreign domiciled entities operating in Guatemala to comply with the same anti-money laundering measures (reporting and record keeping requirements) as domestic institutions. In June 2002, Guatemala enacted the Banks and Financial Groups Law (No. 19-2002), which places offshore banks under the oversight of the Superintendent of Banks. However, the LAMAL will not take effect for the offshore entities until June 2003 at the earliest.

The LAMAL also establishes the Intendance for Verification (IVE) within the Superintendency of Banks—the equivalent of a Financial Intelligence Unit (FIU)—to supervise obligated financial institutions to ensure compliance with the law. 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 may impose sanctions on financial institutions for non-compliance. The LAMAL calls for the IVE to analyze the information it obtains, to offer domestic law enforcement support in connection with money laundering offenses, and to exchange information with similar foreign entities pursuant to a memorandum of understanding.

The IVE is operational and has a staff of 24. From January 2002 to October 31, 2002, the IVE received 394 suspicious transactions reports. Financial institutions regularly file suspicious transaction report and, during 2002 the IVE received approximately 102,667 currency transaction reports that were entered into

Money Laundering and Financial Crimes

the unit's database and some led to investigations. The IVE, however, has not been very cooperative with GOG law enforcement entities. In particular, there is reluctance on the part of the IVE and SIB to share information with prosecutors. This disconnect between regulators and prosecutors is probably the biggest impediment for successful money laundering investigations and prosecutions. In fact, over a year after passing the money laundering legislation, only four cases have been forwarded to the Public Ministry for further investigation and prosecution, and there have been no money laundering convictions.

The Public Ministry within the Public Prosecutor's Office against Corruption created the Anti-Money or Other Assets Laundering Unit. This Public Prosecutor's Office processes cases involving money laundering. As of December 9, 2002, ten money laundering cases initiated by the Special Prosecutor's Office had been filed for prosecution in local criminal courts.

The GOG passed reforms to the "narcoactivity" legislation in 1998 to allow the police to use narcotics traffickers' seized assets. The new money laundering legislation allows for 50 percent of the money to be used by the IVE and others involved in combating money laundering. However, the Supreme Court has resisted this, stating that constitutionally the court has the right to all seized assets. This position has never been legally challenged. An additional problem is that the courts do not allow for seized currency to be deposited into accounts. It must be preserved as evidence in its entirety, until the case is finished. In spite of this attitude, the court has made no real effort to use the assets either, with many cars, boats, and planes rusting away and large sums of money held in evidence lockers. 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.

Guatemala has taken a number of initiatives with regards to terrorist financing. According to the GOG, Article 391 of the Penal Code already sanctions all preparatory acts leading up to a crime, and financing would likely be considered a preparatory act. Technically, both judges and prosecutors could issue a freeze order on terrorist assets, but no test case has validated these procedures. There is no known credible evidence of terrorist financing in Guatemala, and the GOG has been very cooperative in looking for such funds. The GOG is developing legislation against terrorist financing; the inter-agency committee has completed a draft comprehensive counter-terrorism law that includes provisions against terrorist financing. The President has requested that a Spanish legal expert review the proposed legislation before the President presents it to Congress. At the same time, Congress has begun drafting its own legislation specifically to address terrorism financing. This law is intended to function as a complement to the 2001 money laundering law.

Guatemala is a party to the 1988 UN Drug Convention. In November 2000, the GOG ratified the Central American Convention for the Prevention of Money Laundering and Related Crimes. The GOG signed, but has not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Guatemala is a member of OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering, and the Caribbean Financial Action Task Force (CFATF). Guatemala became a party to the UN International Convention for the Suppression of the Financing of Terrorism on February 12, 2002.

The GOG should pass legislation on the financing of terrorists and terrorism and continue efforts to implement the reforms to its anti-money laundering regime. Guatemala should also focus its efforts on boosting its ability to successfully investigate and prosecute money launderers. The biggest hurdle facing Guatemala in the long term may very well be the increasing reach and power of the organized crime organizations that daily utilize corruption, intimidation, and impunity to carry out their illegal business.

Guernsey. The Bailiwick of Guernsey (BOG) covers a number of the Channel Islands (Guernsey, Alderney, Sark, and Herm in order of size and population). The Islands are known as Crown Dependencies because the United Kingdom is responsible for their defense and international relations. However, the BOG is not part of the United Kingdom. Guernsey's parliament legislates in the criminal law field for BOG. Alderney and Sark have their own separate parliaments and civil law systems.

The BOG is a sophisticated offshore financial center and, as such, it continues to be vulnerable to money laundering at the layering and integration stages. Since 1988, the Guernsey Financial Services Commission (the Commission or FSC) has regulated the BOG's financial services businesses. The BOG regulates banks, insurance companies, collective investment schemes, investment firms, fiduciaries, company administrators, and company directors. The BOG does not permit bank accounts to be opened unless there has been a "know your customer" inquiry and verification details are provided. Company incorporation is by act of the Royal Court, which maintains the registry. The court will not permit incorporation unless the Commission and Law Officers of the Crown have given approval.

Guernsey has 70 banks, all of which have offices, records, and a substantial presence on the island. The banks are licensed to conduct business with residents and non-residents alike. There are 579 international insurance companies, and 525 collective investment funds. There are also 19 bureaux de change, which file accounts with the tax authorities. Many are part of a licensed bank, and it is the bank that publishes and files accounts. The Commission conducts regular onsite inspections and analyzes the accounts of all regulated companies.

There are 15,910 companies registered in the BOG. The Commission does not regulate most international business companies (IBCs). Approximately half are owned by non-residents and have exempt tax status. The remainder of the companies are owned by local residents and are trading or private investment companies. Exempt companies do not fall within the standard definition of an IBC. Exempt companies are not prohibited from conducting business in the BOG, but must pay taxes on profits of any business conducted in those islands. Exempt companies must file beneficial ownership information with the Commission. Companies can be incorporated in Guernsey and Alderney, but not Sark, which has no companies legislation. The incorporation of shelf companies, that is using companies that are already in existence to speed incorporation, is not allowed.

In December 2000, the Commission prepared a consultation paper, jointly with the Crown Dependencies of Jersey and the Isle of Man, called "Overriding Principles for a Revised Know Your Customer Framework," to develop a consistent approach on anti-money laundering. The consultation paper stated that each institution would have to conduct an exercise to check its way of doing business to determine that there is sufficient information available to prove customer identity.

The Proceeds of Crime (Bailiwick of Guernsey) Law 1999 (as amended) is supplemented by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2002. These Regulations replaced Regulations enacted in 1999. The legislation criminalizes money laundering on an all crimes basis, except for drug trafficking, which, as noted, is covered by the Drug Trafficking Law 2000. The Proceeds of Crime Law and secondary legislation are supplemented by Guidance Notes on the Prevention of Money Laundering and Countering the Financing of Terrorism. There is no exemption for fiscal offenses. The 1999 Law created a system of suspicious transaction reporting (including tax evasion) to the Guernsey Financial Intelligence Service (FIS). BOG drug 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 consolidated and extended money laundering legislation related to narcotics-trafficking. It introduced the offense of failing to disclose the knowledge or suspicion of drug money laundering. The duty to disclose extends outside of financial institutions to others, for example, bureaux de change and check cashers.

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. Guernsey is a member of the Offshore Group of Bank Supervisors.

Money Laundering and Financial Crimes

On April 1, 2001, the Regulation of Fiduciaries, Administration Businesses, and Company Directors, etc. (Bailiwick of Guernsey) Law, 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 created Codes of Practice for Corporate Service Providers, Trust Service Providers, and Company Directors. Under the law, all fiduciaries, corporate service providers, and persons acting as company directors of any business must be licensed by the Commission. In order to be licensed, these agencies must pass strict tests. These include possession of “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.

On September 19, 2002, the United States and Guernsey signed a Tax Information Exchange Agreement. 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.

There has been anti-terrorism legislation covering the BOG since 1974. The Terrorism (Bailiwick of Guernsey) Law, 2002 replaced the 1990 anti-terrorism legislation. The 2002 Law replicates equivalent UK legislation. The provisions of UN Security Council Resolutions 1373 and 1390 were enacted in domestic law on the same days as enacted in the UK. The BOG has requested that the UK Government seek the extension of the BOG of UN International Conventions on the Suppression of the Financing of Terrorism and the UN International Convention for the Suppression of Terrorist Bombing.

The Crown Dependencies Anti-Money Laundering Group is a forum where the Attorney General from the Crown Dependencies, Director General of the regulatory bodies, police, Customs, and the FIUs meet to coordinate the anti-money laundering and anti-terrorism policies and strategy in the Dependencies.

Suspicious transaction reports are filed with the FIS, Guernsey’s financial intelligence unit. The FIS is the central point within Guernsey for the gathering, collating, evaluating, and disseminating of all financial crime intelligence. The Guernsey FIS is a member of the Egmont Group.

After extension to the BOG, Guernsey enacted the necessary legislation to implement the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters, the 1990 Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime, and the 1988 UN Convention against the Illicit Traffic of Narcotics and Psychotropic Substances. The 1988 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 BOG in 1996.

Guernsey has put in place a comprehensive anti-money laundering regime, and has demonstrated its ongoing commitment to fighting financial crime. BOG officials should continue to carefully monitor its anti-money laundering program to assure its effectiveness, and cooperate with international anti-money laundering authorities.

Guinea. Guinea has an unsophisticated banking system and is not a regional financial center. Banking leaders in Guinea estimate that 70 to 80 percent of business transactions take place in cash. Several expatriate communities in Guinea maintain strong ties to their countries of origin and are sources of international currency transfers. Both formal and informal money transfer services have expanded greatly in Guinea in recent years. Guinea has an active black market for foreign currency—especially euros, U.S. dollars, and CFA francs. Guinea’s mining industry leads to an influx of foreign currency. In addition to large mining operations, Guinea has an industry of small-scale, traditional mining. This industry, which deals primarily with diamonds and gold, lends itself to money laundering, as few records are kept and sales are made in cash. In 2002, Guinean police seized over \$1.5 million high-quality counterfeit U.S. currency tied to gold and diamond trade. Some narcotics-trafficking occurs in Guinea.

Section 4 of the Guinean Penal Code criminalizes money laundering related to narcotics-trafficking. Violations are punishable by 10 to 20 years in prison and a fine of \$2,500 to \$50,000. While some commercial banks in Guinea are voluntarily using software or other methods to detect suspicious transactions, no anti-money laundering regime is in place. The Ministry of Finance has approached an

international accounting and consulting firm to assist the Government of Guinea in writing an anti-money laundering law.

No money laundering cases were prosecuted in 2002.

Guinea is a party to the 1988 UN Drug Convention and has signed, but is not yet a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

Guinea should enact comprehensive anti-money laundering legislation that criminalizes money laundering and terrorist financing.

Guyana. Guyana is not an important regional financial center. The scale of money laundering, though, is thought to be large given the size of the informal economy, which is estimated to be 30 percent of the size of the formal sector. Money laundering has been linked to trafficking in drugs and firearms, as well as corruption and fraud.

Political instability and an internal security crisis have significantly impaired Guyana's efforts to bolster its anti-money laundering regime. Investigating and trying money laundering cases is not a priority for law enforcement as its attention has been diverted to the internal security crisis. The Government of Guyana (GOG) made no arrests or prosecutions for money laundering in 2001, nor were there any arrests or prosecutions for money laundering or terrorist financing in 2002.

The Money Laundering Prevention Act passed in 2000 is not yet in force, due to the lack of implementing legislation. Crimes covered by the Money Laundering Prevention Act include illicit narcotics-trafficking, illicit trafficking of firearms, extortion, corruption, bribery, fraud, counterfeiting, and forgery. The law also requires that incoming or outgoing funds over \$10,000 be reported. Licensed financial institutions are required to report suspicious transactions, although banks are left to determine thresholds individually according to banking best practices. Suspicious activity reports must be kept for six years. The legislation also includes provisions regarding confidentiality in the reporting process, good faith reporting, penalties for destroying records related to an investigation, asset forfeiture, international cooperation, and extradition for money laundering offenses.

The GOG has not yet established a financial intelligence unit. Currently, the fraud branch of the Guyana Police Force's Criminal Investigation Division is responsible for tracing and seizing assets.

The Ministry of Foreign Affairs and the Bank of Guyana, the country's Central Bank, continue to assist U.S. efforts to combat terrorist financing by working towards coming into compliance with UNSCRs 1333, 1368, and 1373. In December 2001, the bank, 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, 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.

Guyana is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and participated in the 2002 round of evaluations of drug strategies. CICAD noted numerous deficiencies in implementation, resources, and political will. Guyana is now also a member of the Caribbean Financial Action Task Force (CFATF), but has not yet undergone a mutual evaluation by that organization. Guyana is a party to the 1988 UN Drug Convention. Guyana has not signed the UN Convention against Transnational Organized Crime, which is not yet in force internationally. It has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

Guyana should create a financial intelligence unit and adopt measures that would allow it to block terrorist assets. As the security situation stabilizes, it should devote more resources to the investigation and prosecution of money laundering.

Money Laundering and Financial Crimes

Haiti. Haiti is not a major regional financial center, and—as investigative and enforcement units are yet to begin to operate—we do not know the extent of money laundering. Given Haiti’s dire economic condition low level of financial sector development and unstable political situation, it is doubtful it is of major significance in the formal financial sector. Alleged money laundering activities appear to be related to narcotics (primarily cocaine) proceeds, although there is a significant amount of contraband passing through Haiti. Criminal proceeds are reportedly derived primarily from domestic activity.

While informal and parallel market activity in Haiti is significant and may be partly funded by narcotics proceeds, smuggling is historically prevalent in Haiti pre-dates narcotics-trafficking. Money laundering occurs in the banking system and in the non-bank financial system, including casinos. Further complicating the picture is the cash that is routinely transported to Haiti from Haitians in the United States in the form of remittances. Distinguishing between legal transfers and illegal flows is no easy task. To our knowledge, money laundering proceeds are controlled by local drug-trafficking organizations. There are allegations that senior government officials may profit from the proceeds from illegal drug transactions. There is no indication of terrorist financing. Haiti, however, is used as a stopover by illegal migrants from several countries.

In recent years, Haiti has taken steps to address its money laundering problems. Since August 2000, Haiti, through Central Bank Circular 95, has required banks, exchange brokers, and transfer bureaus to obtain declarations identifying the source of funds exceeding 200,000 gourdes (approximately \$5,200) or its equivalent in foreign currency. Covered entities must report these declarations to the competent authorities on a quarterly basis. Failure to comply can result in fines up to 100,000 gourdes (approximately \$2,600) or forfeiture of the license of the bank. Unfortunately, because of widespread official laxity and rampant corruption and the fact that nearly two thirds of Haiti’s economy is informal, large amounts of money do not flow through the legitimate financial system that is governed by these regulations.

In April 2001, the Haitian government published the “Law on Money Laundering from Illicit Drug Trafficking and other Crimes and Punishable Offenses.” All financial institutions and natural persons are subject to the money laundering controls established in the new law. The law criminalizes money laundering which it defines as “the conversion or transfer of assets for the purpose of disguising or concealing the illicit origin of those assets or for aiding any person who is involved in the commission of the offense from which the assets are derived to avoid the legal consequences of his acts; the concealment or disguising of the true nature, origin, location, disposition, movement, or ownership of property; and the acquisition, possession or use of property by a person who knows or should know that this property constitutes proceeds of a crime under the terms of this law.” The law provides for relatively long prison sentences and large fines totaling millions in gourdes, and applies to a wide range of financial institutions, including banks, money exchangers, casinos, and real estate agents. Insurance companies are not covered, but as yet represent only a nascent industry in Haiti. The money laundering law requires natural persons and legal entities to verify the identity of all clients, record all transactions, including their nature and amount, and submit the information to the Ministry of Economy and Finance.

In 2002, Haiti formed a National Committee to Fight Money Laundering, the *Comite 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. The CNLBA, through the Financial Intelligence Unit (FIU) or *Unite Centrale de Renseignements Financiers (UCREF)*, is responsible for receiving and analyzing the reports. This information may be exchanged with foreign agencies. Entities or persons are required to report to the UCREF any transaction involving funds that appear to be derived from a crime. Failure to report is punishable by more than three years’ imprisonment. Banks are required to maintain records for at least five years and are required to present this information to judicial authorities and financial information service officials upon request. Article 3.4.1 states that bank secrecy or professional secrecy may not be invoked as grounds for refusing to furnish the information required by article 2.27 or requested in the scope of a laundering investigation ordered by the senior judge of the court of first instance or conducted under the authority of an examining magistrate. Articles 4.2.4 and 4.2.5 have “due

diligence” provisions. The national drug control law addresses the issue of international transportation of illegal-source currency.

The law also requires financial institutions to establish money laundering prevention programs and to verify the identity of customers who open an account or conduct transactions that exceed 200,000 gourdes (approximately \$5,200). When stock or currency transactions exceed 200,000 gourdes and are of a suspicious nature, financial institutions are required to investigate the origin of those funds and prepare an internal report. These reports are available (upon request) to the UCREF. The UCREF was created through an August 2000 circular by the Ministries of Justice and Public Security and is mentioned in the 2001 money laundering law.

However, the money laundering commission is not yet fully functional, and no director general of the UCREF has been appointed. Furthermore, the UCREF does not meet the international standards established for FIUs, and the Egmont Group does not recognize the UCREF. Additionally, corruption and the large informal economy have prevented the 2001 anti-money laundering law from being fully implemented and enforced. There have been no arrests or prosecutions for money laundering or terrorism, as the system is not yet effectively operating.

At present, Haiti is considering modifications to the law to strengthen the judicial procedure and asset seizure and forfeit provisions. The senior judge of the court of first instance may order the freezing of funds or accounts for eight days. While assets and businesses can be seized, the government cannot declare them forfeited until there is a conviction, which does not happen often in Haiti. The judicial branch is the deciding organization, but seizures and use of seized assets is on an ad hoc basis.

The money laundering law has provisions for the exchange of records with other countries, but there is no specific agreement with the United States. Haiti cooperated with the United States following the September 11 attacks. The money laundering law provides for investigation and prosecution in all cases of illegally derived money. Under this law, terrorist finance assets may be frozen and seized. The commission printed and circulated to all banks the list of individuals and entities included on the UN 1267 Sanctions Committee’s consolidated list. The Central Bank chaired meetings with all bank presidents and requested their cooperation.

Beyond this, Haiti has made little progress in the area of terrorist financing. The government has not passed legislation criminalizing the financing of terrorists and terrorism, nor has it signed the UN International Convention for the Suppression of the Financing of Terrorism. Haiti has signed, but not yet ratified, the UN Convention on Transnational Crime, which is not yet in force internationally. Haiti is also a party to the 1988 UN Drug Convention. Haiti is a member of the OAS/CICAD Experts Group to Control Money Laundering, and it recently became a member of the Caribbean Financial Action Task Force (CFATF).

The Government of Haiti should criminalize terrorist financing and take steps to implement the 2001 anti-money laundering law. In addition Haiti should take steps to ensure that the UCREF meets Egmont standards. Finally Haiti should take advantage, to the greatest extent possible of any training and technical assistance opportunities offered by the CFATF and/or the Caribbean Anti-Money Laundering Program (CALP).

Honduras. In 2002, there were major developments in the fight against money laundering in Honduras. Following two years of discussion, a new money laundering law was passed creating a Financial Intelligence Unit, expanding the definition of the crime of money laundering, and criminalizing the financing of terrorism.

Honduras is not an important regional financial center and is not considered to have a significant black market for smuggled goods. The vulnerabilities of Honduras to money laundering stem primarily from significant narcotics-trafficking throughout the region. In Honduras, money laundering takes place through the banking sector, and most likely in currency exchange houses, casinos, and front companies as well. Corruption remains a serious problem, particularly within the judiciary and law enforcement sectors.

Money Laundering and Financial Crimes

On February 28, 2002, the National Congress passed long-awaited legislation to widen the definition of money laundering and strengthen enforcement. Prior to the new law, the Honduran anti-money laundering program was based on Law No. 27-98 of December 1997. Law No. 27-98 criminalizes the laundering of narcotics-related proceeds, and introduced customer identification (no anonymous bank accounts were permitted), record keeping (five years) and transaction reporting requirements for financial institutions, including banks, currency exchange houses, money transmitters, and check sellers/cashiers. Financial institutions falling under Law No. 27-98 are required to record currency transactions over \$10,000 into dollar denominated accounts or 500,000 lempiras (\$29,400) in local currency accounts, and report all unusual and/or suspicious financial transactions to the National Banking and Insurance Commission. After analysis of these reports, the Commission forwards those it believes may be linked to narcotics-trafficking activities to the Public Ministry or to the General Prosecutor's Office. The law includes safe harbor provisions to protect financial institutions and their employees from civil and/or criminal liability when complying with such requirements. Per a January 2002 National Banking and Insurance Commission Resolution (No. 012/08-01-2002), the operation of offshore financial institutions is prohibited, but casinos remain unregulated.

Under the new legislation, Decree No. 45-2002, the previous law was expanded to define the crime of money laundering to include any non-economically justified sale or movement of assets, as well as asset transfers connected with trafficking of drugs, arms, and people, auto theft, kidnapping, bank and other forms of financial fraud, and terrorism. The penalty for money laundering is a prison sentence of 15-20 years. Public prosecutors and investigators are permitted to use electronic surveillance techniques to investigate money laundering, and they now have the ability to subpoena data and information directly from banks.

Decree No. 45-2002 also created a financial information unit, the Unidad de Información Financiera (UIF), within the Honduras National Banking and Securities Commission. The Unidad de Información Financiera receives between 2,600 to 2,700 reports per month of transactions over the designated thresholds. As of November 2002, the UIF was also receiving suspicious activity reports. A public prosecutor is assigned full-time to the Unidad de Información Financiera and public prosecutors, under urgent conditions and with special authorization, may subpoena data and information directly from financial institutions. Since passage of the law, the Financial Information Unit has begun investigating approximately 70 cases of possible money laundering activity.

The arrest of the Jimenez drug trafficking cartel in May 2001, on the north coast of Honduras revealed an extensive money laundering operation of both domestic and foreign illicit proceeds. Their operation revealed a variety of criminal activities including narcotics-trafficking, auto theft, kidnappings, bank fraud, smuggling, prostitution and corruption. The Government of Honduras (GOH) cooperates with U.S. investigations and requests for information pursuant to the 1988 UN Drug Convention. Honduras has signed Memoranda of Understanding to exchange information on money laundering investigations with Panama, El Salvador, Guatemala and Colombia. The GOH also adheres to Basel Committee's "Core Principles for Effective Banking Supervision." At the regional level, Honduras is a member of the Central American Council of Bank Superintendents, which meets periodically to exchange information.

The National Congress enacted an asset seizure law in 1993 that subsequent Honduran Supreme Court rulings have substantially weakened. The new money laundering legislation strengthens the asset seizure provisions of Honduran law. According to the law, officials in the Public Ministry will operate a warehouse for seized assets. The implementing regulations governing the operations of the warehouse are still under discussion. Since passage of the law and during the course of investigating cases of suspected money laundering, Honduran officials have frozen two bank accounts worth approximately \$250,000.

The GOH has been supportive of counter-terrorism efforts. The new law states that an asset transfer related to terrorism is a crime. This law does not explicitly grant the GOH the authority to freeze or seize terrorist assets; on separate authority, however, the National Banking and Insurance Commission has issued freeze orders promptly for the organizations and individuals named by the UN 1267 Sanctions

Committee and those organizations and individuals on the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 (on terrorist financing). The Commission reported that, to date, no accounts linked to the entities or individuals on the lists have been found in the Honduran financial system. 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, are frozen.

Honduran officials are investigating the suspected use of Honduran passports by terrorist networks, as well as allegations of terrorist-related money laundering activity in Honduras. Although the GOH has been working closely with the U.S. Embassy on allegations of terrorist assets in Honduras, the GOH has not yet established a counter-terrorism coordinator.

Honduras is a party to the 1988 UN Drug Convention and has signed, but has not yet ratified, the UN International Convention Against Transnational Organized Crime, which is not yet in force internationally. Honduras is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. In October 2002, Honduras became a member of the Caribbean Financial Action Task Force. The GOH has signed, but not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism and the OAS Inter-American Convention on Terrorism.

The GOH's new legislation has brought significant progress in anti-money laundering efforts. The Unidad de Información Financiera appears to meet many of the expectations for a newly established Financial Intelligence Unit, and Decree 45-2002 has advanced and expanded the criminalization of money laundering and related illicit activities. In the future, the GOH should continue to support and strengthen the developing UIF, and increase efforts to combat terrorist financing.

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 absence of currency and exchange controls facilitate financial activity but also make it vulnerable to money laundering. The primary sources of laundered funds are narcotics-trafficking (particularly heroin, methamphetamine, and ecstasy), tax evasion, fraud, illegal gambling and bookmaking, and illegal alien smuggling. Laundering channels include Hong Kong's banking system, and its legitimate and underground remittance and money transfer networks. Hong Kong is substantially in compliance with the Financial Action Task Force's (FATF) Forty Recommendations on Money Laundering and has developed a strong anti-money laundering regime, though improvements should be made. It is a regional leader in anti-money laundering efforts. The Hong Kong government concentrated its 2002 anti-financial crimes efforts on the passage of anti-terrorist financing legislation to fulfill the requirements of United Nations Security Council Resolution (UNSCR) 1373, and FATF's Special Recommendations on Terrorist Financing. As FATF president in the first half of 2002, Hong Kong played an important leadership role and worked energetically to build international support for effective measures to impede terrorist financing.

Money laundering is a criminal offense in Hong Kong under the Drug Trafficking (Recovery of Proceeds) Ordinance (DTRoP) and Organized and Serious Crimes Ordinance (OSCO). The money laundering offense extends to the proceeds of drug-related and other indictable crimes. Money laundering reporting requirements apply to all persons, including banks and non-bank 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). Financial regulatory authorities issue anti-money laundering guidelines to institutions under their purview and monitor compliance through on-site inspections and other means. 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. Hong Kong law provides that the filing of a suspicious transaction report shall not be regarded as a breach of any restrictions on the disclosure of information imposed by contract or law. Remittance agents and moneychangers must register their businesses with the police and keep

Money Laundering and Financial Crimes

customer identification and transaction records for cash transactions equal to or over \$2,564 (HKD 20,000). Hong Kong does not require reporting of the movement of currency above a threshold level across its borders or reporting of large currency transactions above a threshold level.

There is no distinction made in Hong Kong between onshore and offshore entities, including banks, and no differential treatment is provided for non-residents, 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 non-residents alike. The Hong Kong Monetary Authority (HKMA) regulates banks. The Insurance Authority and the Securities and Futures Commission regulate insurance and securities firms, respectively. All three impose licensing requirements and screen business applicants. Legally established casinos or Internet gambling sites do not exist 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 is a global leader in registering international business companies (IBCs), with nearly 500,000 registered in 2002. Many of the 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. However, solicitors and accountants have filed only a handful of suspicious transaction reports in recent years.

Under the DTRoP and OSCO, a court may issue a restraint order against a defendant's property at or near the time criminal proceedings are instituted. 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. At the end of 2002, approximately \$153 million was under restraint, \$13.5 million ordered to be confiscated, and \$57 million recovered by the government under DTRoP and OSCO. 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: no longer requiring actual notice to an absconded offender; requiring the court to fix a period of time in which a defendant is required to pay a confiscation judgment; permitting the court to issue a restraining order against assets upon the arrest (rather than charging) of a person; requiring the holder of property to produce documents and otherwise assist the government in assessing the value of the property; and creating an assumption 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. The government was unsuccessful in persuading the Hong Kong legislature to enact provisions aimed at improving the chances of obtaining successful prosecutions by reducing the evidentiary threshold for money laundering offenses and suspicious transaction reporting. Opposition to such provisions remains strong among the accounting and legal sectors, and also among legislators concerned that the lowered evidentiary threshold might lead to conviction of innocent persons.

As of the end of October 2002, the banking, securities, and insurance industries filed 8723, 44, and 62 suspicious transaction reports, respectively. The total number of reports in this 10-month period far exceeds the number for all of 2001, and can be attributed to the heightened attention to money laundering and terrorist financing in the aftermath of the September 11, 2001 events. From January through December 2002, there were 22 prosecutions and 12 convictions for money laundering offenses. In a notable case involving cooperation with the FBI and Canadian police, two money launderers pleaded guilty in September 2002 to a charge of laundering \$22 million. The Hong Kong government reported no particular increase in financial crimes during 2002, nor has it found evidence to indicate that narcotics proceeds are being used to fund smuggling activities.

In July 2002, Hong Kong's legislature passed the United Nations (Anti-Terrorism Measures) Ordinance that criminalizes the supply of funds to terrorists. This legislation was designed to bring Hong Kong into

compliance with UNSCR 1373 and FATF's Special Recommendations on Terrorist Financing. Hong Kong must still pass some additional subsidiary legislation, to be considered during the 2002-2003 legislative session, to implement fully certain provisions of this law. Among these are provisions that will set out the specific methods by which the government will be able to freeze terrorist funds.

Hong Kong's financial regulatory authorities have directed the institutions they supervise to conduct record searches for terrorist assets using U.S. Executive Order 13224 and United Nations lists. No terrorist assets have been found. The Hong Kong government intends to submit during the 2002-2003 legislative session new legislation to implement the UN International Convention for the Suppression of the Financing of Terrorism, which the People's Republic of China (PRC) has signed, but not yet ratified. The Hong Kong government will implement the "best practices" adopted by FATF at its October 2002 Plenary to prevent the misuse of charities and non-profit entities for terrorist financing.

At the October 2002 meeting of the Asia/Pacific Group on Money Laundering (APG), the Hong Kong delegation noted that underground banking and remittance agents remain major mechanisms through which criminals transfer proceeds of crimes across borders. Another major area of concern is the laundering of criminal proceeds by non-financial services professionals.

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 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 cooperates closely with foreign jurisdictions in combating money laundering. Hong Kong's mutual legal assistance agreements provide for the exchange of information for all serious crimes, including money laundering, and 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. It also has in force mutual legal assistance agreements with seven other jurisdictions: Australia, France, the United Kingdom, New Zealand, the Republic of Korea, Switzerland, and Canada. It has signed mutual legal assistance agreements with 5 other jurisdictions: Italy, the Philippines, Portugal, Ireland and the Netherlands.

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.

Hong Kong should strengthen its anti-money laundering regime by establishing threshold reporting requirements for currency transactions and putting into place "structuring" provisions to counter evasion efforts. Hong Kong should also establish cross-border currency reporting requirements and encourage more suspicious transactions reporting by lawyers and accountants, as well as business establishments, such as auto dealerships, real estate companies, and jewelry stores. Hong Kong should also take steps to thwart the use of "shell" companies, IBCs, and other mechanisms that conceal the beneficial ownership of accounts by more closely regulating corporate formation agents.

Hungary. Hungary has a pivotal location in Central Europe, with a well-developed financial services industry. Criminal organizations from Russia and other countries are entrenched in Hungary. The economy is heavily cash-based.

Money laundering related to all serious crimes is a criminal offense in Hungary. The cross-border movement of cash greater than one million forints (approximately \$4,000) must be declared to the customs authority, which immediately forwards it to Hungary's Financial Intelligence Unit, the Anti-

Money Laundering and Financial Crimes

Money Laundering Section (AMLS). Reporting and record keeping requirements, internal control procedures, and customer identification practices are required for a broad range of financial institutions. Banks, insurance companies, securities brokers and dealers, investment fund management companies, and currency exchange houses must file suspicious transaction reports (STRs). That requirement must now be met by other classes of professionals, including attorneys, antique dealers, casinos, tax consultants, real estate sales people, and accountants. Due diligence regarding the identification of beneficial owners must be exercised.

Hungary's financial regulatory body, the Hungarian Financial Supervisory Authority (PSzAF), oversees about 2,000 institutions. In 2002, PSzAF decided to increase oversight over the currency exchange sector by forcing money changers without an agreement with a commercial bank to cease operations on July 1, 2002. PSzAF supervises the financial sector, including compliance with anti-money laundering requirements. PSzAF has authority to conduct money laundering inspections and to impose sanctions upon noncompliant institutions. In the past two years, PSzAF has levied fines ranging from 100,000-3 million forints (\$400-13,000) on four occasions, and forced one bank to introduce compliance internal control systems. Most fines were due to deficiencies in customer identification and registration procedures, but in four cases criminal investigations were launched for failure to file STRs.

In June of 2001, the FATF placed Hungary on the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering, principally due to the existence of anonymous savings accounts and the lack of concrete plans for their elimination. In its accompanying report, the FATF also noted as a deficiency the fact that Hungarian financial institutions failed to collect information concerning the beneficial owners of accounts. The U.S. Treasury issued an advisory to all U.S. financial institutions instructing them to "give enhanced scrutiny" to all financial transactions involving Hungary. As a result of actions taken by Hungary in 2001 and 2002 to correct those deficiencies, FATF removed Hungary from the NCCT list and the U.S. advisory was lifted.

In November of 2001, the Hungarian Parliament approved Parliamentary Resolution 61/2001 (IX.24) on Hungary's contribution to Operation Infinite Justice, Parliamentary Resolution 62/2001 (IX.25) on foreign and security policy measures undertaken by Hungary following the terrorist attacks on the United States, and Bill No. T/5216 on counter-terrorism and money laundering. The latter was passed on November 27, 2001, and authorizes economic and other sanctions against countries, their commercial enterprises, and their citizens involved in terrorism. It also empowers the Government of Hungary (GOH) to immediately impose further restrictions on the basis of UN Security Council resolutions or positions held by the Council of Europe, and eliminates legal ambiguities concerning the search for and seizure of terrorist assets.

As of January 1, 2002, all anonymous passbook accounts were to be phased out. Now, savings deposits may only be placed or accepted on a registered basis by identifying both the depositor and the beneficiary. By September 2002, 80 percent of the funds that were deposited in passbook accounts were converted into identified deposits. The GOH concentrated on the accounts with the largest deposits during the first six months of 2002. After July 1, 2002, any conversion of anonymous passbooks holding more than 2 million forints (approximately \$8,800) was automatically forwarded to the AMLS. After December 31, 2004, conversion of any remaining accounts will need written permission from the AMLS.

Also, as of January 1, 2002, only credit institutions and their agents may be authorized by the PSzAF to offer currency exchange services, and as of January 2003, currency exchange activities will be licensed and supervised by the HFSA. Under new regulations, managers and employees of bureaux de change are subject to enhanced scrutiny, including a criminal background check. Some of this enhanced scrutiny will be conducted by the AMLS. In addition, the exchange services have to carry out a legally required identification procedure and to file an STR with AMLS for any currency exchange transaction meeting or exceeding 300,000 forints (approximately \$1,300). The bureaux also are required to have in operation video surveillance systems in their offices to record currency exchange activities.

In January 2002, the GOH created the Commission for Anti-Money Laundering Policy to better implement and coordinate efforts to improve Hungary's anti-money laundering regime. The Commission is particularly important with regard to combating terrorism, because of its ability to respond quickly and effectively to international requests to identify and freeze assets of terrorists.

In April 2002, Section 303 of the Penal Code on Money Laundering was amended to include the laundering of one's own proceeds, laundering through negligence, and conspiracy to commit money laundering, as punishable offenses. The GOH has also adopted a new Government Decree to further strengthen the AMLS and tighten anti-money laundering provisions.

A recent reorganization has placed the AMLS in the Directorate against Organized Crime—ORFK (SZBI). As a police unit, the AMLS also investigates cases. The AMLS has considerable authority to request and release information, nationally and internationally, related to money laundering investigations. Staffing at the AMLS has increased in the past year in order to be able to deal with the rapid increase in the number of STRs received by the expanded range of reporting institutions. AMLS staff members, along with PSzAF employees, are involved in training and raising awareness of employees within the obligated institutions, as well as of members of the general public.

The AMLS also carries out intelligence activity regarding terrorism financing, by way of receiving disclosures from institutions, information exchange with foreign counterparts, and examination and provision to relevant authorities of the lists of persons and organizations related to terrorism issued by the United States, the UN 1267 Sanctions Committee, and the EU Council. Thus far, no such accounts or transactions have been identified, but the GOH authorities state that they are prepared to freeze any such accounts in the future.

Hungary also established in 2000 a criminal investigation bureau within the Tax and Financial Inspection Service, to help spur tax and money laundering prosecutions. Based on information derived from STRs, the GOH has initiated five money laundering investigations in 2002, covering about five billion forints (approximately \$22 million). Two individuals were apprehended and arrested, and the GOH has issued warrants of arrest for others. Recent legislative changes, including one that clarifies that money laundering convictions can be obtained without conviction on the predicate offense, may well increase the number of money laundering prosecutions and convictions.

Hungary has an offshore market but prohibits offshore companies from providing financial and banking services. Hungary has licensed approximately 600 international business companies that are mainly owned by foreigners and enjoy a corporate tax rate of three percent as opposed to the usual rate of 18 percent.

Hungary is party to a Mutual Legal Assistance Treaty with the United States, and signed in January of 2000 a non-binding information-sharing arrangement with the United States, which is intended to enable U.S. and Hungarian law enforcement to work more closely to fight organized crime and illicit transnational activities. In furtherance of this goal, 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 similar cooperation arrangements with 22 other countries and has arrangements for the exchange of information related to money laundering with Austria, Slovakia, and Cyprus. The AMLS has been a member of the Egmont Group since 1998.

Hungary is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, formerly PC-R-EV) and underwent a mutual evaluation in 1998. Hungary is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Hungary became a party to the UN International Convention for the Suppression of the Financing of Terrorism in October 2002.

Hungary should criminalize terrorist financing. Hungary should also move forward to implement effectively its new legislation so that its anti-money laundering regime comports with international standards.

Iceland. Money laundering is not considered a major problem in Iceland. A money laundering law based on the Financial Action Task Force's (FATF) Forty Recommendations requires financial institutions to identify all customers and to report large deposits and suspicious transactions. Banks record the name of every customer who seeks to buy or sell foreign currency. All records necessary to reconstruct significant transactions are maintained for at least seven years. Employees of financial institutions are protected from civil or criminal liability for reporting suspicious transactions.

A 1997 amendment to the criminal code criminalizes money laundering regardless of the predicate offense, although the maximum penalty for money laundering is greater when it involves drug trafficking. The first successful prosecution under the money laundering law occurred in 2001.

Iceland is party to several multilateral conventions on terrorism and rules of territorial jurisdiction, including the 1977 European Convention on the Suppression of Terrorism. In October 2001, Iceland ratified the UN International Convention for the Suppression of Terrorist Bombings, and on April 15, 2002, ratified the UN International Convention for the Suppression of the Financing of Terrorism. The government formally enacted financial freeze orders against individuals and entities on the UNSCR 1267/1390 consolidated list of terrorists. The Parliament of Iceland passed comprehensive domestic legislation that specifically criminalizes terrorism and terrorist acts and requires the reporting of suspected terrorist-linked assets and transactions involving possible terrorist operations or organizations.

Iceland is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime of 1990. Iceland has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Iceland is a member of FATF, and its Financial Intelligence Unit is a member of the Egmont Group.

India. As a growing regional financial center, India is vulnerable to money laundering activities. Some common sources of illegal proceeds in India are narcotics-trafficking, trade in illegal gems, smuggling (including alien smuggling), corruption, and terrorism. Large portions of these illegal proceeds are laundered through the alternative remittance system called "hawala" or "hundi" (estimated to account for up to 30 percent of India's GNP). Under this system, individuals transfer funds or other items of value from one country to another, often without the actual movement of currency. The system provides anonymity and security; permits individuals to convert currency into other currencies; and lets them convert heroin, gold, or trade items into currency. All of this activity can be accomplished with little or no documentation. Historically, gold has been one of the most important instruments involved in Indian hawala transactions. There is a widespread cultural demand for gold in the region. In recent years, the Indian diamond trade has also been increasingly important in providing counter-valuation or a method of "balancing the books" in external hawala transactions. Invoice manipulation, for example, inaccurately reflecting the value of a good sold on the invoice, is also pervasive and is used extensively to both avoid Customs duties and taxes and launder illicit proceeds through trade-based money laundering. Income tax evasion is widespread in all sectors of the economy and is a direct component of the widespread use of hawala.

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 disproportionate 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 (NDPS) 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. However, punishment under NDPS is minimal and no cases have been prosecuted to date.

The Foreign Exchange Regulation Act (FERA) is one of India's primary tools for fighting money laundering. Its objectives include the establishment of controls over foreign exchange, the prevention of capital flight, and the maintenance of external solvency. Perversely, efforts to prevent capital flight and the

imposition of foreign exchange controls encourage the widespread use of hawala the GOI is trying to prevent. A closely related piece of legislation is the Conservation of Foreign Exchange and Prevention of Smuggling Act, which provides for preventive detention in smuggling and other matters relating to foreign exchange violations. The FERA, and its successor, the Foreign Exchange Management Act (FEMA), is enforced by the Enforcement Directorate (ED), which is part of India's Ministry of Finance; the ED is the organization most often involved in the investigation of hawala cases, as they often involve foreign exchange transactions.

The replacement for the FERA, the FEMA, was enacted in late 1999. This Act contains provisions facilitating continued financial liberalization in India in the area of foreign exchange. As under the FERA, the Reserve Bank of India (RBI), India's Central Bank, still plays an active role in the regulation and supervision of foreign exchange transactions, and hawala transactions continue to be illegal. During 2002, RBI became more receptive to anti-money laundering initiatives, especially those related to terrorist financing, and set up a special unit to provide anti-money laundering guidance to the Ministry of Finance. RBI recently worked with the police in the state of Kashmir to provide financial information in relation to a fraud case. Also in 2002, the Government of India (GOI) formed a high-level inter-ministerial group to coordinate all anti-money laundering and terrorist financing issues. The group includes representatives from the regulatory, law enforcement, and intelligence communities.

On November 27, 2002, the lower house of Parliament finally passed the Prevention of Money Laundering Bill, which had first been introduced in 1998. The bill was amended in August 2002 by the upper house to include terrorist financing provisions. The law was signed by India's President 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 creates a financial intelligence unit (FIU) that will be part of the Ministry of Finance.

There have been a number of informal actions taken by individual banking institutions to combat money laundering. Bank tellers and operators are encouraged to utilize the "know your customer" rule. 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 positive 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 the equivalent of \$10,000. Finally, banks have the authority to freeze assets in accounts when there is suspicious activity.

Until the GOI establishes the FIU provided for in its new legislation, the Central Economic Intelligence Unit (CEIB) will continue to serve as the GOI's lead organization for fighting financial crime. Also, the Central Bureau of Investigation is active in anti-money laundering efforts and hawala investigations. Other organizations such as the Directorate of Revenue Intelligence, Customs and Excise, the Reserve Bank of India, and the Finance Ministry are active in anti-money laundering efforts.

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 and include overseas companies, partnership firms, societies and other corporate bodies which are owned, directly or indirectly, to the extent of at least 60 percent by individuals of Indian nationality or origin resident outside India as also overseas trusts in which at least 60 percent of the beneficial interest is irrevocably held by such persons." OBUs must also be audited to affirm that ownership by a non-resident 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. Finally, OBUs must be audited, but the firm that does the auditing does not have to have government approval.

India is a party to the 1988 UN Drug Convention, and is a member of the Asia/Pacific Group on Money Laundering. In October 2001, India and the United States signed a mutual legal assistance treaty, which the U.S. Senate ratified in November 2002. India has also signed a police and security cooperation protocol with Turkey, which among other things provides for joint efforts to combat money laundering.

Money Laundering and Financial Crimes

India became a signatory to the UN International Convention for the Suppression of the Financing of Terrorism on September 8, 2000, but has not become a party to the Convention. The Government of India maintains tight controls over charities, which are required to register with the RBI. In April 2002, the Indian Parliament passed the Prevention of Terrorism Act, which criminalizes terrorist financing. However, terrorism financing in India, as well as the entire sub-continent, is directly linked to the use of hawala.

India should cooperate fully with international initiatives to provide increased transparency in hawala and, in particular, should increase law enforcement actions to counteract all forms of “black” hawala. Indian involvement in the underworld of the international diamond trade should be examined. India has indicated its interest in joining the FATF and the Egmont Group. Enactment of its anti-money laundering bill is a necessary first step in this direction. The task now is to implement the law effectively and to quickly set up the FIU in order to enhance information sharing with its counterparts around the world. Meaningful tax reform will also assist in negating the popularity of hawala and lessen money laundering. Increased enforcement action should also be taken to combat invoice manipulation and trade-based money laundering.

Indonesia. Indonesia. Although not a regional financial center, Indonesia has a financial system prone to money laundering: weak bank supervision, nascent anti-money laundering laws and regulations, lack of effective law enforcement, growing narcotics abuse and widespread corruption. Transparency International ranked Indonesia as the sixth most corrupt country of the 102 countries examined. Indonesia’s banking sector has not yet recovered from the Asian financial crisis of 1997-99 that led to a massive outflow of capital and a cascade of bank failures.

Most laundered money derives from non-drug criminal activity such as gambling, prostitution, bank fraud or corruption. Indonesia also has a long history of smuggling facilitated by thousands of miles of unpatrolled coastline and a law enforcement system riddled with corruption. The proceeds of these activities are then parked offshore and only repatriated as required for commercial and personal needs.

The Financial Action Task Force (FATF) included Indonesia in the list of Non-Cooperating Countries and Territories (NCCT) at its June 2001 plenary. The designation was based on: Indonesia’s lack of a basic set of anti-money laundering provisions; money laundering was not a criminal offense; there was no reporting of suspicious transactions to a Financial Intelligence Unit (FIU); and recently-introduced customer identification requirements only applied to banks. The U.S. Treasury Department issued an Advisory to all U.S. financial institutions instructing them to “give enhanced scrutiny” to all transactions involving Indonesia. FATF has set a deadline of February 2003 for Indonesia to make progress on identified areas or face the possibility of FATF recommending that its members impose countermeasures.

Until recently, banks and other financial institutions did not routinely question the source of funds or require identification of depositors or beneficial owners. Financial reporting requirements were put in place only in the wake of the financial crisis when the Government of Indonesia (GOI) was 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 of 2002 on Criminal Acts of Money Laundering, which made money laundering a criminal offense. The law identifies 15 predicate offenses related to money laundering, including narcotics-trafficking and most major crimes. The law provides for the establishment of a FIU, the Center for Reporting and Analysis of Financial Transactions (PPATK), to develop policy and regulations to combat money laundering. The PPATK will also collect and analyze data and financial reports to assist police and prosecutors on cases. The PPATK was established in December 2002 and expects to be fully functional by mid-2003.

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 100,000,000 (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.”

Separately, banks must report all foreign exchange transactions and foreign obligations to BI. Individuals who import or export more than Rp. 5 million (\$550) in cash must report such transactions to Customs. The import or export of more than Rp 10,000,000 (\$1,100) in cash requires permission from BI. However, BI imposed these requirements for balance of payments purposes, not for anti-money laundering enforcement, and it is not certain that such reports would be available to money laundering investigators. The PPATK is currently drafting presidential decrees that would protect reporting individuals and witnesses who cooperate with law enforcement entities on money laundering cases.

Indonesia has strong bank secrecy laws that prohibit banks from releasing information concerning depositors or their accounts except in specific and limited cases related to tax or criminal investigations. At the request of the Minister of Finance, BI may order banks, in writing, to provide information to tax authorities. In criminal cases, BI may give permission to police, prosecutors, or judges to obtain information from banks on an individual who has been named as a suspect or indicted; banks must comply. The Capital Markets Act 8/1995 imposes somewhat less strict secrecy requirements on securities and investment companies and empowers the Chairman of the Capital Market Supervisory Board to order the release of information in criminal cases. Under the Anti-Money Laundering (AML) Law, in cases of suspected money laundering, bank secrecy laws do not apply to the data collection and analysis functions of the PPATK or to police and prosecutor investigations.

Indonesia’s laws provide only limited authority to block or seize assets. Under BI regulations 2/19/PBI/2000, police, prosecutors or judges may order the seizure of assets of individuals or entities that have either been 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 would be required. In the case of money laundering as the suspected crime, however, bank secrecy laws would not apply according to the anti-money laundering law.

The October 18, 2002 emergency anti-terrorism regulations, the Government Regulations in Lieu of Law of the Republic of Indonesia No. 1 of 2002 on Eradication of Terrorism (Perpu), 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, which are known to be used partly or wholly for acts of terrorism. The AML Law focuses on “proceeds” gained from a list of crimes including narcotics, trafficking in persons, illegal arms sales, smuggling of goods, and terrorism among others. The AML Law criminalizes the laundering of proceeds of crimes, but it is unclear to what extent terrorism generates proceeds. Policy makers are currently drafting clarifying amendments.

The GOI has the authority to trace and freeze assets of individuals or entities designated by the UN 1267 Sanctions Committee, and has circulated the UN 1267 Sanctions Committee’s 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, and BI, takes several weeks from UN designation to bank notification. The GOI, to date, reports that it has not found any terrorist assets.

Money Laundering and Financial Crimes

The GOI has not taken into account alternative remittance systems or charitable or non-profit entities in its strategy to combat terrorist finance and money laundering. The PPATK, however, is working on draft regulations under the AML Law to cover the securities and insurance markets.

Indonesia is a member of the Asia/Pacific Group on Money Laundering. Indonesia is seeking membership in the Bank for International Settlements, and has established a working group to prepare for membership. This implies endorsement of the Basel Committee's "Core Principles for Effective Banking Supervision," that BI claims it follows voluntarily. 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, which is not yet in force internationally. Indonesia has signed, but not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

Indonesia does not have any bilateral agreements allowing for on-site examinations of foreign banks by home country supervisors, nor does it have specific agreements for international exchange of information on money laundering. However, BI asserts that, in principle, it would not object to on-site supervision by host country authorities and would deal with requests for exchange of information on money laundering cases on an ad-hoc basis, in accordance with existing criminal law. Bank secrecy laws may, however, hinder effective information exchange. The AML Law contains a specific provision (Article 44) authorizing bilateral and multilateral cooperation "in the context of an inquiry, investigations, or prosecution before a court of law."

The Indonesia National Police has cooperated with Australian Federal Police and FBI on the October 12, 2002 Bali Bombing Investigation and has subsequently expressed interest in future cooperative efforts.

The GOI should move aggressively to remedy the deficiencies identified in the FATF review process. In particular, it should lower the \$53,000 threshold at which funds are considered to be proceeds from a criminal act; expand customer identification and reporting requirements to additional types of entities, including non-bank financial institutions; and provide legislative protection for individuals who report suspicious transactions. The GOI should also lower the existing threshold of \$55,000 for currency transaction reporting. Additionally, the GOI should issue regulations to bolster its new anti-money laundering legislation, and should implement and enforce those new laws that comport with international standards.

Iran. The Department of State has designated Iran as a State Sponsor of Terrorism. Iran is not a regional financial center. The Minister of Economic Affairs and Finance submitted a bill governing money laundering countermeasures to the Iranian parliament in October 2002. The bill provides for the seizure and forfeiture of properties related to money laundering. A special Council composed of applicable ministers and the Governor of the Central Bank has also been formed to consider necessary powers for the Government of Iran (GOI) to fight economic crimes. On December 26, 2001, Bank Karafarin received a license from the Central Bank and became the first private bank to operate in Iran in 23 years.

Iran has a robust underground economy and the use of alternative remittance systems to launder money is widespread. The draft money laundering legislation is designed—in part—to help prevent underground economic activities. For example, Iran's real estate market is used to launder money. Real estate transactions take place in Iran, but often no funds change hands there; rather, payment is made overseas. This is typically done because of the difficulty in transferring funds out of Iran and the weakness of Iran's currency, the rial. The real estate market, in at least one instance, has been used to launder narcotics-related funds. Hawala is also used to transfer value to and from Iran. Factors contributing to the widespread use of hawala are currency exchange restrictions and the large number of Iranian expatriates. The smuggling of goods into Afghanistan from Iran is also involved with the barter trade for narcotics and trade-based money laundering. Goods purchased in Dubai are sent to the port of Bandar Abbas in Iran and then via land routes to other markets in Afghanistan and Pakistan. The goods imported into Iran and sent into Afghanistan are often part of the Afghan Transit Trade. However, many of these goods are eventually found on the regional black markets.

Iran is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. There is no law against terrorist financing.

Ireland. The primary sources of funds laundered in Ireland are derived from narcotics-trafficking, fraud and tax offenses. Money laundering occurs in financial institutions and the bureaux de change. Additionally, investigations in Ireland indicate that professionals continue to specialize in the creation of legal entities as a means of laundering money. Trusts are also established as a means of transferring funds from the country of origin to “offshore” locations. It is difficult to establish the true beneficiary of the funds, which makes it difficult to follow the money trail and establish a link between the funds and the criminal.

Money laundering relating to narcotics-trafficking and other offenses was criminalized in 1994. 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 and currency transactions exceeding approximately \$15,000, implement customer identification procedures, and retain records of financial transactions. Under certain circumstances, the High Court can order a freeze, and where appropriate, seize the proceeds of crimes. The exchange of information between police and the Revenue Commissioners, where criminal activity is suspected, is authorized.

The use of solicitors, accountants, and “company formation agencies” in Ireland to create “shell companies” has been cited in a number of “suspicious transaction reports,” and in requests for assistance from Financial Action Task Force (FATF) members. Investigations have disclosed that these companies are used to provide a series of transactions connected to money laundering, fraudulent activity, and tax offenses. The difficulties in establishing the “beneficial owner” have been complicated by the fact that the directors are usually nominees and are often principals of a solicitors’ firm or of a company formation agency.

In July 2001, the Government of Ireland (GOI) enacted the Company Law Enforcement Act 2001 (Company Act), to deal with problems associated with shell companies. This is the most important new companies act in more than 40 years. The legislation established the position of Director of Corporate Enforcement, whose responsibility it is to investigate and enforce the Company Act. The changes are directed at ensuring a greater measure of compliance, following the disclosure of major lapses in connection with a range of inquiries in recent years. Under the new law, the beneficial director of a company will have to be named. The Company Act will require all newly registered Irish companies to engage, in part, in business dealings within the State. It will also require that either the company’s director be a resident of Ireland, or the company must post a bond as a surety for failure to comply with the appropriate company law. The GOI is setting up a new multi-agency unit to enforce the law, and is in the process of recruiting personnel.

The GOI introduced new legislation targeting fundraisers for both international and domestic terrorist organizations. The “Suppression of the Financing of Terrorism” bill will extend the existing powers of the GOI to seize property and/or other financial interests belonging to convicted criminals and terrorists. The bill will allow the Garda Siochana (the national police) to apply to the courts to freeze large sums of cash where certain evidentiary requirements are met. In 2002, Irish authorities identified and froze the terrorist-related assets in several accounts.

A money laundering investigation concerning a bureau de change operation uncovered evidence of the laundering of terrorist funds derived from international smuggling. Substantial cash payments into the bureau de change were not reflected in the principal books, records, and bank account. The bureau de change held a large cash reserve that was drawn upon when necessary by members of the terrorist organization. The bureau de change would remit payments from its legitimate bank account to entities in other jurisdictions, on behalf of the terrorist organization.

Money Laundering and Financial Crimes

The Bureau of Fraud Investigation serves as Ireland's Financial Intelligence Unit. The Bureau analyzes financial disclosures and is a member of the Egmont Group. Ireland is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

The Suspicious Transaction Reports filed by financial institutions have increased over the past four years from 1,421 reports filed in 1999 to 3,725 filed in 2002 (through October 31). Investigations of money laundering cases have increased from 1,520 in 1999 to 4,170 in 2002 (through October 31). Convictions for money laundering offenses under the Criminal Justice Act totaled 7 in 1999, 10 in 2000, 4 in 2001 and 2 in 2002 (through October 31). A conviction on charges of money laundering carries a maximum penalty of 14 years' imprisonment and an unlimited fine.

Ireland's offshore banking is concentrated in Dublin's International Financial Services Centre (IFSC). Approximately 400 international financial institutions and companies operate in the IFSC. Services offered include fiscal management, re-insurance, fund administration and foreign exchange dealing. The Central Bank of Ireland regulates the IFSC companies.

In January of 2001, Ireland and the United States signed a Mutual Legal Assistance in Criminal Matters Treaty (MLAT); however, it is not yet in force. An extradition treaty between Ireland and the United States is already in force. Ireland is a member of the Council of Europe and FATF. Ireland is a signatory to the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Ireland has signed, but not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

Expedient implementation of Ireland's new anti-money laundering laws, and stringent enforcement of all such initiatives, will ensure that Ireland maintains an effective anti-money laundering program. The GOI should require that the beneficial owners of all shell companies licensed prior to the passage of the 2001 Company Law Enforcement Act be identified or disbanded.

Isle of Man. The Isle of Man (IOM) is a Crown Dependency of the United Kingdom located in the Irish Sea. Its large and sophisticated financial center is potentially very vulnerable to money laundering at the layering and integration stages.

As of June 30, 2002, the IOM's financial industry consists of approximately 17 life insurance companies; 22 insurance managers; more than 160 captive insurance companies; more than 14.7 billion pounds (approximately, \$24.1 billion) in life insurance funds under management; 59 licensed banks and two licensed building societies; 80 investment business license holders; 27.2 billion pounds (approximately, \$44.6 billion in bank deposits); and 128 collective investment schemes with 5.2 billion pounds (approximately, \$8.5 billion) of funds under management. There are also 124 licensed corporate service providers, with approximately another 65 seeking licenses.

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. 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 Financial Crime Unit (FCU) and the Isle of Man Customs and Excise.

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 such as banks, fund managers, stockbrokers, insurance companies, are required to report suspicious transactions. In addition, financial businesses such as lawyers, registered legal practitioners, accountants holding or handling clients' funds, corporate service providers, and trust service providers are obligated to know their customer.

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. Among other issues, the consultation paper proposes that every institution would have to check its whole book of business to determine that it has sufficient information available to prove customer identity.

An update to this consultation paper was issued in February 2002. It will be necessary to amend regulatory guidance to give effect to the Overriding Principles, and the consultation process to achieve this will commence early in 2003.

The IPA, as regulator of the IOM’s insurance and pensions business, also issues Anti-Money Laundering Standards for Insurance Businesses (the “Standards”), which are binding upon the industry and which include the Overriding Principles. The Overriding Principles have been revised in a manner suitable for their implementation by insurance companies. This includes, similarly, 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 February 1, 2002, and was amended to include wire transfers in June 2002. The insurance industry is currently working towards the implementation of a revised set of Standards, which must be fully operational by March 31, 2003.

The Criminal Justice Act, which was adopted/amended, in 2001 extends the power to freeze and confiscate assets to a wider range of crimes, increases the penalties for a breach of money laundering codes, and repeals the requirement for the Attorney General’s consent prior to disclosure of certain information. The law also addresses the disclosure of a suspicion of money laundering. It is now 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 IOM has also introduced the Customs and Excise (Amendment) Act 2001, which gives various law enforcement and statutory bodies within the Island 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 Island for the purposes of any criminal investigation and proceeding. Such exchanges can be either spontaneous or by request.

As a result of the terrorist events in the United States on September 11, 2001, the Government of the IOM drafted the Anti-Terrorism and Crime Bill 2002. The purpose of the bill is to enhance reporting, by making it an offense not to report suspicious transactions relating to money intended to finance terrorism. The IOM statute will become effective during 2003.

The IOM has also adopted (United Nations Measures) Order 2001, with the purpose of implementing UNSCR 1373, by providing for the freezing of terrorist funds, as well as creating a criminal offense with respect to facilitators of terrorism or its financing. 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.

Additionally, the Island has introduced the Online Gambling Regulation Act 2001 and an accompanying AML (Online Gambling) Code 2002. The Act and the Code are supplemented by regulations issued by the Gambling Control Commission, which provides more detailed guidance on the prevention of money laundering through the use of online gambling.

Suspicious transactions reports are reported to the FCU, which also has the role of being the IOM’s Financial Intelligence Unit (FIU).

In August 2002, new regulations were introduced that require money service businesses (MSBs), such as exchange bureaux and money transmitters, to register with Customs and Excise. The regulation has the

Money Laundering and Financial Crimes

effect of implementing the 1991 EU Directive on Money Laundering (Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering, as revised by Directive 2001/97/EC) in relation to MSB, and provides for supervision of them by Customs and Excise to ensure compliance with the AML Codes.

The IOM is a member of the Offshore Group of Banking Supervisors. 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. The IOM is also assisting FATF Working Groups considering matters relating to customer identification and companies' issues. The IOM is also a member of the International Association of Insurance Supervisors and the Offshore Group of Insurance Supervisors. The FIU belongs to the Egmont Group.

The IOM has developed a relatively comprehensive anti-money laundering program, and should continue its commitment to combating financial crime. IOM officials should continue to closely monitor its anti-money laundering program to assure its effectiveness, and IOM authorities should work with international anti-money laundering authorities to deter financial crime and the financing of terrorism and terrorists.

Israel. The Government of Israel (GOI) has made substantial progress enacting anti-money laundering legislation to support its efforts to strengthen its anti-money laundering regime, which resulted in the 2002 removal of Israel from the Financial Action Task's list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering.

Israel enacted the "Prohibition on Money Laundering Law" (PMLL), on August 8, 2000. The PMLL established a legal framework for an anti-money laundering system, but required the passage of several implementing regulations before the law could fully take effect. In November 2000, Israel enacted an implementing regulation called for by the PMLL. The "Prohibition on Money Laundering (Reporting to Police)" regulation established mechanisms for reporting to the police transactions involving property that was used to commit a crime or that represents the proceeds of crime.

Israel continued its efforts to reform its anti-money laundering system, and enacted additional implementing regulations provided for by the PMLL. The "Prohibition on Money Laundering (The Banking Corporations Requirement Regarding Identification, Reporting, and Record Keeping) Order" was approved in 2001. The Order establishes specific procedures for banks with respect to customer identification for account holders and beneficial owners, record keeping, and reporting of irregular and suspicious transactions reporting. The "Prohibition of Money Laundering (Methods of Reporting Funds when Entering or Leaving Israel) Order," also approved in 2001, requires individuals who enter or leave Israel with cash, bank checks, or traveler's checks above the equivalent of \$12,500 to report that information to customs authorities. Failure to comply is punishable by imprisonment of up to six months and a fine of approximately \$37,000 or ten times the amount not declared, whichever is greater. Additional regulations passed in 2001 addressed financial sanctions for covered institutions that fail to comply with their obligations under the PMLL, including requirements for customer identification, record keeping, and reporting of irregular transactions upon their respective financial sectors.

The PMLL criminalizes money laundering and notes more than 18 serious crimes as predicate offenses for money laundering. These specified unlawful activities for money laundering are in addition to offenses described in the Prevention of Terrorism Ordinance. The PMLL also authorized the issuance of regulations requiring financial service providers to identify, report, and keep records, for specified transactions for seven years. The law also provided for the development of a Financial Intelligence Unit.

Under the PMLL, money laundering offenses are punishable by up to ten-years' imprisonment and heavy fines. In 2002, the Government of Israel reported that there were 18 money laundering cases that had reached various stages of investigation and/or adjudication. Five cases yielded indictments; one case is under consideration by the district prosecutor; one case is completed; one case ended with the deportation of the suspect; and ten cases are in various stages of investigation. In 2002, the government seized

approximately \$19.1 million in illicit assets, of which approximately \$15 million were seized within the framework of money laundering cases.

In February 2002, Israel's FIU, the Israeli Money-laundering Prohibition Authority (IMPA), began operations. The IMPA has received over 100,000 currency transaction reports (CTRs) and 407 suspicious transaction reports (STR) since becoming operational. Banks, portfolio managers, stock exchange members, currency service providers, customs, the postal bank, insurance providers, and provident fund managers must file CTRs and STRs with the IMPA. IMPA develops intelligence cases that it passes on to the Israeli National Police, Customs, and the Israeli Security Agency for Criminal Investigation and Enforcement.

As noted above, FATF removed Israel from the NCCT list in June 2002. Israel's efforts to meet FATF's recommendations include establishing currency-reporting guidelines, creating an FIU, criminalizing money laundering associated with serious crimes, and improving Israel's ability to locate and freeze assets associated with terrorism. In June 2002, IMPA was admitted into the Egmont Group of Financial Intelligence Units. A U.S. advisory issued by the Department of Treasury's Financial Crimes Enforcement Network in June 2000 to U.S. financial institutions, emphasizing the need for enhanced scrutiny of certain transactions and banking relationships in Israel to ensure that appropriate measures are taken to minimize risk for money laundering, was withdrawn in 2002, acknowledging Israel's enactment and implementation of reforms in its counter-money laundering system.

Under the legal assistance law, Israeli courts are empowered to enforce forfeiture orders executed in foreign courts for crimes committed outside Israel. This ability has recently been enhanced by the new anti-money laundering law. Informally, the GOI has cooperated with requests from U.S. law enforcement in matters of financial crime, including those involving narcotics and terrorism. In 2002, Israeli and U.S. law enforcement cooperated as part of an "Operation Joint Venture," a long-term money laundering investigation focusing on an international Israeli network that launders cash proceeds from Colombian drug-trafficking organizations. The Israeli National Police have provided U.S. law enforcement with information on the network that has led to the arrest of six individuals, including two Colombian traffickers. The United States and Israel also have a Mutual Legal Assistance Treaty that entered into force in May of 1999. However, U.S. and foreign law enforcement continue to see Israeli subjects and involvement in a wide variety of money laundering operations.

Israel is a party to the 1988 UN Drug Convention, and has signed, but has not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism. Israel has also signed, but has not yet ratified, the UN International Convention Against Transnational Organized Crime, which is not yet in force internationally.

The Central Bank of Israel should accelerate the process by which it examines industry compliance with its anti-money laundering law, and ensure that financial institutions are moving quickly to fully verify customer identity for accounts opened before the law was enacted. In addition, the government should re-examine the relationship between IMPA and the police to determine ways to maximize interaction between the two agencies. Israel should continue to enact all regulations pursuant to the PMLL to strengthen its anti-money laundering regime. Israel should also focus on the misuse of the international Israeli diamond trade to launder funds.

Italy. Italy's financial sector remains vulnerable to money laundering. Italy is also a drug consumption country and a transshipment point for moving illicit narcotics into Western Europe. In 2002, Italian organized criminal groups—particularly those in the southern part of the country—continued to engage in narcotics and alien smuggling, contraband cigarette smuggling, extortion, usury, and kidnapping. Organized crime launders the proceeds of these activities through Italian banks, casinos, real estate, and the gold market. For example, Italian, Albanian, and Montenegrin criminal organizations form offshore companies to purchase bulk cigarettes that are marked for export, and smuggle them into Italy where they are sold tax-free throughout the European Union. This highly lucrative trade is made more attractive by relatively light penalties—a maximum of five years in prison.

Money Laundering and Financial Crimes

During 2002, Italian authorities uncovered cases of suspected money laundering involving securities brokers, online offerings of foreign exchange derivatives, the use of futures contracts, and the smuggling of diamonds, gold, and other precious metals.

Italian law criminalizes money laundering in connection with felony offenses punishable by imprisonment for 3 or more years. A wide range of financial institutions—including stock brokerages, exchange houses, and insurance companies—must identify their customers, record and report transactions above 10,300 euros (approximately \$10,526), and report suspicious transactions. In addition, institutions and individuals must report cross-border movements of currency that exceed 10,300 euros. Using the cross-border reports, the Anti-Mafia Directorate is conducting a retrospective analysis of irregular and suspect money flows from groups—especially those suspect of links to terrorism and 19 countries of concern. In particular, the Directorate is looking at the transfer of funds, incoming and outgoing, and their origins and destinations.

The Government of Italy (GOI) has established reliable systems for identifying, tracing, freezing, seizing, and confiscating assets from narcotics-trafficking and other serious crimes. The law allows for forfeiture in both civil and criminal cases. While the GOI enforces its existing asset seizure and forfeiture laws, the aggressiveness in doing so is dependent on which local magistrate is working a particular case. Unofficial figures indicate that the Financial Police seized the equivalent of \$465 million in assets from criminal groups during 2002. Approximately \$50 million was ultimately forfeited. Funds from asset forfeitures are placed into the General State Accounts. In accordance with the Council of Europe procedures, the GOI is committed to sharing these assets with cooperating countries.

Decree No. 153/97 designates the Ufficio Italiano dei Cambi (UIC), which is part of the Bank of Italy, to serve as the Italian Financial Intelligence Unit and to act as the recipient of suspicious transactions reports (STRs). The decree also provides a “safe harbor” provision for individuals who report suspicious transactions, and creates an inter-ministerial commission to coordinate anti-money laundering among Italian law enforcement and regulatory agencies. The decree also establishes organizational links among agencies that are involved in the fight against organized crime, and encourages international cooperation against money laundering.

The UIC is a member of the Egmont Group. The UIC receives and analyzes financial disclosures, and forwards them to the appropriate law enforcement agency—the Anti-Mafia Directorate, Carabinieri, Polizia di Stato, or the Guardia di Finanza—for further investigation when deemed necessary. The UIC also performs supervisory and regulatory functions such as issuing decrees, regulations, and circulars. To date, the UIC has memoranda of understanding with France, Spain, the Czech Republic, Croatia, Slovenia, and Australia. It is currently in negotiations with Japan and Switzerland.

Because of the banking controls, narcotics traffickers are using alternative way of laundering their drug proceeds. To prevent and deter the use of non-traditional entities for money laundering, GOI has enacted a decree which broadens the coverage of the anti-money laundering regulations. Those entities now covered include: debt collectors, exchange house, insurance companies, casinos, real estate agents, gold and valuables dealers and importers, and antiques dealers.

Italy is a member of the Financial Action Task Force (FATF). A member of the European Union, Italy is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Italy has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Italian cooperation with the United States on money laundering investigations is exemplary. Italy and the United States have a Customs Assistance Agreement and a Mutual Legal Assistance Treaty and an extradition treaty in place, which ensure the sharing of records relevant to narcotics-trafficking, money laundering, terrorism, and terrorist financing investigations. An effort to remove a reservation to the MLAT that would allow the U.S. and Italy to give forfeiture assistance has not yet taken effect. Currently, the U.S. must avail itself of relevant international conventions to obtain GOI assistance in forfeiture cases. Removing the reservation would also allow for a bilateral agreement to share forfeited assets. Italy also has

information sharing agreements with other countries for the exchange of information related to money laundering cases. The GOI also has a number of bilateral agreements with foreign governments in the area of investigative cooperation on drug trafficking and organized crime. GOI is involved in multilateral negotiations with the EU to enhance asset tracing and seizure.

On January 13, 2000, Italy signed the UN International Convention for the Suppression of the Financing of Terrorism and the Italian Parliament ratified the Convention in December 2002. In October 2001, Italy passed a Decree that created the Inter Ministerial Financial Security Committee, which is charged with coordinating GOI efforts to track and interdict terrorist financing. The Committee has far reaching powers that include obtaining information from all government ministries in waiver of the Official Secrecy Act and the authority to order a freeze of terrorist-related assets. Another decree issued in October 2001 criminalized the financing of terrorist activity with a penalty of imprisonment of seven to fifteen years. Decree Law No. 12/2002 extends the suspicious transaction reporting requirement to cover terrorist financing. Entities subject to the reporting requirement must also inform UIC of any freezing measures they take with regard to accounts suspected of being linked to terrorist entities. They must also make available to UIC all financial information they possess relating to any person or organization on UN or other terrorist lists. During 2002, UIC, in conjunction with the Italian judiciary, initiated a number of proceedings and investigations into suspected terrorist activities. In most cases, prosecutors have authorized UIC to disclose to foreign FIUs information they have uncovered in the course of these investigations. In August 2002, the GOI acted jointly with the U.S. Government to block the financial assets of 25 individuals or groups allegedly associated with Usama Bin Ladin's network.

Although the GOI has comprehensive internal auditing and training requirements for its financial sector, implementation of these measures by non-bank financial institutions still lags behind that of banks, as evidenced by the relatively low number of STRs that have been filed by non-bank financial institutions. The GOI should increase its training efforts and supervision in the area of non-bank financial institutions to decrease their vulnerability to money laundering.

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. Traffickers seek to legitimize the profits from these illegal drug flows, and Jamaica is therefore a prime candidate for money laundering activities, although it is difficult to estimate the extent of money laundering that occurs in the country. Jamaica's banking system, however, has been under intense scrutiny from regulators in the wake of several major banking scandals in the mid- to late-1990s, making Jamaican financial instruments an unattractive mechanism for laundering money. As a result, much of the proceeds from narcotics-trafficking and other criminal activity is used to acquire tangible assets such as real estate or luxury cars, while still more merely passes through Jamaica as cash shipments to South American countries.

The GOJ does not yet require declarations of cross-border movements of currency or monetary instruments. Criminals exploit this weakness and move large amounts of cash through Jamaica—often in shipments totaling hundreds of thousands of U.S. dollars. Even when cash couriers are caught, the absence of a currency declaration requirement hampers police efforts to bring criminal charges against the couriers. Further complicating the picture are the hundreds of millions of U.S. dollars in legitimate remittances sent home to Jamaica by the substantial Jamaican population overseas. Distinguishing between legal transfers and illegal flows is no easy task.

Jamaica's anti-money laundering regime is governed by the Money Laundering Act (MLA) approved by Parliament in December 1996 and implemented on January 5, 1998. The MLA criminalized narcotics-related money laundering and introduced record keeping and reporting requirements for financial institutions on all currency transactions over \$10,000. Exchange bureaus and "cambios" have a reporting threshold of \$8,000. The MLA was amended in March 1999 to raise the threshold to \$50,000, in response to complaints from financial sector institutions that had difficulties with the amount of paperwork resulting from the \$10,000 threshold. At that time, a requirement was also added for banks to report

Money Laundering and Financial Crimes

suspicious transactions of any amount to the Director of Public Prosecutions (DPP). In February 2000, the MLA was amended to add fraud, firearms trafficking, and corruption as predicate offenses for money laundering. The most recent legislative update, in February 2002, imposed a requirement for money transfer and remittance agencies to report transactions over \$50,000.

The Government of Jamaica (GOJ) established a Financial Crimes Division under the DPP to assist in the implementation of its anti-money laundering program. This unit is responsible for receiving and analyzing information contained in suspicious activity reports filed by financial institutions. The unit officially began operations in June 2001. No major cases of money laundering arrests or prosecutions were reported in 2002, although the Financial Crimes Division investigated a number of reports.

Further action is required in the area of asset forfeiture to permit the GOJ to take full advantage of this mechanism in its anti-money laundering efforts. Law enforcement authorities are hampered by the fact that Jamaica has no civil forfeiture law, and under the 1994 Drug Offenses (Forfeiture of Proceeds) Act, a criminal drug-trafficking conviction is required as a prerequisite 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. In at least one case in 2002, however, the GOJ creatively used income tax regulations to levy fines and penalties that resulted in the de facto forfeiture of a large amount of cash being smuggled out of the country.

With regard to anti-terrorism financing, Jamaica has not yet developed its final legislative response, although a comprehensive Anti-Terrorism Act is currently under consideration, with passage expected in 2003. As an interim measure, the Bank of Jamaica requires the banking industry to adopt the "Guidance Notes for Financial Institutions in Detecting Terrorist Financing" issued by the Financial Action Task Force (FATF) in April 2002.

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 Organization of American States (OAS) Inter-American Convention Against Corruption. Jamaica has signed, but not yet ratified the UN Convention Against Transnational Organized Crime which is not yet in force internationally. Jamaica is also a member of the Caribbean Financial Action Task Force and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering.

The GOJ has made progress in fighting money laundering, but further work is necessary to bring its regime into line with international standards. The GOJ should institute measures implementing the FATF's Eight Special Recommendations on Terrorist Financing. Jamaica should enact legislation requiring declarations of large cross-border movements of currency in order to address the problem of cash couriers, as well as accompanying legislation allowing for asset seizure. The scope of predicate offenses for money laundering should be extended to encompass all serious crimes (legislation doing so has been proposed but not yet enacted) and serious thought should be given to returning the reporting threshold to \$10,000 as originally mandated. The GOJ should also ensure that the Financial Crimes Division has sufficient resources to identify and investigate money laundering activity adequately.

Japan. Japan is an important world financial center, and as such is at major risk for money laundering. The principal sources of laundered funds are narcotics-trafficking and financial crimes (illicit gambling, extortion, abuse of legitimate corporate activities, and all types of property related crimes) as well as the proceeds from violent crimes, mostly linked to Japan's criminal organizations, e.g., the Boryokudan. The National Policy Agency of Japan estimates the aggregate annual income from the Boryokudan's illegal activities is estimated to be approximately \$10 billion, \$3.38 billion of which is derived from income from the trafficking of methamphetamines. U.S. law enforcement reports that drug-related money laundering investigations initiated in the United States periodically show a link between drug-related money laundering activities in the United States and bank accounts in Japan. The number of Internet-related money laundering cases is increasing. In some cases, criminal proceeds were concealed in bank accounts obtained through the Internet market.

Prior to 1999, Japanese law only criminalized narcotics-related money laundering. The Anti-Drug Special Law, which took effect in July 1992, criminalizes drug-related money laundering, mandates suspicious transaction reports for the illicit proceeds of drug offenses, and authorizes controlled drug deliveries. This 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 limited scope of the law and the burden required of law enforcement to prove a direct link between money and assets to specific drug activity severely 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 the Boryokudan have been exploiting Japan's financial institutions.

Pursuant to the 1999 Anti-Organized Crime Law, which came into effect in February 2000, Japan expanded its money laundering law beyond narcotics-trafficking to include money laundering predicates such as murder, aggravated assault, extortion, theft, fraud, and kidnapping. The new law also extends the confiscation laws to include the 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.

To facilitate exchange of information related to suspected money laundering activity, the Anti-Organized Crime Law established the Japan Financial Intelligence Office (JAFIO) on February 1, 2000, as Japan's Financial Intelligence Unit. Financial institutions in Japan report suspicious transactions to the JAFIO, which analyzes them and disseminates them as appropriate. JAFIO also issued "Examples of Typical Suspicious Transactions" as a guideline for financial institutions. The guideline was revised in March 2002 to add more specific suspicious transaction cases, such as transactions done by Boryokudan and their associates. Additionally, JAFIO held meetings with financial institutions in various regions in March and April 2002 to introduce current money laundering methods and trends, with the intent of improving the quality of suspicious transaction reports.

The Financial Services Agency (FSA) supervises public-sector financial institutions and 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. Under the 1998 Foreign Exchange and Foreign Trade Control Law, banks and other financial institutions had to report transfers abroad of five million yen (approximately \$44,579) or more. In April 2002, Parliament enacted the Law on Customer Identification and Retention of Records on Transactions with Customers by Financial Institutions, and revised the Foreign Exchange and Foreign Trade Law, so that financial institutions, as of January 2003, are required to make positive customer identification for both domestic transactions and transfers abroad in amounts of more than two million yen (approximately \$17,828.) Banks and financial institutions are also required to maintain records for an adequate period of time should they be needed to reconstruct significant transactions.

Japanese financial institutions have cooperated, when requested, with law enforcement agencies, including U.S. and other foreign government agencies investigating financial crimes related to narcotics. Japan has not adopted "due diligence" or "banker negligence" laws that make individual bankers responsible if their institutions launder money, but there are administrative guidelines in existence that require due diligence. The law does, however, protect bankers and other financial institution employees who cooperate with law enforcement entities.

The 1998 Foreign Exchange and Foreign Trade Control 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 \$8,916), or its equivalent in foreign

Money Laundering and Financial Crimes

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 \$1,782) or six months imprisonment. However, the reporting requirement is enforced only sporadically.

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 to both stem from criminal proceeds, and to be linked to individuals and/or entities designated by FSA Notices as suspected to have relations with terrorist activities. In June 2002, the Act on Punishment of Financing of Offenses of Public Intimidation, which adds terrorist financing to the list of predicate offenses for money laundering and provides for the freezing of terrorism-related assets, was enacted. Japan signed the UN International Convention on the Suppression of the Financing of Terrorism on October 30, 2001, and accepted it on June 11, 2002. After September 11, 2001, Japan froze accounts related to the Taliban. Since then, Japan has regularly frozen assets and accounts linked to terrorists listed by the UN and others. There are indications that Japan is considering new legislation to upgrade its antiterrorism law to enhance the government's ability to freeze and confiscate assets of terrorist organizations.

Underground banking systems operate widely, especially in immigrant communities. Such systems violate the Banking Law and the Foreign Exchange Law. The police have investigated 35 underground banking cases in which foreign groups transferred illicit proceeds to foreign countries. The aggregate value of such transfers has amounted to 420 billion yen (approximately \$3.5 billion) since the beginning of 1992. About 120 billion yen (\$1 billion) have been illegally transferred to China and Korea, and about 90 billion yen (\$750 million) to Peru.

Japan has not enacted laws that allow for sharing of seized narcotics assets with other countries. However, the Japanese Government 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. In December 2000, Japan signed, but has not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Japan is a member of the Financial Action Task Force. The JAFIO joined the Egmont Group of FIUs in 2000. Japan is also a member of the Asia/Pacific Group on Money Laundering. Efforts are now underway to conclude a Mutual Legal Assistance Treaty between Japan and the United States. In 2002, Japan's FSA and the U.S. Securities and Exchange Commission and Commodity Futures Trading Commission signed a non-binding Statement of Intent ("SOI") concerning cooperation and the exchange of information related to securities law violations. The SOI assists in the investigation and prosecution of securities and futures fraud, predicate offenses to money laundering.

Japan has many legal tools and agencies in place to successfully detect, investigate, and combat money laundering. In order to strengthen its anti-money laundering regime, the Government of Japan should stringently enforce the Anti-Organized Crime Law. Japan should enact penalties for non-compliance with the Foreign Exchange and Foreign Trade Law, adopt measures to share seized assets with foreign governments, and enact banker "due diligence" provisions.

Jersey. The Bailiwick of Jersey (BOJ), one of the Channel Islands, is a Crown Dependency of the United Kingdom. The Islands are known as Crown Dependencies because the United Kingdom is responsible for their defense and international relations. Jersey's sophisticated offshore services industry is similar to international financial services centers worldwide. A number of reports and surveys have shown its anti-money laundering and regulatory regimes to be close to international standards.

The financial services industry, regulated by the Jersey Financial Services Commission (FSC), consists largely of bank deposits of \$170 billion; mutual funds of \$150 billion, insurance companies (which are largely captive insurance companies), investment advice, dealing, and management companies (\$50 billion under management), and trust and company administration companies. In addition, the above offer

corporate services, such as special purpose vehicles for debt restructuring and employee share ownership schemes. For high net worth individuals, it offers wealth management services.

Jersey's main anti-money laundering laws are: the Drug Trafficking Offenses (Jersey) Law of 1988, which criminalizes money laundering related to narcotics-trafficking; the Prevention of Terrorism (Jersey) Law, 1996, which criminalizes money laundering related to terrorist activity; and the Proceeds of Crime (Jersey) Law, 1999, which extended the predicate offenses for money laundering to all offenses punishable by at least one year in prison. A new law, the Terrorism (Jersey) Law 2002, is a response to the events of September 11, 2001, and enhances the powers of the insular authorities to investigate terrorist offenses, to cooperate with law enforcement agencies in other jurisdictions, and to seize assets. The Law was adopted by the Island Parliament and awaits Royal Assent.

The FSC has issued anti-money laundering Guidance Notes that the courts take into account when considering whether or not an offense has been committed under the Money Laundering Order. The reporting of suspicious transactions is mandatory under the narcotics-trafficking, terrorism and anti-money laundering laws.

After consultation with the financial services industry, the FSC issued a position paper (jointly issued in Guernsey and the Isle of Man) that set out a number of proposals for tightening further the essential due diligence requirements that financial institutions should meet regarding their customers. The position paper states the FSC's intention to insist, *inter alia*, on affirming the primary responsibility of all financial institutions to verify the identity of their customers, regardless of the action of intermediaries. The paper also states an intention to require a progressive program to obtain verification documentation for customer relationships established before the Proceeds of Crime (Jersey) Law came into force in 1999. New Anti-Money Laundering Guidance Notes are currently being drafted that will incorporate these principles and replace those described above. These Notes are likely to come into force in 2003.

Approximately 30,000 Jersey companies are registered with the Registrar of Companies, who is the Director General of the FSC. In addition to public filing requirements relating to shareholders, the FSC requires details of the ultimate individual beneficial owner of each Jersey registered company to be filed, in confidence, with the Commission. That information is available, under appropriate circumstances and in accordance with the law, to U.S. and other investigators. In addition, a number of companies that are registered in other jurisdictions are administered in Jersey. Some companies, known as "exempt companies," do not have to pay Jersey income tax and are only available to non-residents. Jersey does not provide "offshore" licenses. All regulated individuals are equally entitled to sell their services to residents and non-residents alike. All financial businesses must have a "real presence" in Jersey, and management must be in Jersey.

Jersey has extensive powers to cooperate with other law enforcement and regulatory agencies and regularly does so. The FSC is also able to cooperate with regulatory authorities, for example, to ensure that financial institutions meet anti-money laundering obligations. Recently, the FSC has reached agreements on information exchange with securities regulators in Germany (July 2001), France (November 2001), and the United States (May 2002). The 1988 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 authorities have also put in place sanction orders freezing accounts of individuals connected with terrorist activity.

Jersey has established a financial investigation unit known as the Joint Financial Crime Unit (JFCU). This unit is responsible for receiving, investigating, and disseminating suspicious transaction reports (STRs). The unit includes Jersey Police and Customs officers, as well as a financial crime analyst. The JFCU is a member of the Egmont Group.

Jersey plans to put in place the necessary legislation to be in compliance with the UN International Convention for the Suppression of the Financing of Terrorism as soon as the Terrorism (Jersey) Law 2002 receives approval by the Privy Council. This will enable Jersey to try individuals for terrorist crimes,

Money Laundering and Financial Crimes

notably, including the financing of terrorism committed outside Jersey. Application of the 1988 UN Drug Convention was extended to Jersey on July 7, 1997.

Jersey has established an anti-money laundering program, and should continue to demonstrate its commitment to fighting financial crime. In some instances, Jersey's requirements, such as the regulation of trust company businesses and the requirement for companies to file beneficial ownership with the FSC, go beyond what international standards require, in order to directly address Jersey's particular vulnerabilities to money laundering.

Jordan. Jordan is not a regional financial center. The Central Bank of Jordan, which regulates foreign exchange transactions, issued anti-money laundering regulations designed to meet the FATF 40 Recommendations on Money Laundering in August 2001. Under Jordanian law, money laundering is considered an "unlawful activity" subject to criminal prosecution.

Revisions to the penal code subsequent to the September 11, 2001 attacks on the United States have also criminalized financing of terrorist organizations. Jordan has signed, but not yet ratified, the International Convention for the Suppression of Financing of Terrorism. Jordan has complied with its obligations under UNSCR 1267/1390 by reviewing assets of terrorists and terrorist groups identified at the United Nations 1267 Sanctions Committee, although no such assets have been identified in Jordan to date.

Jordanian officials report that financial institutions file suspicious transactions reports and cooperate with prosecutors' requests for information related to narcotics-trafficking cases. Jordan's Central Bank has instructed financial institutions to be particularly careful when handling foreign currency transactions, especially if the amounts involved are large or if the source of funds is in question. The Banking Law of 2000 waives banking secrecy provisions in cases of suspected money laundering.

Jordan is a party to the 1988 UN Drug Convention. Jordan has taken steps in constructing an anti-money laundering program, but much remains to be done. Jordan should consider establishing a Financial Intelligence Unit (FIU) that can analyze and disseminate suspicious transaction reports to law enforcement agencies. Additional training of Jordanian customs and police services may be required to identify money laundering methodologies and initiate investigations.

Kazakhstan. Kazakhstan has a somewhat advanced financial infrastructure in comparison to other countries in the region. When combined with a significant organized crime presence, entrenched smuggling networks, and corruption involving the oil industry, the country is at risk for money laundering. Smuggling of cash is an ongoing problem in Kazakhstan. Although travelers are required to report the amount of cash they are carrying as they enter or exit the country, porous borders and corrupt officials allow a large amount of cash to pass undetected. Most of the smuggled cash is probably related to illegal capital flight, but there are reports that Kazakhstan has become a transport route for cash and trade items moving into Afghanistan to finance terrorist organizations.

Money laundering was criminalized in Kazakhstan by Article 30 of the 1998 anti-drug law, which makes it illegal to launder money in connection with the sale of illegal drugs. However, the definition of money laundering used in the act is narrow. A further limit to the effectiveness of the law is that bank records may not be examined until after a criminal case has been initiated. The Government of Kazakhstan (GOK) is reportedly aware of the problems with the policing of financial crimes, including money laundering, and is taking corrective measures. In January 2002, the Tax Committee was replaced by the Financial Police Agency, which has authority to investigate money laundering and other financial crimes. In March 2002, the Financial Police reported that in the previous year they had presented for prosecution 31 cases of money laundering, none of which were associated with narcotics-trafficking.

The National Bank has established a "know your customer" program and has asked local banks to report suspicious financial activities. Perhaps as a result, there are reports that large amounts of money seem to be moving into less regulated parts of the economy. As of January 2003, both the Financial Police and the National Bank are sponsoring different drafts of anti-money laundering legislation with the goal of passing an effective anti-money laundering law in 2003.

Kazakhstan should pass comprehensive anti-money laundering and counter-terrorist financing laws.

Kenya. Kenya is a regional financial and trade center for East, Central, and Southern Africa. Kenya's capital, Nairobi, has approximately 50 banks. Kenya's economy has a large informal sector and a thriving network of cash-based, unrecorded transfers, primarily used by expatriates to send and receive remittances internationally.

Section 49 of the Narcotic Drugs and Psychotropic Substance Control Act of 1994 criminalizes money laundering related to narcotics-trafficking. Narcotics-related money laundering is punishable by a maximum prison sentence of 14 years. Central Bank regulations require banks to verify the identity of customers wishing to open an account or conduct a transaction. Under the regulations, banks must maintain records of large transactions. Banks and other financial institutions are required to report large transactions to the Central Bank.

In 2002, the Kenya Bankers Association issued guidelines requiring banks to report suspicious transactions to the Central Bank. These guidelines do not have the force of law.

The Government of Kenya (GOK) has drafted, but not yet passed, legislation that would criminalize terrorist financing. The GOK has also drafted legislation that would criminalize money laundering beyond the scope of narcotics-trafficking, establish a Financial Intelligence Unit, and allow for the seizure of assets belonging to terrorist financiers and members of organized criminal groups. Currently, only the proceeds of narcotics-trafficking are subject to seizure.

Kenya is a party to the 1988 UN Drug Convention and a signatory to the UN International Convention for the Suppression of the Financing of Terrorism. Kenya is an active member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body.

Kenya should enact a comprehensive anti-money laundering regime that criminalizes terrorist financing and money laundering related to all serious crimes, as Kenya has committed to doing as a member of ESAAMLG.

Korea (Democratic Peoples Republic of Korea). The Department of State has designated North Korea as a State Sponsor of Terrorism. Information about the money laundering situation in North Korea is generally unavailable. North Korea's self-imposed isolationism and secrecy as well as its refusal to participate in international organizations make knowledge of the role of North Korea's financial system and drug trafficking situation supposition at best.

What little is known and documented, however, includes North Korea's continued use of Macau as a base of operations for money laundering and other illicit activities. Macau is a useful intermediary, for it provides North Koreans with access to global financial systems. There are reports that Pyongyang also has used Macau to launder counterfeit \$100 bills and Macau's banks as a repository for the proceeds of North Korea's growing trade in illegal drugs.

North Korea has signed, but not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

North Korea should enact a comprehensive anti-money laundering regime and take steps to stop financial crimes originating in North Korea.

Korea (Republic of Korea). 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 persons engaged in financial institutions, apart from judicial requests for information, not 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.

Money Laundering and Financial Crimes

In a move designed to broaden its anti-money laundering regime, the Republic of Korea (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.

The Financial Transactions Reports Act (FTRA), passed in September 2001, requires financial institutions to report suspicious transactions to a Financial Intelligence Unit (FIU) within the Ministry of Finance and Economy. In November 2001 the Korean Cabinet issued regulations implementing the newly enacted FTRA, and officially launched the Korea Financial Intelligence Unit (KoFIU). KoFIU 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 domestic law enforcement and the Public Prosecutor's office. Financial institutions must report transactions of over 50 million won (\$10,000) that are suspected of being tied to criminal proceeds or to tax evasion. They may report transactions in lesser amounts if there are "reasonable" grounds for doing so. Improper disclosure of financial reports is punishable by up to five years imprisonment and a fine of up to 30 million won (approximately \$25,000). In addition, KoFIU supervises and inspects the implementation of internal reporting systems established by financial institutions.

As of December 31, 2002, KoFIU received a total of 275 STRs from financial institutions. KoFIU completed its analysis of 206 cases, amounting to KRW 96 billion, that were then disseminated to law enforcement agencies, including the public prosecutor's office, the National Police Agency, the National Tax Service, the Korea Customs Service and the Financial Supervisory Service. FIU is still investigating another 69 STRs. Last November, one businessman was prosecuted for laundering a total of 24 billion Korean won (approximately \$22 million) through 634 checks.

Money laundering controls are applied to non-banking financial institutions, such as exchange houses, stock brokerages, casinos, insurance companies, merchant banks, mutual savings, finance companies, credit unions, credit cooperatives, trust companies, securities companies, insurance companies, credit insurance corporations and exchange houses. Intermediaries such as lawyers, accountants, or broker/dealers are not covered. 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.

The Anti-Public Corruption Forfeiture Act of 1994 provides for the forfeiture of the proceeds of assets derived from corruption. In November 2001, the ROK 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 Seoul District Prosecutor's office seized \$109,000 worth of assets related to illegal foreign exchange transactions in the one case it prosecuted. Drug trafficking-related assets worth \$53,000 of assets were forfeited during 2002. The ROK actively cooperates with the United States and other countries to trace or seize assets.

As of today South Korea does not have any specific laws regarding terrorist financing per se. An Anti-Terrorism Act is pending before the National Assembly. Should this Act be passed, it will include articles that specifically criminalize terrorist financing. The Supreme Prosecutors' Offices look at black market exchanges and the Korea Customs Service monitors trade-based money laundering in an effort to prevent and/or curb such activities. As of this date, no additional legislative initiatives are pending. Reportedly, at this time are no known charitable or non-profit entities operating in Korea that are used as conduits for

the financing of terrorism, although the Korean government's own efforts to monitor and prevent illegal financial transfers overseas would also inhibit these entities from operating freely.

Through its Korean Financial Investigative Unit (authorized by the Ministry of Finance and Economy) the ROK circulated to its financial institutions the list of individuals and entities that have been included in the UN 1267 Sanctions Committee's consolidated list as being linked to Usama Bin Ladin, members of the al-Qaida organization or the Taliban, or that the USG or the EU have designated under relevant authorities. Due in part to Korea's remaining restrictive foreign exchange laws, no listed terrorists are known to be operating in Korea at this time or to be maintaining financial accounts. Consequently, Korean banks have not identified any terrorist assets.

The ROK 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, which is not yet in force internationally. In October 2001, the ROK signed the UN International Convention for Suppression of the Financing of Terrorism. The ROK is an active member of the Asia/Pacific Group on Money Laundering. The ROK became a member of the Egmont Group in 2002 and applied for membership in the Financial Action Task Force. 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 2002, the ROK signed information-sharing memorandums of understanding with the Belgian, Polish and U.K. FIUs. Also in 2002, the ROK proposed signing an MOU with the U.S. Financial Crime Enforcement Network, the U.S. FIU, for the exchange of money laundering-related information. The ROK is awaiting a response.

The passage of the new measures provides the ROK with important legal tools to combat money laundering. Korea should criminalize the financing and support of terrorism and should continue to move forward to adopt and implement its pending legislation. The ROK should extend its anti-money laundering regime to financial intermediaries. The ROK should continue its policy of active participation in international anti-money laundering efforts, both bilaterally and in multilateral fora.

Kuwait. Kuwait is not a major regional financial sector; it has seven commercial banks and one Islamic bank, all of which provide traditional banking services comparable to those of Western-style commercial banks. Kuwait also has three specialized government banks that provide medium and long-term financing.

On March 10, 2002, the Emir signed Law No. 35, which criminalizes money laundering. The law stipulates that banks and financial institutions may not keep or open any anonymous accounts or accounts in fictitious or symbolic names; banks must require proper identification of regular and occasional clients according to official documents issued by competent state authorities. The law also requires banks to keep all records of transactions and customer identification information for a minimum of five years, perform training and establish internal control systems, and report any suspicious transactions.

Law 35 designates the Public Prosecution Department as the sole authority to receive reports on money laundering operations, and to take the necessary actions. The 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. The law includes articles on international cooperation, and monitoring cash and precious metals transactions. Provisions of Article 4 of Law No. 35 state that every person shall, upon entering the country, inform the custom authorities of any national or foreign currency, gold bullion, or any other precious materials in his/her possession valued in excess of Kuwait Dinars 3,000 (about \$ 10,000).

The law authorizes the Minister of Finance to set forth the resolutions necessary to ensure its implementation. The Minister of Finance can issue resolutions to enhance combating money laundering operations without the need to amend the legislation. Moreover, banks and financial institutions may face a steep fine (approximately \$3.3 million) if found in violation of the legislation.

In addition to those imposed by Law 35, Kuwait's anti-money laundering reporting requirements are contained within the Central Bank of Kuwait's Instructions No. (2/SB/50/97). Instructions contain

Money Laundering and Financial Crimes

provisions for: customer identification and the prohibition against opening or keeping anonymous accounts or accounts in obviously fictitious names (Articles 1 and 2), record keeping requirements and the seizing of suspected funds (Articles 3 and 4), and a prohibition against bank staff members' divulging to customers about the reporting of their suspicious transactions (Article 6).

Further provisions call for paying special attention to complex, large, or unusual transactions, and the reporting of crimes and suspicious transactions (STRs) to the Central Bank of Kuwait, which then notifies the Ministry of Interior (Article 7); coordination among banks on STR trends and patterns (Article 8); reporting of Currency Transaction Reports (CTRs) above 10,000 Kuwaiti dinars (KD) (approximately \$33,000) (Article 9); internal bank controls for detecting money laundering and bank staff training programs (Article 10); anti-money laundering guidelines for financial institutions in the form of "Guidelines for the Identification of Suspicious Transaction Patterns" (Article 11); and compliance requirements for branches and subsidiaries of Kuwaiti banks located abroad (Article 12).

Implementing legislation must still be developed to delineate the functions of the Financial Intelligence Unit (FIU) and to set up the requisite financial institution reporting system. Kuwait has still not formally established its FIU.

In September 2002, insurance companies, exchange bureaus, gold and precious metals shops, brokers in the Kuwait Stock Exchange, and all other financial brokers, were placed under strict supervision of the Ministry of Commerce and Industry. Such sectors have to abide by all regulations concerning customer identification, record keeping of all transactions for five years, internal control systems, and the reporting of suspicious transactions.

Although Kuwait has criminalized all forms of money laundering activities, substantial areas of the Kuwaiti financial sector are either under-regulated or not regulated or supervised at all. Islamic banks are not under the supervision of the Central Bank. Kuwait's one Islamic bank, Kuwait Finance House (KFH), is a charitable organization licensed and supervised out of the Ministry of Commerce and Industry, which apparently does not perform any type of examination of the KFH books. Another significant loophole is that so-called "VIP" transactions are not subject to the reporting requirements.

Following the September 11, 2001 attacks against the United States, certain Islamic charity organizations such as the Revival of Islamic Heritage Society (RIHS) and its subsidiary, the Afghan Support Committee (ASC), which operate from Kuwait and have branches in Pakistan and Afghanistan, were suspected of providing funds to al-Qaida. U.S. authorities have designated the branches in Pakistan and Afghanistan as being used to funnel funds to terrorist organizations. There is no indication that such activities occurred with the knowledge of the Kuwaiti head office.

In August, 2002, the Kuwaiti Ministry of Social Affairs and Labor issued a ministerial decree to create a Department of Charitable Organizations. The primary responsibilities of the new department are to receive applications of 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 Department will establish guidelines explaining how charities must collect donations and finance their activities. The new Department will also be charged with conducting periodic inspections to insure that they maintain administrative, accounting, and organizational standards according to Kuwaiti law.

The 2002 law on money laundering does not cite terrorist financing as a crime; however, the definition of criminal activity is broad. Kuwait established a national committee to follow up on all issues concerning terrorism. Reportedly there have been no money laundering or terrorist financing arrests or prosecutions in 2002. However, two terrorist suspects were charged in late 2002 with "gathering funds for, and financing the establishment of, military training camps abroad."

The Gulf Cooperation Council represents Kuwait on the Financial Action Task Force (FATF). Kuwait is not a signatory to the UN International Convention for the Suppression of the Financing of Terrorism, but is a party to the 1988 UN Drug Convention. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Kuwait should move to implement and enforce Law 35 and the anti-money laundering regulations. A specific counter-terrorism finance law should be enacted. Kuwait should establish a FIU and provide the FIU the ability to share information with foreign regulators and law enforcement authorities.

Kyrgyzstan. Kyrgyzstan (the Kyrgyz Republic) is not a regional financial center. Money laundering is not a crime in the Kyrgyz Republic. Moreover, it has a comparatively underdeveloped banking system. Like other countries in the region, the Kyrgyz Republic is susceptible to alternative remittance systems to launder money or transfer value such as hawala and trade fraud. The major sources of illegal proceeds include narcotics-trafficking, smuggling of consumer goods, tax and tariff evasion, and official corruption.

The Central Bank has provisions that require customer identification procedures and make an exception to bank secrecy rules for suspicious transaction reporting, but these provisions are reportedly ignored by the commercial banks. Oversight of the banking sector remains weak and Kyrgyzstan's law enforcement agencies lack the resources and expertise to conduct effective financial investigations.

Recognizing that the first step in constructing an effective anti-money laundering program is to criminalize money laundering, in 2002 the Government of Kyrgyzstan (GOK) drafted a law "On Opposition to Legalization (Laundering) of Incomes Obtained in Illegal Way in the Kyrgyz Republic." The draft law defines predicate offenses or criminal conduct as income "obtained as a result of committed crime." Mandatory suspicious transaction reporting by Kyrgyzstan financial institutions is included in the draft law. The law does not address money laundering methodologies that by-pass financial institutions. Details and possible revisions of the draft legislation are as yet unclear.

The Kyrgyz Republic is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. The Kyrgyz Republic has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Kyrgyz Republic should approve comprehensive anti-money laundering and anti-terrorism finance legislation that adheres to international standards, and become a party to the UN International Convention for the Suppression of the Financing of Terrorism. The GOK should also be aware that money laundering can easily by-pass financial institutions and take enforcement measures to address these vulnerabilities.

Laos. Laos is not a regional financial center and has no anti-money laundering legislation. Banking laws and regulations governing money laundering also do not exist. The country does have strict laws on the export of its currency, the Lao kip. The proceeds of drug trafficking most likely are sent to other countries through alternative remittance systems.

In late 2001, the Government of Laos (GOL) agreed to freeze terrorist financial assets. However, the Lao banking system is underdeveloped and there has been little progress to date.

The GOL is a party to the 1971 UN Convention on Psychotropic Substances and has stated its goal to become a party to the 1988 UN Drug Convention. GOL sends its officials to relevant Association of Southeast Asian Nations (ASEAN) regional conferences on money laundering.

Laos should pass anti-money laundering and anti-terrorism financing legislation. Laos should also sign the UN International Convention for the Suppression of Financing of Terrorism.

Latvia. The problems associated with money laundering continue to be a concern in Latvia in spite of compliance with legislative norms, regulations and "best practices" within the financial sector. Sources of laundered money include counterfeiting, corruption, white-collar crime, extortion, financial-banking crimes, stolen cars, and prostitution. Organized crime is thought to account for two-thirds of laundered proceeds. Latvia's mainly cash economy has been moving toward the use of electronic, credit, and other non-cash payments. At the same time, there are no restrictions in Latvia for cross-border currency movement (cash or non-cash, domestic or foreign) or the physical movement of other financial

Money Laundering and Financial Crimes

instruments. In August 2002 there were 222 operational bureaux de change, 21 casinos, 251 gaming halls, and 9,500 gambling machines.

The Government of Latvia (GOL) criminalized money laundering for all serious crimes in 1998. There are requirements for customer identification, the maintenance of records on all transactions, and the reporting of large cash transactions (40,000 lats or approximately \$64,600), and suspicious transactions to the Office for the Prevention of the Laundering of Proceeds Derived from Criminal Activity (Control Service), which is Latvia's Financial Intelligence Unit (FIU). The Control Service, which employs 13 persons, was established under the oversight of the Prosecutor's Office. Additional allocations for financing the Control Service for the year 2003 were made for the purpose of increasing the staff, purchasing technical resources and enhancing software development.

The number of suspicious disclosures reported to the Control Service increased from 17 percent of all reported transactions in 2000 to 32 percent in 2001. By September 2002, 50 criminal cases had been initiated by the Prosecutor's Office, three of which are pending. General trends in possible money laundering activity include the increasing use of bogus (fictitious) businesses or offshore companies. Another trend is the so-called "one-day-transaction" that actually entails a number of successive transactions in a short space of time.

Since July 2001, the Finance and Capital Market Commission (FCMC) has served as the public regulator, overseeing the Central Bank, the Securities and Exchange Commission, and insurance companies. The FCMC has approved guidelines for identifying customers and unusual and suspicious transactions, including guidance on the internal control mechanisms that financial institutions should have in place. It has advised financial institutions to pay much closer attention to transactions involving FATF-designated list of Non-Cooperative Countries and Territories or NCCT countries. The FCMC has also posted on its web page a list of persons suspected of having links to terrorism and the FATF guidelines for financial institutions for detection of cases of terrorism financing. Latvia continues to address the issue of offshore investments. Information on offshore company owners had been confidential. A commercial law, effective January 2002, now requires more information on the branches of offshore companies in Latvia. The law requires that at least half the board members of such companies must be permanent residents of Latvia, parent companies must submit their annual reports to a new commercial register, and changes in the parent companies' authorized personnel in Latvia must likewise be reported, in order to facilitate checking suspicious transactions.

The European Union 2001 Report on Latvia's Progress towards Accession to the EU characterized the perceived level of corruption in Latvia as relatively high. This was echoed by the Transparency International Corruption Perceptions Index 2002, which assigns Latvia a score of 3.7. ("Highly clean" rates a "10.") In January 2002 the Crime and Corruption Prevention Council was established; in April the Parliament adopted the Law on Prevention of Conflict of Interest of Public Officials; and, in May the Law on Corruption Prevention and Enforcement Bureau was adopted. The law established and funded one bureau whose sole task is to address and combat public corruption.

Reportedly, interagency cooperation between Latvian law enforcement agencies tends to be best at the highest governmental levels, but weaker at the working level due to lack of financial, material, and human resources. The investigative and gathering of evidence processes need streamlining. Two teams were created to work only on money laundering investigations. One was formed at the Financial Police, the other at the Economic Police. The latter has been operational since March 2002. To date, there have been no criminal convictions and no forfeitures of illicit proceeds based on money laundering.

Latvia participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-money Laundering Measures (Moneyval, formerly PC-R-EV), and as a member underwent a mutual evaluation in March 2000 that resulted in many of the aforementioned changes. It is currently in the process of the second round of evaluations. Latvia ratified the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of Proceeds from Crime in 1998, and the Council of Europe Criminal Law Convention on Corruption in December 2001. A Mutual Legal Assistance Treaty

has been in force between the United States and Latvia since 1999. Latvia is a party to the UN Drug Convention, and in December 2001 ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. The Control Service has been a member of the Egmont Group since 1999 and has cooperation agreements on information exchange with FIUs in Belgium, Bulgaria, the Czech Republic, Estonia, Finland, Italy, Lithuania, and Slovenia.

The GOL has initiated a number of measures toward combating the financing of terrorism, and became a party to the UN International Convention for the Suppression of the Financing of Terrorism (November 14, 2002), as well as five other international conventions on combating terrorism. Regulations have been adopted regarding the implementation of sanctions imposed by UNSCR 1267 and 1333. Regulations of the Cabinet of Ministers No. 437 “On the Sanction Regime of the United Nations Security Council against the Afghan Islam Emirates in the Republic of Latvia” guides the implementation of the sanctions imposed by the above-referenced UNSCRs. Latvia already had a mechanism for freezing financial resources or other property.

Amendments to the law “On Prevention of the Laundering of the Proceeds from Crime” have been in force since February 2002, which, among other things, provide for: 1) recognizing terrorism as a predicate offense for money laundering, 2) classifying financial resources or other property as proceeds derived from crime if they are directly or indirectly controlled or owned by a physical or juridical person included in the terrorist watch list, 3) making the Latvian FIU the authority that disseminates information on the watch list to credit and financial institutions, 4) giving the FIU authority to demand that credit and financial institutions suspend debit operations in the accounts of such persons or suspend movement of other property of such persons for up to six months, and 5) giving the FIU the authority to cooperate with foreign or international anti-terrorism agencies concerning issues of control over the movement of financial resources or other property linked to terrorism.

Since September 11, 2001, Latvian authorities have taken concrete steps to implement the above regulations. They have given considerable effort to tracing transactions executed by terrorists or their accomplices. Other practical measures include organizing relevant training courses for personnel in financial institutions, creating a special anti-terrorism information network within the financial system, nominating a person to deal with anti-terrorism issues at the FIU, and establishing an FIU reporting system and procedures concerning terrorist finances.

The GOL should continue to research ways to improve cooperation between Latvian law enforcement agencies at the working level. Latvia’s success in combating money laundering will depend on its perseverance and political will to combat corruption and organized crime. The GOL should adopt and implement cross-border currency controls, should regulate its bureaux de change and its gaming industry as well as the offshore companies that it licenses.

Lebanon. Lebanon has one of the more sophisticated and well-capitalized banking sectors in the region. Combined with the tradition of bank secrecy, the extensive use of foreign currency (particularly dollars), the influx of remittances from expatriate workers, and a general lack of accountability and enforcement, this allowed for an environment conducive to laundering money from sources that include narcotics, counterfeiting, smuggling, evasion of international sanctions as well as of domestic tax and currency regulations, and other organized criminal activity. Expatriate Lebanese citizens have established themselves in the underworld of the gold trade in Panama and other locations in Latin America and the diamond trade in Africa. Lebanese buyers in Liberia, Sierra Leone, and other African countries purchase raw diamonds from un-staked or illicit mines in exchange for cash. The diamonds are then passed through customs and shipped abroad to international markets in Israel, Belgium, and India for cutting, polishing, and selling.

Lebanon made significant progress in institutionalizing its anti-money laundering efforts in 2002, which culminated in the Financial Action Task Force’s (FATF’s) removal of Lebanon from the list of non-cooperative countries in June 2002. With its removal from the NCCT list, the U.S. Treasury’s Financial Crimes Enforcement Network (FinCEN) Advisory which had instructed all U.S. financial institutions to

Money Laundering and Financial Crimes

“give enhanced scrutiny” to all transactions involving Lebanon was also lifted. Lebanon’s efforts to meet FATF’s recommendations include criminalizing money laundering, establishing currency reporting guidelines, and creating a financial intelligence unit (FIU). In October 2002, the Cabinet approved legislation to criminalize the financing of terrorism. The draft law is currently awaiting parliamentary action.

In April 2001, Lebanon adopted Law No. 318 creating a framework for the lifting of 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. 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, building, and selling, real estate, and dealers in high-value commodities. In addition, companies engaged in high-value items (precious metals, antiquities) and real estate are obligated to report suspicious transactions in accordance with Law 318. Charitable and non-profit organizations must be registered with the Ministry of Interior, are required to have proper “corporate governance” including audited financial statements and are subject to the same “suspicious” reporting requirements.

All financial institutions and money exchange houses are regulated by the Central Bank (Banque du Liban). In May 2001, Law 318 was further delineated by Banque du Liban 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 a financial intelligence unit (FIU), the “Special Investigation Commission” (SIC), which is an independent entity with judicial status to investigate money laundering operations and to monitor compliance of banks and other financial institutions with the provisions of Law No. 318. SIC serves as the centerpiece 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. 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 requests for assistance are processed.

Since its inception, SIC has been active in providing support to international case referrals. Through the first nine months of its operation, it received 37 case referrals relating to money laundering and terrorist financing activities. All were investigated and bank secrecy regulations were lifted in 22 instances. The cases included 14 requests from the United States. From January 1 through mid-November 2002, SIC investigated 113 cases involving allegations of money laundering. Twenty of the cases were related to terrorist financing. SIC has circulated to all financial institutions the list of individuals and entities included on the UN 1267 sanctions committee’s consolidated list as being linked to al-Qaida or Taliban.

Offshore banking is not permitted in Lebanon. Current legislation stipulates that assets proven by a final court ruling to be related to or proceeding from money laundering will be confiscated. In addition, conveyances used to transport narcotics will be seized. Legitimate businesses established from illegal proceeds after passage of Law 381 are also subject to seizure.

The SIC has signed a number of memoranda of understanding with some FIUs concerning anti-money laundering and combating terrorist financing. Lebanon has endorsed the Basel Core Principles and is in the process of implementing them. Lebanon is party to the 1988 UN Drug Convention (although it has expressed reservations to several sections of the Convention relating to bank secrecy), and in December 2001 it signed the UN Convention against Transnational Organized Crime, which is not in force internationally.

The Government of Lebanon made significant progress in its efforts to develop an effective anti-money

laundering system. Passage of the amendments to Law 318 will be the best indicators that Lebanon remains on the right track in the fight against money laundering. The SIC is urged to work with financial institutions to increase the level and quality of suspicious transaction reporting. More efficient cooperation between SIC and other concerned parties, such as police and customs, could yield significant improvements in investigations or initiating investigations. Lebanon should sign the International Convention for the Suppression of Financing of Terrorism, and move swiftly to approve the draft law criminalizing terrorist financing.

Lesotho. Lesotho does not have a significant money laundering problem. There is currently no legislation criminalizing money laundering or terrorist financing. In 2001, the Government of Lesotho (GOL) began drafting an anti-money laundering statute based on the South African Development Community model. However, the GOL has not yet introduced the bill in Parliament.

Lesotho requires banks to know the identity of their customers and to report suspicious transactions to the Central Bank. The GOL also requires banks to report all transactions exceeding 100,000 maloti (approximately \$11,000) to the Central Bank.

Lesotho is a party to both the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. Lesotho has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Lesotho should criminalize money laundering and terrorist financing and should develop a viable anti-money laundering regime. Lesotho should also join the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body.

Liberia. Liberia is vulnerable to money laundering because it is a major transshipment point for illegal diamond smuggling, especially rough diamonds from Sierra Leone, and illegal arms trading. Liberia is also a growing transit country for narcotics on their way to Europe from Nigeria. As a significant diamond producing country, Liberia has attracted international attention because of its failure to effectively regulate its diamond industry under a certificate of origin regime, as called for by the UN. Money laundering involving diamonds and other precious metals and gems remains a concern. In May 2001, the UN Security Council adopted a resolution, since extended into 2003, prohibiting any trade in rough diamonds with Liberia. The Security Council took this step as a means of controlling the illicit trade in "conflict" diamonds from, or moving through, Liberia. Despite the fact that UN sanctions remained in place throughout 2002, Liberians continued to mine and smuggle stones. The Liberian Government claims it has not discouraged local diggers for fear that hundreds or thousands of unemployed miners would converge on the capital. The UN sanctions allegedly have caused a 40 percent drop in the price of stones on the local market. As a result, and given the proximity of Liberia's principal alluvial deposits to the border with Sierra Leone, local diggers are illicitly moving Liberian rough diamonds into Sierra Leone, where they fetch a better return, and can more easily be represented as of non-Liberian origin. Diamonds have also been used on a broad scale to purchase arms and otherwise fund conflict in the region, as detailed in the reports of UN experts. A typical money laundering scheme might include a businessman entering Liberia with a large amount of cash. The investor might purchase or otherwise obtain rough diamonds from illicit miners (without stakes) or other illicit sources in exchange for cash. These diamonds would then be passed through customs and shipped abroad to international markets in Israel, Belgium, and India for cutting, polishing, and resale.

Foreign diamond traders, including Eastern Europeans and Lebanese, often come to Monrovia to purchase diamonds on the black market and then export them out of Liberia through Monrovia's Roberts International Airport. Local security commanders and government officials are often paid to allow diamonds to pass through customs unchecked.

In 2001, the Liberian Government developed a prototype certificate of origin for diamonds based on the Kimberley process. However, the UN has not yet approved this certification regime as sufficiently effective to justify the removal of sanctions.

Money Laundering and Financial Crimes

Under anti-money laundering regulations enacted in 2001, monies that are carried out of the country over the sum of 7,000 Liberian dollars (approximately \$150) must be in the form of travelers' checks, money orders, or bank drafts. When entering the country, amounts of money that exceed 10,000 Liberian dollars (approximately \$215) must be declared to the Central Bank of Liberia. However, this regulation is not regularly enforced, and widespread corruption exists in Liberia's customs authorities.

Liberia's offshore activity is concentrated in the ship registry business, which is managed by the Liberian International Ship and Corporate Registry (LISCR), based in Virginia. The LISCR also manages Liberia's corporate registry. Offshore companies are permitted to issue bearer shares.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA), based in Dakar. Liberia is a member of GIABA, although no Liberian representatives attended the GIABA anti-money laundering seminar in November 2002. In July 2002 Liberia participated in the 2002 West African Joint Operation Conference (WAJO) that promotes regional law enforcement cooperation against drug trafficking, terrorism, and money laundering.

Liberia is not a party to the 1988 UN Drug Convention, nor has it signed the UN International Convention for the Suppression of the Financing of Terrorism.

Liberia should enact a comprehensive anti-money laundering regime that criminalizes money laundering and terrorist financing. Liberia should also enforce its cross-border reporting requirements and take steps to properly regulate its diamond industry.

Liechtenstein. The Principality of Liechtenstein's (Liechtenstein) well-developed offshore financial services sector, relatively low tax rates, loose incorporation and corporate governance rules, and a 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. Rumors and accusations of misuse of Liechtenstein's banking system persist in spite of the progress this principality has made in its efforts against money laundering.

Liechtenstein's financial services sector includes 17 banks, three non-bank financial companies, and 16 public investment companies, as well as insurance and reinsurance companies. Its 230 licensed fiduciary companies and 60 lawyers serve as nominees for, or manage, more than 75,000 entities (mostly corporations, Anstalts, or trusts) available primarily to nonresidents of Liechtenstein. Approximately one-third of these entities hold the controlling interest in other entities, chartered in countries other than Liechtenstein. Laws permit corporations to issue bearer shares.

Narcotics-related money laundering has been a criminal offense in Liechtenstein since 1993, but 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.

Liechtenstein's Financial Intelligence Unit (FIU), the Einheit fuer Finanzinformationen (EFFI) became operational in March 2001, and a member of the Egmont Group in June 2001. The EFFI works closely with the prosecutor's office and law enforcement authorities, as well as with a new unit of the National Police that deals with economic and organized crime. The FIU began operations on the basis of an executive order, but Liechtenstein formally adopted a law in May 2002 providing a statutory basis for the FIU's authority.

The EFFI has developed a system for suspicious transaction reporting (STR) analysis that involves internal analysis, consultation with police and a ten-day period to decide whether to forward the report to prosecutors for further action. EFFI has set up a database to analyze the STRs. Currently, banks, insurers, financial advisers, postal services, bureaux de change, attorneys, financial regulators, and casinos are required to file STRs.

The Financial Supervision Authority (FSA) is responsible for supervising all banks and fiduciaries licensed to operate in Liechtenstein. The FSA has the authority to conduct on-site spot checks and request information as required.

Following the Financial Action Task Force's (FATF) identification in 2000 of Liechtenstein as non-cooperative in international efforts to fight money laundering (NCCT), the U.S. Treasury Department issued an Advisory instructing U.S. financial institutions to "give enhanced scrutiny" to all transactions involving Liechtenstein. The Government of Liechtenstein (GOL) took legislative and administrative steps to improve its anti-money laundering regime. Specifically, the GOL amended its Due Diligence Act to incorporate "know your customer" principles that require banks and all other financial intermediaries to identify their clients and the beneficial owners of accounts. The GOL revised relevant portions of its criminal code to add a wide range of predicate crimes to the definition of money laundering and expanded money laundering offenses, in non-narcotics offenses, to cover "own funds." The new laws also address the independence of accountants reporting to the FSA on anti-money laundering compliance.

The GOL also reformed its system of suspicious transaction reporting. Reporting is now permitted for a much broader range of offenses and may be made based on a suspicion rather than the previous standard of "a strong suspicion." Nonetheless, the new law continues to require that financial institutions undertake some "clarification" of transactions before making a report, and there is some concern that this may be inhibiting the level of reporting or involve some risk of "tipping off."

The reforms to Liechtenstein's anti-money laundering regime have had positive results. In 2001, the EFFI reported 158 suspicions of money laundering, as opposed to 67 in the previous year, an increase of 136 percent. The EFFI recognizes the numerically low participation level among Liechtenstein's financial institutions. Only six banks out of 17 reported to the EFFI, seven out of 87 lawyers, and 20 out of 645 fiduciaries. Most of the customers involved in money laundering activities were from Germany (21 percent), Italy (10 percent), and Russia (9.5 percent). While U.S. customers only account for five percent of the money laundering reports, most of the assets under investigation in 2001 originated from the United States, (\$667 million), followed by France (\$533 million) and Russia (\$146 million).

The relatively small number of STRs filed by financial institutions in Liechtenstein has generated several money laundering investigations. For example, on July 19, 2001, the GOL formally charged two previously indicted managers of trusts with conspiring to launder millions of dollars for the Colombian Cali drug cartel, and related criminal organizations, through Liechtenstein bank accounts. On March 21, 2002, the Liechtenstein Ministry of Justice filed a complaint against Gabriel Marxer, a former parliamentarian, on the grounds he participated in the laundering of \$6.5 million originating from United States businessman James C. Sexton. United States authorities initiated the investigation as part of a large anti-fraud operation. Police authorities arrested eight people and blocked two bank accounts. The amount frozen has not yet been disclosed.

The GOL has made progress in strengthening its anti-money laundering regime and implementing recent reforms. It has increased the resources, both human and financial, devoted to fighting money laundering. The GOL has also improved its international cooperation provisions in both administrative and judicial matters, and has committed all financial institutions (banks and non-bank intermediaries) to obtain full identification of accounts' beneficial owners. To comply with new legislation that froze unidentified accounts on January 1, 2002, trustees and other financial intermediaries identified and filed client profiles with banks for over 45,000 customers, or approximately 97.2 percent of the total unidentified accounts by December 31, 2001. To remedy problems with the implementation of the laws, a Due Diligence Unit (SSP) was established to supervise compliance with anti-money laundering regulations. Its chief reports directly to the Prime Minister. Under the direction of the SSP, audits were conducted of a number of trustees supervised under the Due Diligence Act, and deficiencies were reviewed. The SSP works effectively and closely with the EFFI, the Office of the Prosecutor, and with the Police. Liechtenstein judges have worked hard to fully reduce the backlog of judicial assistance requests.

Money Laundering and Financial Crimes

The FATF recognized in June 2001 that Liechtenstein had remedied the serious deficiencies in its anti-money laundering regime and removed Liechtenstein from the FATF NCCT list. Similarly, the U.S. Treasury Department withdrew its Advisory against Liechtenstein. On July 24, 2002, the FATF informed the GOL that it would end the monitoring of the country, thus recognizing the measures taken against money laundering. "Liechtenstein has addressed all previously identified deficiencies and therefore, will no longer require monitoring by the FATF," the FATF's annual report stated.

Liechtenstein has in place legislation to seize, freeze, and share forfeited assets with cooperating countries. Liechtenstein has issued ordinances to implement United Nations Security Council Resolution (UNSCR) 1267, which requires all states to freeze funds and other financial resources of the Taliban, including funds derived by an undertaking owned or controlled by the Taliban, and UNSCR 1333, which requires all states to freeze funds and other financial assets of Usama Bin Ladin and his associates, including those in the al-Qaida organization. Amendments to the ordinances in October and November 2001, allowed the GOL to freeze the accounts of individuals and entities who were designated pursuant to these UNSCR resolutions. The GOL updates these ordinances regularly. On November 7, 2001, law enforcement entities in Switzerland, Liechtenstein, and Italy conducted raids and seized documents relating to Al Taqwa and Nada Management. Liechtenstein froze five Al Taqwa accounts and investigated five companies. In connection with these actions, the GOL responded to a mutual legal assistance request from Switzerland and opened a domestic investigation based on money laundering and organized crime.

Liechtenstein is a member of the Council of Europe Select Committee on Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, PC-R-EV), and is a party to the Council of Europe Convention on Laundering, Search and Confiscation of Proceeds from Crime. On October 3, 2001, the GOL signed the UN International Convention for the Suppression of the Financing of Terrorism. Liechtenstein has also signed, but has not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Liechtenstein has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision." Liechtenstein and the United States are concluding negotiations on a Mutual Legal Assistance Treaty (MLAT).

A FATF review in June 2002 found that the numbers of submitted STRs has increased, and Liechtenstein has made progress in addressing the previous shortcomings in its anti-money laundering regime. The GOL should continue to build upon the foundation of its evolving anti-money laundering regime. The GOL should insist that trustees and other fiduciaries comply fully with all aspects of the new anti-money laundering legislation and attendant regulations. The GOL should also criminalize the financing and support of terrorism.

Lithuania. Lithuania is not a regional financial center. However, its geographic location and limited experience in regulating financial institutions and transactions makes it attractive for some money launderers. Although some money laundering is related to narcotics proceeds, most is tied to tax evasion, smuggling, illegal production and sale of alcohol, capital flight, and profit concealment. It is estimated the shadow economy accounts for some 20 percent of the economy. Large-scale laundering via commercial banks carries significant risk, but money laundering outside the banking system is widespread due to loopholes in the tax system, corruption, and the prevalence of alternative remittance systems.

The criminal code created in 1997 was amended to criminalize the act of money laundering. In January 1998, the Law on the Prevention of Money Laundering (LPML), entered into force. The LPML provides for suspicious transaction reporting and the identification of customers whose transactions exceed litas (LTL) 50,000 (approximately \$15,000) or the equivalent in foreign currency. The LPML also made provisions for maintaining a register of customers who engage in transactions that exceed LTL 50,000 or the equivalent in foreign currency; and retain certain documents for a minimum of ten years. Along with collection of reports, the LPML specifies information to be reported to the tax police. The Bank of Lithuania (BOL) issues currency transaction reporting requirements and regulations and is required to share money laundering violation information with law enforcement and other state institutions upon

request. Non-bank financial institutions operate under guidelines similar to banks. The BOL has the authority to examine the books, records, and other documents of all financial institutions.

The Money Laundering Prevention Division (MLPD) of the Financial Crimes Investigation Service is Lithuania's Financial Intelligence Unit. The MLPD is a member of the Egmont Group. Lithuania has signed memoranda on exchange of laundering-related financial and intelligence information with financial intelligence agencies of Belgium, Croatia, the Czech Republic, Estonia, Finland, Latvia, and Poland. The Lithuanian Tax Police Department, in charge of investigations of financial crimes, also has cooperation agreements with law enforcement agencies of Belarus, Georgia, Kazakhstan, Russia and Ukraine. In May 2002, the Lithuanian parliament ratified a governmental agreement with Germany on cooperation in work against organized crime, terrorism and other serious crimes.

Lithuania is a party to the 1988 UN Drug Convention, and ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally, in 2002. Lithuania is also a party to the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime. There is a mutual legal assistance treaty (MLAT) between the United States and Lithuania, which entered into force in 1999. Lithuania is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, formerly PC-R-EV), and the MLPD is a member of the Egmont Group.

Lithuania should sign the UN International Convention for the Suppression of the Financing of Terrorism and criminalize terrorist financing.

Luxembourg. Luxembourg is the seventh-largest financial center in the world, with more than 200 international financial institutions that benefit from the country's strict bank secrecy laws, and operate a wide range of services and activities. Luxembourg is currently the third largest domicile for investment funds (behind the United States and France), with over \$950 billion in net assets managed by the investment fund industry. Luxembourg is considered an offshore financial center. Foreign-owned banks account for around 94 percent of total bank assets, the majority of which are subsidiaries of German, French and Belgian banks. For this reason, and given their proximity to Luxembourg, a large number of suspicious transaction reports (STRs) in Luxembourg are generated from transactions involving clients in these countries. Luxembourg currently has no cross-border currency reporting requirements. As of December 2002, 177 banks were operating as "universal banks," with the ability to provide a wide range of services. As of October 2002, Luxembourg had 1,960 "undertakings for collective investment" (UCIs), or mutual fund companies, which included but were not limited to investment funds, 93 insurance companies (estimate), and 265 reinsurance companies. The size and sophistication of Luxembourg's financial center pose major risks for money laundering. Although Luxembourg bank secrecy rules may appear vulnerable to abuse by those transferring illegally obtained assets, under Luxembourg law the secrecy rules are waived in the prosecution of money laundering and other criminal cases.

Luxembourg has a well-developed legal and regulatory system to combat money laundering, and financial sector laws are modeled to a large extent by EU directives. The Law of 7 July 1989, updated in 1998, serves as Luxembourg's primary anti-money laundering law, criminalizing the laundering of proceeds for an extensive list of predicate offenses. The Law of 5 April 1993 implements the 1991 EU anti-money laundering directive (91/308/EEC), and includes customer identification, record keeping, and suspicious transaction reporting requirements. The Act of 11 August 1998 extends anti-money laundering provisions to notaries, casinos, and external auditors, and adds corruption, weapons offenses, and organized crime to the list of predicate offenses for money laundering. Among other things, the Act of 10 June 1999 extends anti-money laundering provisions to accountants. Luxembourg is presently in the domestic implementation phase of the EU directive on the Prevention of the use of the Financial System for the Purpose of Money Laundering (2001/97/EC). The new legislation, expected to be enacted in 2003, will extend reporting requirements to lawyers, certain real estate professionals, and dealers in high-value goods.

The Parquet Economique et Financier Luxembourg/Service Anti-Blanchiment (the Public Prosecutor), serves as Luxembourg's Financial Intelligence Unit (FIU), receiving and analyzing suspicious transaction

Money Laundering and Financial Crimes

reports from the financial sector. The Commission de Surveillance du Secteur Financier (CSSF) is an independent government body that serves as the oversight authority for banks and the securities market, and supervises professionals covered by the country's anti-money laundering laws. The Commissariat aux Assurances (CAA) has oversight authority over the insurance sector, and the Luxembourg Central Bank oversees the payment and securities settlement system. 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. No distinctions are made in Luxembourg 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 government registry publicly lists company directors, and nominee (anonymous) directors are not permitted. Bearer shares are permitted. 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.

The Government of Luxembourg (GOL) is actively engaged in efforts to combat money laundering, and to further develop its effectiveness in this area. Under the direction of the Ministry of the Treasury, the CSSF has established a public-private committee comprising supervisory authorities, law enforcement authorities, the FIU, and representatives of financial professions and other professions under the scope of EU and Luxembourg anti-money laundering rules. The committee, the Comité de Pilotage anti-Blanchiment (COPILAB) meets monthly to develop a common approach to strengthen Luxembourg's anti-money laundering regime.

Suspicious transaction reporting requirements apply not only to banks, but also to auditors, accountants, notaries, and life insurance providers. Financial institutions are required to retain records for a period of five years. Individuals aiding government officials in money laundering investigations are protected by law. Since 2000, the number of STRs filed by obligated institutions have more than tripled; the number of STRs received by authorities for 2002 is expected to have reached 600. Nonetheless, there have been no arrests or prosecutions for money laundering since January 2001. Luxembourg authorities regularly exchange information with counterparts in other countries, and attribute the lack of arrests for money laundering to the fact that suspected perpetrators are usually not physically present in Luxembourg.

Since September 11, 2001, Luxembourg has committed itself to fighting the financing of terrorism. 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. Dialogue and other bilateral proceedings between the GOL and the United States have been particularly extensive. The GOL also has actively disseminated information concerning suspected terrorists throughout its institutions in an effort to identify and freeze the assets of these individuals.

Upon request from the United States, Luxembourg froze the bank accounts of individuals suspected of involvement in terrorism. Luxembourg also froze eighteen accounts on its own. Five court challenges have been filed thus far by the account holders. During 2002, over \$200 million in suspect accounts were frozen by Luxembourg authorities pending further investigation (most of which were not fruitful, and the assets were then released). Currently, terrorism financing is addressed under Luxembourg's money laundering statutes. However, the GOL has draft legislation, expected to be enacted during the first half of 2003, that will criminalize terrorism financing separately from money laundering as well as codify it as a predicate offense of money laundering. 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 anti-money laundering rules would apply to such systems, and no separate legislative initiatives are currently being considered to address them.

Luxembourg is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Luxembourg laws facilitating international cooperation in money laundering include the Act of 8 August 2000, which enhanced and simplified procedures on international judicial cooperation in criminal matters, and the Law of 14 June 2001, which ratified the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime. Luxembourg has a definitive system not only for the seizure and forfeiture of criminal assets, but also for the sharing of those assets with other governments. Luxembourg is a member of the European Union, the Financial Action Task Force (FATF), and the Organization for Economic Cooperation and Development (OECD). The Luxembourg FIU is a member of the Egmont Group and has negotiated memoranda of understanding (MOU) 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. In September 2001, Luxembourg signed, but has not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism. A proposed law for the ratification of the Convention is currently before the Luxembourg parliament.

Luxembourg has enacted laws and adopted practices that help to prevent the abuse of its bank secrecy laws. The GOL should continue to strengthen enforcement to prevent international criminals from abusing Luxembourg's financial sector and should give serious consideration to legislative amendments to address the continued use of bearer shares and the lack of cross-border currency reporting requirements.

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 and is not a financial center. The offshore financial sector is not fully developed.

The IMF conducted a financial sector assessment of Macau, and the results published in August 2002 stated that Macau was "materially non-compliant" with the money laundering principles of the Basel Committee's "Core Principles for Effective Banking Supervision." The assessment concluded that an anti-money laundering legal framework was in place in Macau, but recommended improvements in implementation and enforcement.

Macau's 1993 Financial System Act lays out regulations to prevent the use of the banking system for money laundering. It 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 Macau Special Administrative Region Government (MSARG), including pawnbrokers, antique dealers, art dealers, jewelers, and real estate agents. There is no significant difference in the regulation and supervision of onshore versus offshore financial activities.

The gaming sector and related tourism are critical parts of Macau's economy. Direct taxes from gaming comprised 60 percent of government revenue in 2001 and about 30 percent of GDP in 2000. The MSARG ended a long-standing gaming monopoly early in 2002 when it awarded concessions to two additional operators. These two firms have yet to begin gaming operations. 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.

Money Laundering and Financial Crimes

The VIP rooms cater to clients seeking anonymity within Macau's gambling establishments and are particularly removed from official scrutiny. As a result, the gaming industry, in particular, provides an avenue for the laundering of illicit funds.

The Macau Inspectorate of Gaming has not played an active role in preventing money laundering in the casinos. The casinos have not filed any suspicious transaction reports. The MSARG is drafting regulations designed to prevent money laundering in the gambling industry as part of the restructuring of that sector.

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 MSARG has the authority to freeze terrorist assets, although a judicial order is required. Macau financial authorities directed the institutions they supervise to conduct record searches for terrorist assets, using U.S. Executive Order 13224 and United Nations lists. No assets have been found to date.

The Macau legislature passed an anti-terrorism law in April 2002 that increases Macau's compliance with UNSCR 1373. The legislation criminalizes violations of UN Security Council resolutions, including anti-terrorist resolutions, and strengthens anti-terrorist financing provisions. The UN International Convention for the Suppression of the Financing of Terrorism will apply to Macau when the People's Republic of China accedes to it.

The increased attention paid to financial crimes in Macau after the events of September 11 led to an increase in the number of suspicious transaction reports. Fifty-five reports were filed from January to November 2002. In previous years, only a handful of reports were filed each year.

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, moneychangers, and remittance agents addressing record keeping and suspicious transaction reporting for cash transactions over \$2,500. MSARG officials attended anti-money laundering training sessions offered by the Asia/Pacific Group on Money Laundering (APG). The police boosted hiring in 2002, which will provide more resources for anti-money laundering efforts.

The United States has no law enforcement cooperation agreements with Macau, though international cooperation can be requested on the basis of international conventions in force in Macau. The MSARG is preparing legislation to enable it to negotiate mutual legal assistance agreements with other jurisdictions.

Macau is a member of APG and the Offshore Group of Banking Supervisors. The People's Republic of China is a party to the 1988 UN Drug Convention, and through it the Convention is applicable to Macau.

Macau has taken a number of steps in the past two years to create an effective anti-money laundering regime. Macau is urged to implement and enforce existing laws and regulations. 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, the regulations it has drafted on the prevention of money laundering in casinos. Macau should establish a Financial Intelligence Unit as soon as possible. The MSARG should also consider measures that provide for cross-border bulk currency and threshold reporting. Macau should increase public awareness of the money laundering problem, improve interagency coordination, and boost cooperation between the MSARG and the private sector in combating money laundering.

Macedonia, Former Yugoslav Republic of. The Former Yugoslav Republic of Macedonia (FYROM) is not a regional financial center. The country's economy is heavily cash-based because of the population's distrust of the banking, financial, and tax systems. Money laundering in the FYROM is most likely connected to financial crimes such as tax evasion, smuggling, financial and privatization fraud, bribery, and corruption. A small portion of money laundering is believed to be connected to narcotics-trafficking.

Article 273 of the FYROM's criminal code, which came into force in 1996, criminalizes money laundering related to all crimes. The legislation specifically identifies narcotics and arms trafficking as predicate offenses, and contains an additional provision that covers funds that are acquired from other punishable

actions. In November 2001, Parliament passed the Law on Money Laundering Prevention (LMLP), which explicitly defines money laundering for the first time in Macedonian legislation. The LMLP, which went into effect in March 2002, requires financial institutions to know, record, and report the identity of clients that perform cash transactions exceeding 10,000 euros, to prepare programs to protect themselves against money laundering, and to report suspicious transactions. The Customs administration is required to register and report the cross-border transport of currency or monetary instruments exceeding 10,000 euros.

Furthermore, the LMLP establishes the Directorate for Money Laundering Prevention within the Ministry of Finance. The Directorate collects, processes, analyzes, and stores data received from financial institutions and other government agencies. Reporting entities are legally protected in their cooperation with law enforcement entities. The Directorate has the authority to submit collected information to the police and the judiciary.

In June 2002, parliament passed a Law establishing a Financial Police Unit. The unit is yet to be created, but the implementation program is already in place. The unit will be within the Ministry of Finance, and it will investigate suspicious transactions reported to the Directorate and other potential financial crimes.

Macedonian authorities require court orders before they can freeze assets with suspected links to money laundering or terrorist financing. The FYROM has proposed amendments to the LMLP that will allow financial institutions to temporarily freeze assets of suspected money launderers and terrorist financiers.

Macedonia has concluded a number of Police Cooperation Agreements with almost all of the countries from the Region (Albania, Bulgaria, Croatia, Romania, Slovenia, Austria, Turkey, Greece, Russian Federation, Ukraine, Egypt) and has a number of mutual legal assistance agreements with many countries. Exchange of police information is regularly provided through Interpol channels. The FYROM also provides law enforcement information in connection with requests from other countries with which it lacks a formal information exchange mechanism, including the United States.

The FYROM is a member of the Council of Europe (COE) Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, formerly PC-R-EV), and in October 1999, underwent a mutual evaluation by the group. The FYROM is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

The FYROM should criminalize terrorist financing and take further steps to develop a viable anti-money laundering regime.

Madagascar. Madagascar is not a regional financial center. Criminal activity in Madagascar reportedly includes smuggling in animal products such as tortoise shells and reptile skins for sale in the international market. These schemes have in the past been related to money laundering activities within the country.

Madagascar's 1997 anti-money laundering law criminalizes money laundering related to narcotics-trafficking. The Central Bank and the Ministry of Finance can request a court order to freeze a bank account or another financial asset. The National Assembly is considering an updated anti-money laundering law that reportedly would criminalize money laundering for all crimes, criminalize terrorist financing, and require banks and other financial institutions to report suspicious transactions.

Madagascar is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Madagascar has signed, but not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

Madagascar should enact a comprehensive anti-money laundering regime that criminalizes terrorist financing and money laundering for all serious crimes.

Malawi. Malawi is not a regional financial center. The Reserve Bank of Malawi (RBM), Malawi's Central Bank, supervises the country's six commercial banks. Some money laundering is tied to smuggling. Under

Money Laundering and Financial Crimes

Malawi's existing exchange control regime, foreign exchange remittances not backed by a "genuine transaction" are illegal; traders therefore launder funds in their efforts to remit savings abroad.

Financial institutions are required to record and report the identity of customers making large transactions, and banks must maintain those records for seven years. Banks are allowed, but not required, to submit suspicious transaction reports to the RBM. The RBM inspects banks' records every quarter and has access to those records on an "as needed" basis for specific investigations.

Malawi's current laws do not specifically criminalize money laundering, but can be used to prosecute money laundering cases. The Government of Malawi (GOM) has drafted a "Money Laundering and Proceeds of Serious Crime" bill, which is part of Parliament's pending business for 2003. The draft law would specifically criminalize money laundering related to all serious crimes. The draft law would also establish a legal framework for identifying, freezing, and seizing assets related to money laundering.

While the GOM has not specifically criminalized terrorist financing, the RBM has the legal authority to identify and freeze assets suspected of involvement in terrorist financing. The RBM has circulated to the financial community all names included on the UN 1267 Sanctions Committee consolidated list and all other names suggested by the United States Government as connected to terrorist financing. The RBM continues to monitor the financial system for money laundering activity.

Malawi has signed the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) Memorandum of Understanding. Malawi is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Malawi should take steps to strengthen its anti-money laundering and counter-terrorist financing regimes as it has agreed to do as a member of ESAAMLG. Malawi should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Malaysia. Malaysia is not a major regional financial center, although it does offer a wide range of financial services in its formal financial sector, its offshore financial center, and through alternative money remittance systems that are potentially attractive to money launderers. The true extent of money laundering in Malaysia is not known, and to date there have been no effective prosecutions of money laundering activities.

Malaysia's Anti-Money Laundering Act (AMLA) became effective in January 2002. The AMLA criminalizes money laundering and lifts bank secrecy provisions for criminal investigations involving approximately 150 predicate offenses. The law imposes obligations on financial institutions regarding customer identification, record keeping, and suspicious transaction reporting by both bank and non-bank financial institutions. Banks include commercial and merchant banks, Islamic banks, and Labuan offshore banks. Non-banking financial institutions (NBFIs) include finance companies, discount houses, money brokers, insurers, Takaful (i.e., Islamic insurance) companies, securities dealers, moneychangers, futures brokers, development banks and casinos. Reporting individuals and their institutions are protected by law with respect to their cooperation with law enforcement.

Suspicious transaction reports are required under Section 14 of the AMLA. However, thresholds, requirements, and forms are industry or code-of-conduct based; thus, there is no consistency. Banks, insurers, insurance brokers, and moneychangers in the conventional, Islamic, and offshore sectors are required to file suspicious transaction reports. Money laundering controls have not yet been extended to many non-banking financial institutions, including exchange houses, stock brokerages, and casinos or to intermediaries such as lawyers, accountants, and brokers. Development banks and casinos are scheduled to come under reporting requirements in 2003. The AMLA allows for the development of regulations to standardize these requirements. However, as of yet no regulations have been implemented. Approximately 800 suspicious transaction reports were filed since the law's implementation in January 2002.

The January 2002 law also created a Financial Intelligence Unit (FIU) located in the Central Bank, Bank Negara Malaysia (BNM). The FIU, now operational, is tasked with receiving and analyzing information,

and forwarding its findings to the appropriate legal and regulatory authorities for prosecution, as required. Malaysia's longstanding National Coordination Committee to Counter Money Laundering (NCC) is composed of members from 13 government agencies. The NCC oversaw the drafting of the anti-money laundering law and coordinates government-wide anti-money laundering efforts.

The Government of Malaysia (GOM) has a well-developed regulatory framework, including licensing and background checks, to oversee onshore financial institutions. BNM guidelines require customer identification and verification, financial record keeping, and suspicious activity reporting. These guidelines are intended to require banking institutions to determine the true identities of customers opening accounts and to develop a "transaction profile" of each customer with the intent of identifying unusual or suspicious transactions. The actual examination coverage of anti-money laundering efforts is still in development for all segments. Currently seventeen examiners are responsible for money laundering inspections for both onshore and offshore banks. Examination procedures are being developed, and additional examiner training is forthcoming.

In 1998 Malaysia imposed foreign exchange controls that restrict the flow of the local currency, the ringgit, from Malaysia. Some currency smugglers have since been arrested. Under these exchange control laws, onshore banks must note cross-border transfers over 10,000 ringgit (approximately \$2,630).

The potential for money laundering activities at the offshore banking facility in the Labuan Offshore Financial Center (often referred to simply as "Labuan") is of concern, as there is no requirement for the beneficial owners of international business companies (IBCs) to be identified. The Labuan Offshore Financial Services Authority (LOFSA) regulates the wide range of financial services, such as offshore banking and trust partnerships, provided by the offshore sector. Labuan hosts 53 offshore banks (46 foreign-owned), approximately 50 insurance companies, four mutual funds, 15 fund managers, 29 leasing operations, and 18 active trust companies. Because there is no requirement to register offshore trusts, their number is not known. Nominee trustees are permitted in Labuan, as are nominee directors of the 2,070 IBCs incorporated or registered in Labuan. There is no requirement to disclose the beneficial owner of a corporation. There is, however, a government registry of corporate directors and shareholders, although this information is not available to the public.

Malaysia has not criminalized terrorist financing per se, although terrorist financing is included as a predicate offense in the country's anti-money laundering law. Additionally, the GOM has the authority to identify, freeze, and seize terrorist- or terrorism-related assets. Malaysia has issued orders to all licensed financial institutions, both onshore and offshore, to freeze the assets of individuals and entities listed by the UN Security Council Resolution (UNSCR) 1267. As of December 31, 2002, Malaysia had located no terrorist-related assets.

Malaysia forbids illegal deposit taking, unlawful compensation deals, illegal remittance or transfer, and money laundering, which provides the legal groundwork to deal with alternative remittance systems, such as hawala, black market exchanges and trade-based money laundering. However, Malaysia faces a challenge in regulating alternative remittance systems that are, by their nature, unofficial and unrecorded. Though the government has rules regulating charities and other non-profit entities, authorities have generally taken a hands-off approach to both groups.

The Malaysian FIU and its Australian counterpart, AUSTRAC, signed a memorandum of understanding to facilitate the sharing of financial intelligence for the purposes of combating money laundering. The GOM has offered to conclude a similar memorandum of understanding between Malaysia's FIU and FinCEN, the U.S. FIU, for the purpose of facilitating the exchange of financial intelligence. Malaysia allows foreign countries to check the operations of their banks' branches. Malaysia has cooperated closely with U.S. law enforcement in investigating terrorist, counternarcotics, and other cases. In April 2002, the GOM passed the Mutual Assistance in Criminal Matters Bill 2002. Malaysia has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. The GOM has not signed the UN International Convention for the Suppression of the Financing of Terrorism. Malaysia is a party to the 1988 UN Drug Convention. Malaysia has endorsed the

Basel Committee's "Core Principles for Effective Banking Supervision" and is a member of the Offshore Group of Banking Supervisors and the Asia/Pacific Group on Money Laundering. Malaysia is seeking membership in the Egmont Group.

The GOM should continue to enhance the viability of its evolving anti-money laundering regime by amending its anti-money laundering legislation to include as predicate offenses all serious crimes and should expand coverage of the Anti-Money Laundering Act to all financial institutions, onshore and offshore, not presently covered. Malaysia should adequately regulate non-governmental organizations, including charities, to ensure they are not used for terrorist or other criminal ends. The GOM should issue and implement all regulations, as required in the AMLA, and issue standardized requirements that are applied consistently for all financial institutions, bank and non-bank, supervised by Bank Negara Malaysia. Bank Negara will also need to increase its staff of examiners. For all entities such as trust companies and IBCs, Malaysia should insist on "fit and proper tests" for all management, and identification of all beneficial owners. The GOM should also insist on the registration of trusts, and stringent auditing and examination requirements in its offshore financial center, to prevent the misuse of the offshore financial center by organized crime and terrorist organizations, and their supporters. Additionally, the GOM should accede to the UN International Convention for the Suppression of the Financing of Terrorism, and, to further implement UN Security Council Resolutions 1373 and 1390, should enact legislation that explicitly criminalizes terrorist financing.

The Maldives. The Maldives is not considered an important regional financial center. The financial sector of the Maldives is very narrowly based with five commercial banks (one international bank, three branches of public banks from neighboring countries and the state owned bank), two insurance companies, and a government provident fund. There are no offshore banks.

The Maldives Monetary Authority (MMA) is the regulatory agency for the financial sector. MMA has authority to supervise the banking system through the Maldives Monetary Authority Act. These laws and regulations provide the MMA access to records of financial institutions and allow it to take actions against suspected criminal activities. Banks are required to report any unusual movement of funds through the banking system on a daily basis. However, there is no specific legislation dealing with money laundering. Currently, separate laws address the narcotics trade, terrorism, and corruption: Law No. 17/77 on Narcotic Drugs and Psychotropic Substances prohibits consumption and trafficking of narcotics. The law also prohibits laundering of proceeds from narcotics trade. Law No 2/2000 on Prevention and Prohibition of Corruption prohibits corrupt activities by both public and private sector officials. It also provides for the forfeiture of proceeds and also empowers judicial authorities to freeze accounts pending a court decision.

Reportedly, the Government of Maldives (GOM) has approved the development of an Anti-Money Laundering Law and establishment of a Financial Intelligence Unit.

Law No. 10/90 on Prevention of Terrorism in the Maldives deals with some aspects of money laundering and terrorist financing. Provision of funds or any form of assistance towards the commissioning or planning any such terrorist activity is unlawful. The MMA has issued "know your customer" directives and other instructions to banks enforcing freeze order requests, which are binding on banks and other financial institutions. The MMA monitors unusual financial transactions through banks, financial institutions, and money transfer companies through its bank supervision activities. The four foreign banks operating in the country also follow instructions issued with regard to terrorist financing by their parent organizations. To date, there have been no known cases of terrorist financing activities through banks in the Maldives.

The Maldives is a party to the 1988 UN Drug Convention.

The Maldives should enact comprehensive anti-money laundering and anti-terrorist financing legislation that adheres to world standards. The GOM should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Mali. Mali is not a regional financial center nor is money laundering considered to be a problem.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA), based in Dakar, Senegal. In November 2002, the GIABA hosted an anti-money laundering seminar for representatives of 14 ECOWAS members, including Mali. In July 2002, Mali participated in the 2002 West African Joint Operation Conference (WAJO) that promotes regional law enforcement cooperation against drug trafficking, terrorism, and money laundering.

Mali became a party to the UN International Convention for the Suppression of the Financing of Terrorism on March 28, 2002. On April 12, 2002, Mali ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Mali is a party to the 1988 UN Drug Convention.

Mali should enact comprehensive anti-money laundering legislation that criminalizes terrorist financing and money laundering for all serious crimes.

Malta. Malta has spent the last decade preparing itself for accession to the European Union (EU). As a result, it has toughened up its regulations to accommodate European investors and introduced several laws designed to shed its image as an offshore tax haven. Malta has made significant headway, introducing EU-compliant legislation for the prevention of money laundering, and strong financial services legislation. Malta does not appear to have a serious money laundering problem.

The Government of Malta (GOM) criminalized money laundering in 1994. Maltese law imposes a maximum fine of approximately \$2 million and/or 14 years in prison for those convicted. Also in 1994, the GOM issued the Prevention of Money Laundering Regulations, applicable to financial and credit institutions, life insurance companies, and investment and stock firms. These regulations impose requirements for customer identification, record keeping, the reporting of suspicious transactions, and the training of employees in anti-money laundering topics. In 1996, the banking unit at the Maltese Financial Services Authority (MFSA) updated the Guidance Notes issued by the Central Bank of Malta. The MFSA is the regulatory agency responsible for licensing new banks and financial institutions; additionally the MFSA has historically monitored financial transactions going through Malta. It has recently widened its regulatory scope to encompass banking, insurance, investment services, company compliance, and the stock exchange. MFSA also took over the role of supervisory authority of the banking sector. Presently there is an initiative to consolidate all guidance notes for all of the covered financial services.

In December 2001, Malta's parliament established the Financial Intelligence Analysis Unit (FIAU) through an amendment to the Prevention of Money Laundering Act. The unit became fully functional in the summer of 2002. Its board consists of members of the Central Bank of Malta, the MFSA, the Ministry of Finance, the Police, Malta's Custom and Security Service, and the Attorney General. The FIAU coordinates the fight against money laundering, collects information from financial institutions, and liaises with parallel international institutions as well as local investigative authorities (the MFSA & the GOM Police). The FIAU is charged with investigating suspicious financial transactions and other questionable money-related activity, and has organized training sessions and conferences for Maltese financial practitioners to make them aware of the implications of the 2001 Money Laundering Act.

Malta has also moved to bolster the prosecutorial opportunities in financial crime investigations. The GOM has recently designated one of the country's five prosecutors to deal solely with money laundering cases. Bank secrecy laws are completely lifted by law in cases of money laundering (or other criminal) investigations. The Attorney General is currently pursuing an investigation into an alleged money laundering case involving two lawyers. Neither has yet been charged, but they are being investigated for their alleged role in a smuggling operation involving Northern Ireland. The marked increase in the number of suspicious transaction reports (STRs), up from nine in 1998 to 43 in 2002, also indicates Malta's determination to crack down. Enforcement should continue to strengthen as the new FIAU begins its work analyzing STRs for referral for police investigation.

Money Laundering and Financial Crimes

Malta remains an offshore jurisdiction and is a member of the Offshore Group of Banking Supervisors. Over 200 companies retain offshore status against some 30,000 that do not, and legislation dealing with offshore business will remain in force until 2004. Offshore registration of banks and international business corporations (IBCs) was halted in January 1997, and the GOM has publicly announced that offshore business will completely cease by 2004. Companies and trusts are now fairly well regulated, and international entities are subject to 35 per cent tax. Bearer shares or anonymous accounts are no longer permitted in Malta.

The Financial Action Task Force (FATF), which reviewed Malta's financial regime via the FATF Non-cooperative Countries and Territories exercise in 2000, did not name Malta as a non-cooperative jurisdiction but did urge Malta "to accelerate the phasing-out of the nominee company system." As a result, the number of IBCs has declined from 417 in 2001, to 285 in 2002, and the number of offshore banks has declined from 3 to 1 (Erste Bank).

Malta has criminalized terrorist financing. In 2002, the criminal code was amended in such a way that terrorist financing would meet the standard for categorization as a "serious crime" under Malta's Prevention of Money Laundering Act. To date, the Act itself does not specifically mention or define terrorist financing.

The MFSA circulates to its financial institutions the names of individuals and entities included on the UN 1267 Sanctions Committee's consolidated list. To ensure compliance, the list is posted on the MFSA website and the MFSA contacts every financial institution directly to confirm whether or not the institution has done business with any person or entity appearing on the consolidated list. To date no assets have been identified, frozen, and/or seized as a result of this process.

Alternative remittance systems such as hawala, black market exchanges, and trade-based money laundering, are not a problem in Malta. Such activities are against the law in Malta, and if discovered, those participating would be prosecuted. Anyone wishing to raise money for charitable reasons must receive a government license. The overwhelming majority of all charitable fund raising in Malta is done by the Catholic Church and related institutions.

Malta is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, formerly PC-R-EV). Malta is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime. Malta has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Malta ratified the UN International Convention for the Suppression of the Financing of Terrorism in November 2001. Malta has also ratified the Council of Europe European Convention on the Suppression of Terrorism and has amended its criminal code to be in alignment with these conventions.

Malta's recent acceptance by the Organization of Economic Cooperation and Development (OECD) is perhaps the best indicator that Malta is no longer considered a tax haven. Malta should continue to enhance its anti-money laundering regime. If Malta's Prevention of Money Laundering Act only references the proceeds of a terrorist act as a predicate offense and does not specifically criminalize the support or financing of terrorism, the legislation should be amended to include this activity or a new legislation should be enacted.

Marshall Islands. The Republic of the Marshall Islands (RMI), a group of atolls located in the North Pacific Ocean, is a sovereign state in free association with the United States. The population of RMI is approximately 65,000. The financial system in RMI has total banking system assets of \$87.2 million and total deposits of \$77.4 million, with domestic deposits exceeding 50% of Gross Domestic Product. The RMI financial sector consists of three banks, two of which are insured by the Federal Deposit Insurance Corporation, and a government-owned development bank whose primary function is to perform development lending in government-prioritized sectors; and several low-volume insurance agencies that primarily sell policies on behalf of foreign insurance companies. In realization of the country's

vulnerability to systemic shock in the financial sector, the government introduced a reform program geared toward enhancing transparency, accountability and good governance.

In June 2000, the Financial Action Task Force (FATF) placed the Marshall Islands on the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering. The designation was based on RMI's lack of basic anti-money laundering regulations (including the criminalization of money laundering), customer identification requirements and a suspicious transaction reporting system. Additionally, the RMI had registered about 4,000 international business corporations. The relevant information regarding the beneficial owners of these IBCs was guarded by secrecy provisions in its law, and consequently, this information was not accessible to financial institutions, international regulatory bodies or law enforcement agencies.

Over the past two years, the Marshall Islands enacted significant legislative reforms to address the major deficiencies identified by the FATF. Money laundering was criminalized and customer identification and suspicious transaction reporting mandated. The Marshall Islands also issued guidance to its financial institutions for the reporting of suspicious transactions. In addition, the RMI drafted anti-money laundering regulations.

In November 2000, the Government of the Marshall Islands (GRMI) approved the establishment of a Financial Intelligence Unit that may exchange information with international law enforcement and regulatory agencies. The Domestic Financial Intelligence Unit (DFIU) is located within the Banking Commission. The DFIU receives, analyzes, and disseminates currency and suspicious transaction reports.

In May 2002, the RMI passed and enacted its Anti-Money Laundering Regulations, 2002. The 2002 Regulations provide the standards for reporting and compliance within the financial sector. Components of this legislation include reporting of beneficial ownership, internal training requirements regarding the detection and prevention of money laundering by financial institutions, record keeping, and suspicious and currency transaction reporting. Additionally, the Banking Commission and the Attorney General's office worked with the U. S. Government to develop a set of examination policies and an examination procedures manual. Both sets of documents are being used by examiners from the Banking Commission as guides in the on-site reviews of banks' and financial institutions' compliance with the anti-money laundering regulations. Since the establishment of the statutory and regulatory framework, the banking commission has conducted on-site examinations of financial institutions and cash dealers.

The Banking Commission has issued two sets of advisories on suspicious transaction reporting and currency transaction reporting. The advisories are accompanied by reporting forms and instructions that are similar to those used in the United States. Guidelines on customer due diligence and record keeping have also been issued to the industry, as a supplement to the advisories.

In September 2002, amendments were made to the anti-money laundering legislation. The first amendment was to remove the \$10,000 threshold for transaction record keeping. The original legislation stated that banks only had to keep the records of transactions that were over \$10,000.

Marshall Islands non-resident corporations (NRCs), the equivalent of international business companies, are of concern with respect to money laundering. By December 2000, there were reportedly 4,000 NRCs registered, half of which were companies formed for registering ships. Currently, there are 5,500 registered NRCs. NRCs are allowed to offer bearer shares. Corporate officers, directors, and shareholders may be of any nationality and live anywhere. NRCs are not required to disclose the names of officers, directors, and shareholders or beneficial owners, and corporate entities may be listed as officers and shareholders. Although NRCs must maintain registered offices in the Marshall Islands, corporations can transfer domicile into and out of the Marshall Islands with relative ease. Marketers of offshore services via the Internet promote the Marshall Islands as a favored jurisdiction for establishing NRCs. In addition to NRCs, the Marshall Islands offer non-resident trusts, partnerships, unincorporated associations, and domestic and foreign limited liability companies. Offshore banks and insurance companies are not permitted in the Marshall Islands.

Money Laundering and Financial Crimes

The substantial and comprehensive effort to align the Marshall Island's anti-money laundering regime with international standards, including the adoption of new laws, a new regulatory scheme, and the establishment of an FIU, resulted in its 2002 removal from FATF's NCCT list.

The Marshall Islands is not a signatory to the 1988 UN Drug Convention. As of September 2002, RMI has enacted a Proceeds of Crime Act, Counter-Terrorism Act, and Foreign Evidence Act but is not a signatory to the UN International Convention for the Suppression of the Financing of Terrorism nor of the Convention against Transnational Organized Crime, which is not yet in force internationally.

The Marshall Islands became a member of the Egmont Group of FIUs, as well as a member of the Asia/Pacific Group on Money Laundering in June 2002. RMI is also a founding member of the recently established Pacific Islands Financial Supervisors, a group of regulators from the Pacific Islands Forum countries that will be representing the region in the Basel group.

The GRMI should continue to enhance and implement its money laundering legislation and increase supervision of the offshore sector. In particular, the GRMI must effectively implement the laws and procedures it has put in place. If the Counter-Terrorism Act does not criminalize the financing of terrorists and terrorism, it should be amended to do so. The RMI should sign and ratify the UN International Convention for the Suppression of the Financing of Terrorism. Additionally, the GRMI should expand the record keeping, reporting and licensing requirements for all non-bank financial institutions.

Mauritius. Mauritius is a developing financial hub and a major route for foreign investments into the Asian sub-continent. Officials in Mauritius indicate that the majority of money laundering in Mauritius takes the form of schemes to purchase goods in other countries with illegal funds and selling the goods in Mauritius.

Money laundering is a criminal offense in Mauritius. On June 8, 2002, Mauritius approved the Financial Intelligence and Anti-Money Laundering Act, which replaced the Economic Crime and Anti-Money Laundering Act of 2000. The Financial Intelligence and Anti-Money Laundering Act provides for the establishment of a Financial Intelligence Unit (FIU) located within the Ministry of Economic Development, Financial Services, and Corporate Affairs. The FIU became operational on August 9, 2002. The Financial Intelligence and Anti-Money Laundering Act also imposes penalties on persons committing money laundering offenses; establishes suspicious activity reporting obligations for banks, financial institutions, cash dealers, and relevant professions; and provides for cooperation with the FIUs of other countries.

The FIU has the responsibility of collecting and analyzing suspicious activity reports (SARs), and forwards those reports to the Independent Commission Against Corruption (ICAC). The ICAC, set up in June 2002, has the power to investigate money laundering offenses. The ICAC also has the authority to freeze and seize the assets related to money laundering. The FIU is also working to develop the information technology structure to properly store the SARs.

In 2000, the Financial Action Task Force (FATF) conducted a review of Mauritius's anti-money laundering regime against the 25 specified criteria for evaluating non-cooperative countries and territories. After conducting the review, FATF did not designate Mauritius as a non-cooperative country.

Mauritius has an active offshore financial sector. In 2001, the Financial Services Development Act was passed. This Act established the Financial Service Commission (FSC), which performs the functions that were formerly carried out by the Mauritius Offshore Business Activities Authority (MOBAA). The FSC is responsible for licensing and regulating of non-banking financial services. All applications to form offshore companies must be reviewed by the FSC. Information on companies can also be requested from the FSC. Along with reviewing of applications, the FSC supervises activities of offshore companies.

The Prevention of Terrorism Act of 2002 was promulgated in Mauritius on February 19, 2002. This legislation criminalizes terrorist financing. Finally the legislation gives the Government of Mauritius

powers to track and investigate terrorist-related funds, property, and assets, and cooperate with international bodies.

Mauritius is a party to the 1988 UN Drug Convention. Mauritius has signed, but not yet ratified, both the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Mauritius is a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. In August 2002, representatives from Mauritius attended the ESAAMLG plenary and Ministerial Council Meeting in Swaziland, and volunteered for the first round of ESAAMLG mutual evaluations, scheduled to take place in 2003. Mauritius is a member of the Offshore Group of Banking Supervisors.

Mauritius should continue to work with ESAAMLG to strengthen the region's anti-money laundering regimes.

Mexico. The illicit drug trade continues to be the principal source of funds laundered through the Mexican financial system. Other crimes, including corruption, kidnapping, firearms trafficking, and immigrant trafficking, are also major sources of illegal proceeds. 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 or currency derived from illegal drug sales in the United States.

According to U.S. law enforcement officials Mexico remains one of the most challenging money laundering jurisdictions for the United States. While Mexico has taken a number of steps to improve its anti-money laundering system, significant amounts of narcotics related proceed are still smuggled across the border. In addition, such proceeds can still be deposited into the financial system through Mexican banks or casas de cambio, or repatriated across the border without record of the true owner of the funds. Furthermore, despite advances in international cooperation and information sharing it still remains difficult for U.S. law enforcement to obtain key financial records from Mexico and to extradite money laundering defendants. These problems have hampered a number of recent U.S. law enforcement initiatives.

The Government of Mexico (GOM) continues efforts at implementing an anti-money laundering program according to international standards such 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 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.

Regulations have been implemented for banks and other financial institutions (mutual savings companies, insurance companies, financial advisers, currency exchange houses, stock market, money remittance companies, and credit institutions) to know and identify customers, and maintain records of transactions. These entities must report transactions over \$10,000, transactions involving employees of financial institutions who engage in unusual activity, and "unusual transactions" to the Secretariat of Finance and Public Credit's (Hacienda) General Directorate for Investigations of Transactions (DGAIO), Mexico's financial intelligence unit (FIU).

Since 1998, the DGAIO has received over 30 million reports of "relevant transactions" averaging 500,000 per month, and since 1997, over 20,000 Suspicious Activity Reports (SARs), averaging 500 per month. Regulations effective in February 2001 extended reporting, record keeping, and customer identification requirements to non-bank financial institutions. Also in 2001, Mexico established suspicious transaction reporting requirements for the smaller foreign exchange houses that process most of the remittances from Mexican workers in the United States.

Money Laundering and Financial Crimes

The Special Unit to Combat Money Laundering (UECLD) of the Attorney General's Office was formally established on July 17, 2000, with authority to initiate, coordinate, and determine the appropriate preliminary inquiries in order to consign them to the judicial authorities and follow up the processes, as well as to seize the illicit proceeds. During 2001-2002, the UECLD initiated 131 preliminary inquiries, of which 69 have been consigned to the judiciary. It issued 130 arrests warrants and 24 condemnatory sentences involving 33 individuals, and seized 250,913,665 Mexican pesos, \$11,622,521, 1,000 Italian lira, and 1,000 Spanish pesetas. However, there continues to be a substantial lack of cooperation between the PGR and the Hacienda in money laundering investigations.

In August, investigators and prosecutors from the PGR and the Finance Ministry received training in investigative techniques and investigative task forces. It is anticipated that the use of the task force approach taught during this course will promote greater inter-agency cooperation.

In addition, FIU personnel have initiated working level relationships with federal law enforcement entities, including the PGR's Special Unit on Organized Crime (UEDO) and the Federal Investigative Agency (AFI), to support criminal investigations with ties to money laundering. Improved exchange of information among the FIU, financial institutions, and other government entities charged with money laundering investigations should facilitate successful prosecutions of criminals involved in money laundering.

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.

During 2001-2002, the GOP conducted operations in several ports of entry and departure, particularly at Mexico City International Airport where the following seizures were made: 833,027 Mexican pesos, \$8,854,545, 1,981,000 Colombian pesos, 10 pounds sterling, 110 guilders, 8,500 Taiwanese dollars, and 2,000 colons.

In addition, in December 2002, a Mexican court sentenced Jose Ocampo Verdugo to 17 years and six months in prison for money laundering. Authorities had arrested Ocampo, the owner of Caja Popular Puerto Vallarta, in November 1999, because he had laundered drug proceeds on behalf of the Amezcua drug trafficking organization. Also in December 2002, Mexican authorities charged Ivonne Sota Vega ("La Pantera") with money laundering for the Arrellano Felix Organization through the administration, purchase, and sale of real property.

Mexico has expanded its anti-money laundering legislation and developed a broad network of bilateral agreements with the United States, and regularly meets in bilateral law enforcement working groups with the United States. Nevertheless, United States requests to Mexico for the seizure, forfeiture, and repatriation of criminal assets have not met with success. Most recently, after a four-year delay, Mexico informed the United States that it would not be able to repatriate assets in an armored car robbery case in which the convicted criminal in the United States admitted that all the funds he deposited into an account in Mexico were funds he stole from the victim financial institution. United States efforts to obtain financial records have been unsuccessful, despite the existence of new agreements and mechanisms.

The GOM and the United States Government (USG) continue to 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 October 2001, the U.S. Customs Service and Mexico City entrepreneurs inaugurated a Business Anti-Smuggling Coalition (BASC) that includes the establishment of a financial BASC chapter created to deter money laundering.

In addition to its membership in the FATF, Mexico participates in the Caribbean FATF as a cooperating and supporting nation. Mexico is an observer member of the South American Financial Action Task Force (GAFISUD). Through membership and participation in the FATF and its regional subgroups, the

Egmont Group of FIUs and the OAS/CICAD Experts Group to Control Money Laundering, Mexico continues to expand its presence at international anti-money laundering fora. As current President of the OAS/CICAD Group of Experts to Control Money Laundering (2002-2003), in July 2002, Mexico hosted the XV meeting of the Group. The key accomplishment during this meeting was the subsequent approval by CICAD of the incorporation of the FATF Eight Special Recommendations on Terrorist Financing into the OAS Model Regulations on Money Laundering. The GOM is a party to the 1988 UN Drug Convention, and the 2000 United Nations Convention against Transnational Organized Crime, which is not yet in force internationally. In September 2000, the GOM signed the UN International Convention for the Suppression of the Financing of Terrorism. The GOM responded to USG efforts to identify and block terrorist-related funds. Although no assets were frozen, it continues to monitor suspicious financial transactions.

The GOM should improve the mechanisms and implementation for asset forfeiture and money laundering cooperation with the United States. The GOM should consider upgrades for computer hardware and of analytical software to enhance processing and analysis of suspicious transactions and reports of large value. The GOM should also criminalize terrorist financing. Furthermore despite the preventive mechanisms that have been put in place, improved cooperation among law enforcement authorities, and a strong public campaign against corruption, the GOM continues to face challenges in prosecuting and convicting money launderers and should continue to focus its efforts on improving its ability to investigate and prosecute money launderers.

Micronesia. The Federated States of Micronesia (FSM) is a sovereign state in free association with the United States. It is not a regional financial center. There have been no known money laundering schemes related to narcotics proceeds. Financial crimes, such as bank fraud, do not appear to be increasing in frequency. Contraband smuggling, centered on alcohol and tobacco products, may generate illicit proceeds. There may be limited financial crimes outside the formal banking sector by cash dealers involved in remittances to the home countries of some foreign workers.

There are three financial institutions in the country: Bank of Guam, Bank of the FSM, and the FSM Development Bank. The Bank of Hawaii closed its FSM branches in November 2002. The Bank of the FSM and the FSM Development Bank are local institutions. The Bank of the FSM is the only non-U.S. bank insured by the Federal Deposit Insurance Corporation (FDIC). The Bank of Guam is also FDIC insured. The FSM Banking Board performs "spot audits" on all the banks.

In December 2000, FSM enacted the Money Laundering and Proceeds of Crime Act (the Act). The Act went into effect July 1, 2001, and is codified as FSM Code, Title 11, Chapter 9. The Act criminalizes money laundering and provides for the freezing and seizure of assets. Predicate crimes include all serious offenses punishable by imprisonment of more than one year. The Act also provides for collection of financial information and intelligence, and international cooperation in money laundering matters. Micronesia began drafting implementing regulations for the Act in 2001. Legislation aimed at enhancing law enforcement cooperation with the United States and other countries in investigating serious crimes was enacted as the Mutual Assistance in Criminal Matters Act of 2000 (FSM Code, Title 12, Chapter 17). The law sets forth procedures for requesting assistance and responding to requests from other countries. Legislation to explicitly criminalize terrorist financing is pending.

FSM became a party to the UN International Convention for the Suppression of the Financing of Terrorism on September 23, 2002. The FSM Department of Justice has established a protocol for regular notification to the Banking Board of the names of suspected terrorist individuals and organizations. No assets of individuals or entities so designated have been seized or frozen.

FSM should continue to cooperate with the United States and regional groupings on money laundering and financial crimes. FSM should also continue to enhance its anti-money laundering regime by criminalizing terrorist financing and adopting and implementing the pending laws and regulations.

Moldova. Moldova is not considered an important regional financial center. Moldova's banking system is relatively new and is vulnerable to money laundering. There does not appear to be significant narcotics-related money laundering. However, there are reports that Russian crime groups purchase businesses in Moldova through which they launder illegal proceeds. The Moldovan economy is predominantly cash-based.

Moldova passed an anti-money laundering law in November 2001 and amended it on June 21, 2002. The law criminalizes money laundering for "all crimes" and requires banks and non-bank financial institutions to report suspicious transactions. Suspicious transactions are determined to be any transaction over \$7,200 for individual transactions, \$14,400 for wire transfers, and \$21,600 for transfers by a business. Travelers entering Moldova are required to complete a currency reporting form. Banks must maintain account and transaction records for five years. The law protects financial institutions against criminal, civil, and administrative liability arising from the reporting of suspicious transactions. Commercial banks can be held responsible for negligence if money laundering occurs in their institution.

The Office of the Prosecutor General has established a financial intelligence unit to initiate investigations based on suspicious transaction reports. There have been no arrests for money laundering.

In November 2001 Moldova passed the Law on Combating Terrorism, which criminalizes terrorist financing. Article 106 of the Moldovan criminal code, scheduled for enactment in January 2003, would give law enforcement authorities the ability to freeze and seize illicit funds.

Moldova became a party to the UN International Convention for the Suppression of the Financing of Terrorism on October 10, 2002. Moldova is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Moldova is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, formerly PC-R-EV), a FATF-style regional body.

Monaco. The Principality of Monaco is considered vulnerable to money laundering, because of its strict bank secrecy laws, extensive network of casinos and its unregulated offshore sector. Russian organized crime and the Italian Mafia reportedly have laundered money in Monaco.

There are approximately 70 banks and financial institutions in Monaco, with more than 300,000 accounts (with a population of about 5,000 Monegasque nationals and another 25,000 foreign residents). Approximately 85 percent of the banks' customers are non-resident.

Most of the banking sector is concentrated in portfolio management and private banking. The subsidiaries of foreign banks operating in Monaco can withhold customer information from the parent bank. Monaco also has an offshore sector, and permits the formation of both trusts and five different types of international business companies (IBCs): limited liability companies, branches of foreign parent companies, partnerships with limited liability, partnerships with unlimited liability, and sole proprietorships. However, ready-made "shelf companies" are not permitted. The incorporation process generally takes four to nine months. Monaco does not maintain a central registry of IBCs, and authorities have no legal basis for seeking information on the activities of offshore companies.

Money laundering in Monaco is a criminal offense. Banks, insurance companies, and stockbrokers are required 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. Another law imposes a five-to-ten-year jail sentence for anyone convicted of using ill-gotten gains to purchase property (which is itself subject to confiscation).

Monaco established its Financial Intelligence Unit, the Service d'Information et de Controle sur les Services Financiers (SICCFIN), to collect information on suspected money launderers. In 2000, the Financial Action Task Force criticized the anti-money laundering regime of Monaco for the insufficient resources provided to SICCFIN. According to a press report of November 2001, Monaco and France have reached an agreement on initiatives to counter money laundering in the principality. The French

Finance Ministry stated that SICCFIN had doubled the number of its staff, and that there had been a “noteworthy” increase in the number of suspicious activity reports being filed. In March 2002, Monaco and France signed a memorandum of understanding regarding the sharing of information between the securities regulatory commissions of the two countries, in connection with money laundering.

In January 2002, Monaco and Switzerland signed an agreement to cooperate with one another in the fight against money laundering. The agreement includes provisions for information exchange between the two countries. Later in the year Monaco signed similar agreements with Liechtenstein and Panama. In previous years Monaco had reached similar agreements with Luxembourg, France, Spain, Belgium, Portugal and the United Kingdom.

Monaco is a party to the 1988 UN Drug Convention. In June 2001 it submitted a notification indicating that it had ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. SICCFIN is a member of the Egmont Group of FIUs. Monaco became a party to the UN International Convention for the Suppression of the Financing of Terrorism in November 2001. In April and August 2002, Monaco promulgated Sovereign Orders to import into domestic law the international obligations it accepted when it ratified that Convention. In May 2002, Monaco acceded to the Council of Europe Convention on the Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. In July and August 2002, Monaco passed Act 1.253 and promulgated two Sovereign Orders, intended to implement UNSCR 1373 to criminalize terrorism and its financing.

Monaco’s actions to increase the resources of SICCFIN should increase the efficacy of Monaco’s anti-money laundering regime, particularly in the area of cooperation with SICCFIN’s foreign counterparts. Monaco should establish a central registry for IBCs, and grant SICCFIN the authority to obtain information on the activities of offshore companies.

Mongolia. Mongolia is not a financial center. Mongolia’s vulnerability to transnational crimes such as money laundering has grown with the country’s increased levels of international trade and tourism. Mongolia’s long unprotected borders with Russia and China make it particularly vulnerable to smuggling and narcotics-trafficking. Illegal money transfers and public corruption are other sources of illicit funds. Mongolia does not have anti-money laundering legislation. It also has been slow in establishing interagency coordination mechanisms to help monitor international financial transactions. Moreover, growing corruption, a weak legal system, an inability to effectively patrol its borders to detect smuggling, and lack of capacity to conduct transnational criminal investigations all hamper Mongolia’s ability to fight all forms of transnational crime.

Mongolia is not party to the 1988 UN Drug Convention. However, in recent years Mongolia has increased its participation in fora that focus on transnational criminal activities. For example, Mongolia has observer status in the Asia/Pacific Group on Money Laundering. Mongolia has signed, but not yet ratified, the UN International Convention for Suppression of the Financing of Terrorism.

Mongolia should pass anti-money laundering and terrorist financing legislation.

Montserrat. Montserrat is a Caribbean overseas territory of the United Kingdom. Volcanic activity between 1995 and 1998 reduced the population and business activity on the island, although an offshore financial services sector remains that may attract money launderers because of a lack of regulatory resources. As with the other British Caribbean overseas territories, Montserrat underwent an evaluation of its financial regulation in 2000, co-sponsored by the local and British governments.

Indeed the report highlighted the need to devote additional resources in order to properly supervise its offshore financial institutions. The government plans to use licensing revenues to help provide funding for additional supervisory resources but acknowledged that if it cannot dedicate the resources necessary to resolve the deficiencies noted in its report “it will recognize that there will be no option but to review its involvement in offshore finance.”

Montserrat’s offshore sector consists of approximately 15 offshore banks and approximately 22 international business companies (IBCs) and 30 Companies Act companies the majority of which engage

only in conducting local business. The Financial Services Centre (FSC) regulates offshore banks, whereas the Eastern Caribbean Central Bank (ECCB) supervises Montserrat's three domestic banks. IBCs may be registered using bearer shares, providing for anonymity of corporate ownership.

The Proceeds of Crime Act (POCA), 1999 criminalized the laundering of proceeds from any indictable offense and mandated the reporting of suspicious transactions to a Reporting Authority. However, the Reporting Authority has not yet been established. Although the Act directs the Governor to issue a code of practice establishing further regulations for financial institutions, the code of practice has not yet been issued. The government is planning to introduce captive insurance legislation that will require licensing and regulation, and until such legislation is enacted, there will be no offshore captive insurance industry. The government may also ask that the ECCB take over responsibility for supervising Montserrat's offshore banking sector as the ECCB has done in several other Caribbean jurisdictions.

U.S. law enforcement cooperation with Montserrat is facilitated by a treaty with the United Kingdom concerning the Cayman Islands relating to mutual legal assistance in criminal matters that was extended to Montserrat in 1991. Montserrat's current legislation, however, makes information exchange difficult between regulators and foreign authorities. Montserrat is a member of the Caribbean Financial Action Task Force (CFATF), and is subject to the 1988 UN Drug Convention.

Montserrat should issue regulations to implement the POCA and establish the Reporting Authority to act as a Financial Intelligence Unit that can share information with foreign authorities with appropriate safeguards. It should enact measures to identify and record the beneficial owners of IBCs and immobilize bearer shares. It should also increase resources to financial supervision, particularly in the area of on-site supervision, especially as it looks to expand its offshore sector, to help ensure that money launderers do not abuse Montserrat's financial services.

Morocco. Morocco is not a regional financial center and the extent of the money laundering problem in Morocco is not known. There have been reports of money laundering activities within the country related to international arms smuggling. Morocco remains an important producer and exporter of cannabis, with estimated revenues of \$3 billion. Some of these proceeds may be laundered in Morocco and abroad. Large numbers of Moroccans have a strong economic dependence on the narcotics trade. There is no indication that international or domestic terrorist networks have engaged in wide-spread use of the narcotics trade to finance terrorist organizations and operations in Morocco. There are reports that money may be laundered through bulk cash smuggling and the purchase of smuggled goods. Banking officials have indicated that the country's system of unregulated money exchanges provides opportunities for launderers. Morocco has offshore banks.

The Moroccan banking system is modeled after the French system and 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, which monitors and regulates the banking system. Bank Al Maghrib has decreed that all financial institutions must institute a customer identification policy and maintain specified transaction records.

As of January 2003, Morocco is moving towards the enactment of a single unified law to combat terrorism financing and money laundering. The legislation mandates specific reporting requirements by banks. It also designates the Central Bank as the country's lead financial enforcement entity and specifies investigative procedures. Morocco should enact legislation that adheres to world standards. Morocco is a party to the UN International Convention for the Suppression of Financing of Terrorism.

Mozambique. Mozambique is not a regional financial center. Most money laundering in Mozambique is related to bank fraud and corruption. However, lax oversight and weak banking regulations suggest that Mozambique's financial institutions are vulnerable to money laundering. In particular, there is growing concern that the proceeds of arms trafficking, stolen vehicles sales, narcotics-trafficking, prostitution, and contraband smuggling may be laundered through Mozambique's financial institutions.

Mozambique's non-bank financial sector, primarily comprised of exchange houses, may be susceptible to money laundering. In August 2002, an Indian national with connections to a Maputo exchange house was detained at an airport in Mozambique attempting to board a flight to Johannesburg with approximately \$1 million. He subsequently escaped from jail.

Mozambique's National Assembly passed an anti-money laundering law in December 2001, which was ratified by the Council of Ministers on February 5, 2002. As of the end of 2002, however, implementing regulations had not been drafted. The law extends the crime of money laundering to encompass predicate offenses beyond narcotics-trafficking to most other serious crimes. The law also allows for asset seizure and forfeiture and requires financial institutions to verify the identity of their customers, keep transaction records for at least 15 years, and report suspicious transactions. The law protects employees of financial institutions who cooperate with money laundering investigations and exempts such cooperation from bank and professional secrecy rules. The law also contains "banker negligence" provisions, which hold individual bankers responsible for money laundering.

Bankers have the right to refuse service to anyone who refuses to identify the beneficiary of an account. Judicial authorities are given the right to request account information from financial institutions and to gain access to computer records from banks, individuals, and companies that are suspicious. Judicial authorities also have the right to authorize the tapping of phone conversations as part of financial investigations.

Customs regulations require those entering or leaving the country with foreign currency or negotiable instruments in amounts greater than \$5,000 to file a report with Customs. Taking local currency out of the country is prohibited. In December 2002, South African authorities apprehended a Pakistani national attempting to cross the South Africa-Swaziland border with \$40,000 hidden under his clothing. He had traveled numerous times between South Africa and Mozambique.

The Government of Mozambique (GOM) has the authority to freeze and seize assets related to terrorist financing. The GOM has circulated the list of terrorist individuals and entities designated by the UN 1267 Sanctions Committee, as well as the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224.

Mozambique is a member of the Eastern and Southern Africa Anti-Money Laundering Group, a FATF-style regional body. Mozambique has signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism. Mozambique is a party to the 1988 UN Drug Convention. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Mozambique should implement its anti-money laundering law, establish a Financial Intelligence Unit, and criminalize terrorist financing.

Namibia. Namibia is not a regional financial center. Namibia has one government bank and six commercial banks. Of particular concern in Namibia is the smuggling of precious minerals and gems, the proceeds of which Namibian authorities think may be laundered through Namibian banking institutions.

Namibia has not criminalized money laundering. Banks are required to report suspicious transactions and to record and report the identity of customers engaging in large transactions. Bankers and other individuals making suspicious transaction reports are protected by law with respect to their cooperation with law enforcement authorities. Banks and other financial institutions are required to maintain records related to large transactions and make those records available to government authorities for use in narcotics-related and other criminal investigations.

Namibia is in the process of drafting an anti-money laundering law that would apply to bank and non-bank financial institutions. The law would criminalize money laundering and terrorist financing. It would also address cross-border currency reporting requirements and information sharing with foreign law enforcement authorities. Other aspects of the bill are still being considered.

Money Laundering and Financial Crimes

In August 2001, Namibia hosted the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) Task Force and Ministerial Council Meeting. Namibia served as the Chair of ESAAMLG from August 2001 until August 2002.

Namibia is not a party to the 1988 UN Drug Convention. On August 16, 2002, Namibia ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Namibia has signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism.

Namibia should pass a law that criminalizes money laundering and terrorist financing as part of a viable anti-money laundering regime, as it has committed to doing through its membership in ESAAMLG.

Nauru. Nauru is a small central Pacific Island nation with a population of approximately 10,600. It is an independent republic and an associate member of the British Commonwealth. The Republic of Nauru is an established “zero” tax haven, as it does not levy any income, corporate, capital gains, real estate, inheritance, estate, gift, sales, or stamp taxes. It is an offshore banking center with a number of weaknesses in its regulatory structures. The government-owned Bank of Nauru acts as the Central Bank for monetary policy but it has no regulatory function over offshore banks. Nauru’s legal, supervisory, and regulatory framework has provided significant opportunities over time for the laundering of the proceeds of crime.

In June 2000, the Financial Action Task Force (FATF) placed Nauru on the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering. The FATF, in its June 2000 report, cited several concerns, including excessive bank secrecy provisions, a lack of basic anti-money laundering regulations, and Nauru’s failure to criminalize money laundering. In July 2000, the U.S. Treasury Department issued an advisory to U.S. financial institutions, warning them to give enhanced scrutiny to all financial transactions originating in, or routed to or through Nauru, or involving entities organized or domiciled, or persons maintaining accounts in Nauru. In June 2001, FATF determined that Nauru had made insufficient progress toward remedying deficiencies in its anti-money laundering regime and warned that FATF would impose countermeasures by September 30, 2001 if Nauru failed to address such deficiencies.

In response to mounting international pressure, the Government of Nauru passed the Money Laundering and Proceeds Crime Act of 2001 (AMLA 2001) in August 2001. The AMLA 2001 requires financial institutions to maintain accounts in the name of the account holder, thus prohibiting anonymous accounts and accounts held in fictitious names. It also requires financial institutions to record and verify the identity of accountholders, to report suspicious activity, and to develop internal anti-money laundering policies and procedures. Section 33 of AMLA 2001 protects financial institutions from liability for reporting suspicious activity. The AMLA 2001 allows for the establishment of a Financial Institutions Supervisory Authority (FISA), with the authority to supervise financial institutions’ compliance with the AMLA 2001. The FISA will also be the recipient of reports of suspicious transactions filed by financial institutions. Thus far, FISA has not been formed and no suspicious transaction reports have been filed.

Finally, the AMLA 2001 provides for mutual assistance with respect to money laundering investigations. There were, however, limitations placed on compliance with foreign requests for assistance. Nauru may refuse to comply with a request if the action sought by the foreign authority is contrary to any provision of the Republic of Nauru Constitution, or would prejudice the national interest.

On September 7, 2001, FATF issued a press release recognizing the passage of the AMLA 2001. FATF, however, found the legislation to have several deficiencies, and urged Nauru to enact appropriate amendments by November 30, 2001 in order to avoid the application of countermeasures. On December 5, 2001, FATF called upon its members to impose countermeasures against Nauru because of Nauru’s failure to remedy deficiencies in its anti-money laundering regime. Countermeasures may include heightening requirements on financial institutions to identify their customers and expanding suspicious activity reporting, among other measures. On December 6, 2001, Nauru amended the AMLA 2001 to

address certain deficiencies in the original act, including clarifying that the law applies to all financial institutions incorporated under the laws of Nauru (as opposed to just financial institutions conducting business within Nauru), and by broadening the definition of money laundering. Despite the passage of anti-money laundering legislation with amendments, there is a lack of a legal framework and effective regime for the regulation and supervision of offshore banks.

In January 2002, the U.S. Treasury Department supplemented its previously issued advisory by reminding U.S. banks and other financial institutions of their obligations under the newly enacted Section 313 of USA PATRIOT Act of 2001 concerning correspondent accounts with foreign shell banks. Under this new law, U.S. financial institutions, as well as other financial institutions operating in the United States, are required to terminate any U.S. correspondent accounts provided to foreign shell banks, and they must take reasonable steps to ensure that correspondent accounts held by foreign banks are not being used to provide U.S. banking services indirectly to foreign shell banks.

On Friday, December 20, 2002, the Secretary of Treasury, after consultation with the Departments of Justice and State, as well as other concerned U.S. government agencies, designated Nauru as a jurisdiction of “primary money laundering concern” under section 311 of the USA PATRIOT Act (the Act). In the announcement, the U.S. Treasury published a list of 161 banks licensed by the Republic of Nauru, the majority of which are believed to be shell banks. Under the Act, once a jurisdiction has been designated as a “primary money laundering concern” there are five special measures that can be imposed, either individually or jointly in any combination. In the announcement, U.S. Treasury proposed invocation of special measure five, requiring U.S. financial institutions to close payable-through or correspondent accounts involving the designated country.

The Government of Nauru has cooperated with officials from the United States and other countries in certain criminal investigations involving Nauruan institutions. Nauru recently joined the United Nations. Nauru has observer status within the Asia/Pacific Group on Money Laundering. Nauru has signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism. Nauru has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Nauru continues to remain on the FATF NCCT list, having failed to address the vulnerabilities to its offshore sector. Nauru’s government should act immediately to abolish its offshore banking sector, which, because it consists primarily of shell banks, cannot be adequately supervised to ensure that it is not exploited by transnational criminal elements. Nauru must pass and enact banking regulations to bolster its AMLA 2001. Nauru must set up its Financial Institutions Supervisory Authority and begin accepting suspicious transaction reports, as set out in the AMLA 2001. Nauru should criminalize the financing and support of terrorists and terrorism.

Nepal. Nepal is not a regional financial center and there are no indications that Nepal is used as an international money laundering center. The Government of Nepal (GON) has not criminalized money laundering and legislation on money laundering, mutual legal assistance and witness protection, developed as part of the GON’s Master Plan for Drug Abuse Control, remained stalled in 2002. Banks are not required to record the identity of customers engaging in significant transactions. However, any Nepalese citizen who wishes to open a foreign currency account must obtain a license to do so from the National Bank (NRB), and Nepalese citizens wishing to take currency overseas must obtain a letter of credit from a bank recognized by the NRB. The NRB has the authority to seize any assets that it determines to be the proceeds of illegal activity. Nepal has explored the development of an offshore sector.

The hawala system (hundi in Nepal), in which illegal proceeds are laundered through alternative informal remittance systems, is widespread. There have been no significant initiatives to regulate the system in Nepal. In Nepal, hundi is linked to the issues of capital flight, tax avoidance, and corruption. Reportedly, efforts to provide transparency in hawala transactions in foreign jurisdictions have resulted in the increased use of regulated financial institutions in Nepal.

Money Laundering and Financial Crimes

Nepal is not a signatory to the UN International Convention for the Suppression of the Financing of Terrorism. No suspect assets belonging to entities on UN list 1267 have been identified in Nepal. Nepal is a party to the 1988 UN Drug Convention.

Nepal should enact anti-money laundering and counter-terrorist finance legislation and develop a comprehensive anti-money laundering regime that would require the mandatory filing of suspicious transaction reports, and establish a financial intelligence unit. The GON should also initiate training for law enforcement and customs agencies to enable them to recognize and investigate money laundering.

Netherlands Antilles. The Aruba, which has autonomous control over its internal affairs, is a part of the Kingdom of the Netherlands. The Netherlands Antilles is comprised of Curacao, Bonaire, the Dutch part of Sint Maarten/St. Martin, Saba, and Sint Eustatius. The Government of the Netherlands Antilles (GONA) is located in the capital of Curacao, Willemstad, which is also the financial center of the five islands. There is a lack of border control between Sint Maarten and St. Martin that creates opportunities for money launderers.

The Netherlands Antilles has a significant offshore financial sector with 39 international banks and approximately 50 trust companies providing financial and administrative services to their international clientele, including 18,750 international companies, mutual funds, and international finance companies. The law and regulations on bank supervision state that international banks must have a physical presence on the island and hold records there. The Central Bank supervises the international banks. Authorities in other countries supervise some mutual funds. International corporations may be registered using bearer shares. It is the practice of the financial sector in the Netherlands Antilles to maintain copies of bearer share certificates for international corporations, which include information on the beneficial owner, either with the bank or the company service providers. There is a proposal to require that the name of the ultimate beneficial owner of the bearer share be recorded in a registry and made accessible to law enforcement officials upon a treaty-based request for the information.

Onshore banks are increasingly using their discretionary authority to protect themselves against money laundering. The largest commercial bank has lowered its limits on moneygrams from \$10,000 to \$2,000. Banks are reluctant to do business with the Internet gaming providers, provoking complaints from that sector.

Money laundering is a crime. 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. It is sufficient to establish that the money launderer knew, or should have known, of the money’s illegal origin. In 2000, the National Ordinance on Freezing, Seizing, and Forfeiture of Assets derived from crime went into effect. The law allows the prosecutor to seize the proceeds of any crime once the crime is proven in court.

Over the past couple of years, the GONA has taken steps to strengthen its anti-money laundering regime by expanding suspicious activity reporting requirements to gem and real estate dealers; enhancing the possibilities of freezing, seizing, or the forfeiture of criminal assets; 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 penalized currency and securities transaction, by including the use of valuable goods. In 2002, the largest money laundering case took place in Aruba and is still pending before the courts.

In 2002 a new ordinance, called the “National Ordinance on the Supervision of Fiduciary Business,” instituted a Supervisory Board that oversees the international financial sector. The GONA plans to bring the supervision of this sector under the Central Bank’s supervisory authority. At the same time, GONA subjected the members of this sector to “know-your-customer” rules. Also in May 2002 cross-border currency reporting legislation came into force. The law specifies reporting procedures for an individual bringing in or taking out more than NAF 20,000 (approximately \$11,000) in cash or bearer instruments. In

July, an individual traveling from Puerto Rico and carrying \$193,000 in a suitcase, destined for the free trade zones, was arrested for failing to declare the cash under this new law.

A legislative proposal giving the Central Bank authority to supervise the mutual fund sector is expected to go into effect as early as January 2003. The free trade zones are minimally regulated; however, administrators and businesses in the zones have indicated an interest in receiving guidance on detecting unusual transactions. This guidance is expected to be prepared in early 2003.

Unusual transactions are by law reported to the Financial Intelligence Unit called the Netherlands Antilles Reporting Center, Meldpunt Ongebruikelijke Transacties (MOT NA). As of November 21, 2002, the MOT NA had received 25,323 unusual transaction reports, and the unit analyzed and disseminated 781 unusual transaction reports to authorities. The number of reports received is a sharp increase over the 7,700 reported in 2001 and reflects additional indicators, an expansion in reporting institutions and a backlog in processing.

The current staff of the MOT NA continues to work diligently to enhance the effectiveness and efficiency of its reporting system. In 2002, the MOT NA had a staff of five, an increase from a fluctuating two-four in 2001; in 2003 the staff is expected to increase by another five members. Significant progress has been made in automating suspicious activity reporting; in 2002 reporting institutions sent 99.2 percent of their reports to the MOT NA electronically. One hundred percent of the dissemination is now done on-line, and soon most of the matches with external databases will be done electronically. The MOT NA has issued a manual for casinos on how to file reports and has started to install the software in the casinos, which will allow the reports to be submitted electronically.

On October 18, 2002, the GONA published new indicators for the reporting of unusual transactions with regard to terrorism financing. The new indicators require that unusual transactions reported to the police or judicial authorities in connection with money laundering or the financing of terrorism must also be reported to the MOT NA. This requirement also extends to unusual transactions relating to credit cards and money transfers, as well as to unusual transactions with regard to game of chance transactions.

The MOT NA is an active member of the Egmont Group. Netherlands Antilles law allows the exchange of information between the MOT NA and foreign Financial Intelligence Units by means of memoranda of understanding (MOUs) and by treaty. In 2002 the MOT NA received 32 requests for information on 782 subjects. The MOT NA issued eight requests for information on 25 subjects. The MOT NA's policy is to answer requests within 48 hours after receipt. However, the large lists of terrorist inquiries have presently forced the MOT NA to an average answering time of eight days.

In January 2002, the GONA enacted legislation allowing a judge or prosecutor to freeze assets related to the Taliban cum suis and Usama Bin Ladin cum suis (cum suis means that all companies and persons connected with Usama Bin Ladin are included.). 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 that were 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.

As part of the Kingdom of the Netherlands, the Netherlands Antilles participates in the Financial Action Task Force (FATF). It is a member of the Caribbean Financial Action Task Force (CFATF). In 1999, the Netherlands extended application of the 1988 UN Drug Convention to the Netherlands Antilles. The Kingdom of the Netherlands, of which the Netherlands Antilles is a part, signed the International Convention for the Suppression of the Financing of Terrorism on January 10, 2000. In accordance with Netherlands Antilles law, which stipulates that all the legislation must be in place prior to ratification, the Government of the Netherlands Antilles is preparing legislation which will enable the Netherlands Antilles to ratify the Convention. The Netherlands's Mutual Legal Assistance Treaty with the United States also applies to the Netherlands Antilles. With regard to requests for assistance relating to fiscal offenses addressed to the Netherlands Antilles, an agreement was signed in April 2002 between the

Money Laundering and Financial Crimes

Netherlands, and the United States, which is also applicable to the Netherlands Antilles, for the exchange of information with respect to taxes. This agreement is scheduled to come into force on January 1, 2004.

The Government of the Netherlands Antilles has shown a commitment to combating money laundering by establishing a solid anti-money laundering program. An increase to the MOT staff is particularly notable. The GONA should criminalize the financing of terrorists and terrorism, and its focus should continue on increasing regulation and supervision of the offshore sector and free trade zones and pursuing money laundering investigations and prosecutions.

The Netherlands. The Netherlands is a major regional financial center and as such is vulnerable to the laundering of funds generated from a variety of illicit activities, including narcotics-trafficking and financial fraud. Money laundering in the Netherlands is most likely controlled by major drug cartels and other international criminal organizations. The Netherlands' Security Service investigates terrorist financing, and is cooperating with law enforcement entities that are experienced in this area.

In 1994, the Netherlands criminalized money laundering related to all crimes, although prosecutors first had to prove the predicate offense before prosecuting for money laundering. In 2002, legislation was enacted making money laundering a separate offense, easing somewhat the government's burden of proof regarding the criminal origins of proceeds. Under the new law, the government needs only to prove that the proceeds "apparently" originated from a crime.

All financial institutions in the Netherlands, including banks, bureaux de change, and credit card companies, are required to report cash transactions over 2,000 euros (approximately \$2,000), as well as any less substantial transaction that appears unusual, 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 commercial dealers of high-value goods. The reporting requirements are expected to be expanded in mid-2003 to include trust and service company providers, notaries, lawyers, real estate agents, accountants, tax advisors. Under the Identification of Services Act (WID), all those that are subject to reporting obligations must identify their clients, either at the time of the transaction or at some point prior to the transaction, before providing financial services.

Financial institutions are also required by law to maintain records necessary to reconstruct financial transactions for at least five years and to respond quickly to government requests for information in narcotics-related cases. The requirements also have been applicable to the Central Bank of the Netherlands (to the extent that it provides covered services) since 1998. 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.

Since 1996, entities providing commercial services, such as accountants, lawyers, and notaries, have applied money laundering reporting procedures within their professions. The competent authorities have established unusual activity and transaction indicators in preparation for the implementation of the 2001 amendment to the EU Directive on Money Laundering, which will enable trust and service company providers, notaries, lawyers, real estate agents, accountants, tax advisors to report unusual transactions.

The Money Transfer and Exchange Offices Act, which was enacted in June 2002, 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.

The MOT reviews and analyzes the unusual transactions and cash transactions filed by banks and financial institutions. It forwards suspicious transaction reports with preliminary investigative information to operational law enforcement agencies and to the office for operational support of the National Public Prosecutor for MOT cases (BLOM). In 2001, the last year for which complete figures are available, the MOT recorded 76,085 unusual transactions in its database, of which it forwarded 20,233 as suspicious. In order to facilitate the forwarding of suspicious transactions, the MOT and BLOM created an electronic

network called Intranet Suspicious Transactions. Also, a website for the actual reporting of unusual transactions by financial institutions was developed, thus completing the electronic infrastructure. Furthermore, the MOT receives data from the Public Prosecution Service/Criminal Asset Deprivation Bureau and cross checks it in the MOT database. Suspicious transaction reports with matching data from the Criminal Asset Deprivation Bureau are disseminated to the BLOM.

In 2002, the “Sanction Provision for the Duty to Report on Terrorism” became effective. This new ministerial decree requires financial institutions to report all transactions (actually carried out or intended) that involve persons, groups, and entities that have been linked, both domestically and internationally, with terrorism, to the MOT. Terrorist financing is a crime in the Netherlands.

The MOT is a member of the Egmont Group of FIUs. It is also involved in efforts to expand cooperation between disclosure offices, particularly within the EU. The Netherlands is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime. The Dutch participate in the Basel Committee, and have endorsed the Committee’s “Core Principles for Effective Banking Supervision”. In February 2002, the Netherlands became a party to the UN International Convention for the Suppression of the Financing of Terrorism. The Netherlands has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. The Netherlands is a member of the Financial Action Task Force (FATF) and participates in the Caribbean Financial Action Task Force (CFATF) as a Cooperating and Supporting Nation. The Netherlands is also a member of the Dublin Group, and chairs its Central European Regional Group. There is a Mutual Legal Assistance Treaty in effect between the Netherlands and the United States, as well as an Agreement regarding Mutual Cooperation in the Tracing, Freezing, Seizure and Forfeiture of proceeds and Instrumentalities of Crime and the Sharing of Forfeited Assets.

In the past two years, a group of European FIUs (the United Kingdom, France, Italy, Luxembourg, and the Netherlands) developed a network system called FIU NET for international information exchange. The task force that manages this process is chaired by the head of the MOT.

Since March 2002, the MOT has been the main contractor for the European Commission in a Anti-Money Laundering Project for the PHARE (Economic Reconstruction Assistance to Estonia, Latvia, Lithuania, Poland, the Czech Republic, Slovakia, Hungary, Slovenia, Romania, Bulgaria, Cyprus, and Malta) program. The purpose of the project is to provide support to Central and Eastern European countries in the development and/or improvement of anti-money laundering regulations. For this purpose, the MOT has established a project team of six persons. In addition to the team, there is a consortium of international experts. The PHARE Anti-Money Laundering Project will continue until December 25, 2003.

The Netherlands has a comprehensive anti-money laundering regime.

New Zealand. New Zealand is not a major regional or offshore financial center. It has a small number of banks and financial institutions whose operations can be effectively monitored by government authorities. There is evidence that some money laundering does take place, although not to a significant extent. Narcotics proceeds and commercial crime are the primary sources of illicit funds. International organized criminal elements do operate in New Zealand.

A 1995 amendment to New Zealand’s Crimes Act 1961 criminalized the laundering of proceeds knowingly derived from a serious offense. The Financial Transaction Reporting Act 1996 contains obligations for a wide range of financial institutions, including banks, credit unions, casinos, real estate agents, lawyers, and accountants. These entities must identify clients, maintain records, and report suspicious transactions. The Act also contains a “safe harbor” provision and requires the reporting of large cross-border currency movements.

The Terrorism Suppression Act, enacted in October 2002, criminalized terrorist financing. This Act also made the necessary changes to the existing law to enable New Zealand to ratify the UN International

Money Laundering and Financial Crimes

Convention for the Suppression of the Financing of Terrorism on November 4, 2002. The Act gives the government wider authority to designate entities as terrorist organizations and freeze their assets. The Prime Minister is responsible for making the designation upon a recommendation prepared by the New Zealand Police. Once the designation is made, the New Zealand Police informs banks and other appropriate parties. A public notice is also published. The Police are currently developing additional procedures to implement the provisions of the Terrorism Suppression Act.

New Zealand has consistently implemented financial controls against entities included on the UN 1267 Sanctions Committee consolidated list. It has not yet identified in New Zealand any assets from these entities.

New Zealand and the United States do not have a Mutual Legal Assistance Treaty. However, New Zealand legislation applies certain provisions of the Mutual Assistance in Criminal Matters Act 1992 unilaterally to the United States. In practice, New Zealand and U.S. authorities have had a good record of cooperation and information sharing in this area.

New Zealand is a party to the 1988 UN Drug Convention, and in July 2002, ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. New Zealand is a member of the Financial Action Task Force, the Asia/Pacific Group on Money Laundering (APG), and the Pacific Islands Forum. Its Financial Intelligence Unit is a member of the Egmont Group. The New Zealand government has played a leadership role in promoting efforts to combat money laundering in the South Pacific region, providing substantial amounts of technical assistance and training.

New Zealand has established a comprehensive anti-money laundering regime. It should build upon this base by continuing its implementation of its Terrorism Suppression Act. Additionally, New Zealand should continue its recognized leadership in the international arena.

Nicaragua. While Nicaragua is not a regional financial center, Nicaragua's status as a drug transit zone and its highly vulnerable banking system make the country an attractive target for narcotics-related money laundering.

The Government of Nicaragua (GON) has pledged to fight terrorism, money laundering, and narcotics-trafficking. However, resource constraints and corruption complicate efforts to counter these threats. Between August 2000 and 2001, four of Nicaragua's eleven banks failed amid allegations of fraud and mismanagement. Nicaragua suffers generally from economic instability, weak regulation, and lax oversight of its financial system.

Nicaragua's Law 177 of 1994 criminalized money laundering related to narcotics-trafficking and other illicit activities. Law 285 of 1999 reformed Law 177 and requires banks to report cash deposits that exceed \$10,000 to the Bank Superintendency, which forwards these reports for analysis to the Commission of Financial Analysis (CFA) within the National Anti-Drug Council. Though not a Financial Intelligence Unit, the CFA is assigned responsibility for detecting money laundering trends, coordinating with other investigative agencies, and reporting its findings to the National Anti-Drug Council. On paper, the CFA is composed of representatives from various elements of law enforcement and banking regulators, but in practice the CFA is not operational.

Law 285 prohibits anonymous accounts and requires financial institutions to identify customers and maintain transaction records for five years. Law 285 also requires travelers entering the country to declare cash, monetary instruments, or precious metals exceeding \$10,000 or its foreign equivalent. Law 285's implementing measure, Decree 74, requires that financial institutions report all complex, unusual, and significant transactions, and transactions with no apparent legal purpose, to the Bank Superintendency and to the CFA.

Currently, there is a new law that has been put before the Nicaraguan National Assembly establishes money laundering as an autonomous crime (the previous law was ambiguous in a way that allowed some to argue that only money laundering connected to illicit drug activity was illegal) and requires more stringent reporting of large or suspicious bank deposits. The new legislation also sets up a Commission of

Financial Analysis that will conduct both analysis and investigations. The law is expected to be enacted in 2003.

During the past year, the GON has pushed a strong anti-corruption campaign. Several prominent figures from the previous administration have been arrested and provisionally convicted for corruption and money laundering. Other major figures are now using parliamentary immunity to avoid facing money laundering charges in local courts.

Nicaragua is a party to the 1988 UN Drug Convention, and has ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Nicaragua is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Nicaragua has signed the Central American Treaty for the Prevention and Repression of Money and Asset Laundering Related to Illicit Activities Connected with Drug Trafficking and Related Crimes. Nicaragua also became a party to the UN International Convention for the Suppression of the Financing of Terrorism on November 14, 2002. Nicaragua ratified the OAS Mutual Legal Assistance Convention in 2002. Nicaragua was reinstated to the Caribbean Financial Action Task Force (CFATF) in 2002 after having been suspended due to a lack of participation.

The GON should begin allocating resources and developing technical expertise for complete operation of the CFA in order to strengthen its financial systems against money laundering and terrorist financing and ensure compliance with relevant anti-money laundering controls. The GON also should take a more active stance vis-à-vis the international community, which could provide useful support and anti-money laundering training.

Niger. Niger is not a regional financial center. While there are criminal activities that take place within the region, there is no evidence to suggest that money laundering activities take place on a large scale within Niger. Seven small commercial banks and one modest-sized local bank operate in Niger. Black market currency exchanges operate freely and currency easily flows unregulated through Niger's porous borders. Most economic activity takes place in the informal sector.

The Central Bank of West African States (BCEAO), based in Dakar, Senegal, is the Central Bank for the countries in the West African Economic and Monetary Union (WAEMU): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal, and Togo, all of which use the French-backed CFA franc currency. All bank deposits over approximately \$7,700 made in BCEAO member countries must be reported to the BCEAO, along with customer identification information. In September 2002, the WAEMU Council of Ministers, which oversees the BCEAO, issued a directive requesting that each member country set up a national committee under their Minister of Finance to deal with financial information as it relates to money laundering. The BCEAO would be in charge of coordinating such committees. Each member country is now responsible for putting legislation in place to implement this directive, and the legislation is expected to be harmonized regionally.

Although currently there are no legal requirements to do so, banks in Niger report suspicious activity to the BCEAO and to local law enforcement. In 2002, one bank account in Niger was frozen due to its relationship to illegal financial activity.

The WAEMU Council of Ministers issued another directive in September 2002 requesting member countries to pass legislation requiring banks to freeze the accounts of any persons or organizations targeted by the UNSCR 1267/1390 consolidated list.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA), based in Dakar, Senegal. In November 2002, GIABA hosted an anti-money laundering seminar for representatives of 14 ECOWAS members, including Niger. In July 2002, Niger participated in the 2002 West African Joint Operation Conference (WAJO) that promotes regional law enforcement cooperation against drug trafficking, terrorism, and money laundering.

Niger is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Niger is a member of the West African Economic and Monetary Union (WAEMU).

Niger should criminalize money laundering and terrorist financing. Niger should also make suspicious transaction reporting mandatory.

Nigeria. The Federal Republic of Nigeria is the most populous country in Africa and is West Africa's largest economy. Nigeria is a hub of trafficking in persons, narcotics-trafficking, and criminal financial activity for the entire continent. Nigerian trafficking and money laundering organizations have proven adept at devising new ways of subverting international and domestic law enforcement efforts and evading detection. This success in avoiding detection and prosecution has led to an increase in financial crimes of all types, including bank fraud, real estate fraud, identity theft, and advance fee fraud. Despite the efforts of the government to counter years of rampant corruption, crime continues to plague Nigerians.

Advance fee fraud is a lucrative financial crime that generates for criminals hundreds of millions of dollars in illicit profits annually. Initially Nigerian criminals made advance fee fraud infamous; recently nationals of many African countries and from a variety of countries around the world have begun to perpetrate it. This type of fraud is referred to internationally as "Four-One-Nine" fraud (419 is a reference to fraud section in Nigeria's criminal code). While there are many variations, the main goal of 419 fraud is to trick victims into payment of an advance fee by persuading them that they will receive a very large benefit in return. These "get rich quick" schemes have ended for some victims in monetary losses, kidnapping, or murder. Businesses and individuals around the world have been and continue to be targeted by perpetrators of 419 fraud, often via the Internet.

In the past, attempts to prosecute narcotics and money laundering cases have been hampered by an ineffective judicial system and widespread government corruption. Nigeria was ranked 101st out of 102 on Transparency International's 2002 Corruption Perceptions Index.

In June 2001, the Financial Action Task Force (FATF) placed Nigeria on the list of Non-Cooperative Countries and Territories (NCCT) in combating money laundering. Among the deficiencies cited by FATF were the failure to criminalize money laundering for offenses other than those related to narcotics, the lack of customer identification requirements for over-the-counter transactions under a threshold of \$100,000, inadequate suspicious transaction reporting requirements, the absence of anti-money laundering measures applied to stock brokerage firms and other financial institutions, and the high level of government corruption. In April 2002, FinCEN, the U.S. Financial Intelligence Unit, 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.

In June 2002, FATF stated that it would consider recommending countermeasures against Nigeria at its October 2002 plenary if Nigeria did not engage with the FATF Africa Middle East Review Group and move quickly to enact legislative reforms that addressed FATF concerns. In October, noting that the Government of Nigeria (GON) had begun to take legislative action, FATF recommended countermeasures against Nigeria if the GON did not enact sufficient legislative reforms by December 15, 2002.

On December 14, 2002, the National Assembly of Nigeria passed three pieces of anti-money laundering legislation. President Obasanjo signed the legislation into law the same day. The first piece of legislation—"An Act to Amend the Money Laundering Act 1995 and for Matters Connected Therewith"—requires customer identification for over-the-counter transactions over \$5,000, and specifies penalties for failure to comply. Under the law, financial institutions must report cash transactions that exceed one million naira (approximately \$8,800) for individuals and five million naira (approximately \$45,000) for corporate bodies. The amendment also criminalizes money laundering for all crimes. The second piece of legislation—an amendment to the Banking and Other Financial Institutions Act (BOFI)—expands anti-money laundering measures to cover stock brokerage firms and foreign currency exchange facilities. The BOFI amendment

also gives the Central Bank greater authority to freeze suspicious accounts and to deny bank licenses. Finally, “An Act to Provide for the Establishment of a Commission for Economic and Financial Crimes and for Matters Connected Therewith” (Financial Crimes Commission Act) establishes the Financial Crimes Commission (FCC)—a Financial Intelligence Unit that will coordinate anti-money laundering investigations and information sharing. The FCC will have the authority to share information with the Financial Intelligence Units of other countries. The Financial Crimes Commission Act criminalizes terrorist financing.

Nigeria is a party to both the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Nigeria has signed, but is not yet a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

The United States and Nigeria signed a Mutual Legal Assistance Treaty (MLAT) in 1989, 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.

The GON should create the FCC and ensure that it is adequately staffed and funded. Nigeria should enact legislation that requires financial institutions to report suspicious transactions regardless of whether the financial institution decides to carry out the transaction. The GON should continue to engage with FATF to ensure that Nigeria’s remaining anti-money laundering deficiencies are corrected so that Nigeria has a viable anti-money laundering regime that comports with all international standards and is capable of sharing information with foreign regulatory and law enforcement agencies globally.

Niue. Niue is a self-governing parliamentary democracy in the South Pacific that maintains a free association with New Zealand. Niueans are citizens of New Zealand and are part of the British Commonwealth.

Concerns were raised in the past about Niue’s vulnerability to money laundering. Legislation from the mid-1990s created an offshore financial center heavily dependent upon international business companies (IBCs). In addition, a small number of offshore banks were licensed. Niue also offers trusts, partnerships, financial management, and insurance services. Niue allows the creation of asset protection trusts that are impervious to many types of legal claims arising in other jurisdictions. In addition, trusts in Niue are exempt from taxation if the parties to the trust are not residents of Niue.

The International Business Companies Act of 1994 is the legislative basis for establishing IBCs. Marketers of offshore services promote Niue as a favored jurisdiction for establishing IBCs for a variety of reasons. Niue does not require the disclosure of beneficial ownership of IBCs, permits bearer shares, allows the marketing of shelf companies, and does not require IBCs to keep a register of directors. Internet marketers also offer shelf companies complete with associated offshore bank accounts and mail-drop forwarding services. Regardless of how the IBCs are marketed, all are legally formed and registered by a Panamanian law firm on behalf of Niue.

In June 2000, the Financial Action Task Force (FATF) placed Niue on the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering because of numerous deficiencies in Niue’s anti-money laundering regime. In particular, the report cited deficiencies in customer identification requirements, and concerns that the structure and effectiveness of the regulatory regime for offshore financial institutions and IBCs were inadequate. Following the FATF exercise, the U.S. Treasury Department issued an advisory to United States financial institutions advising them to give enhanced scrutiny to all financial transactions involving Niue.

The Proceeds of Crime Act 1998 criminalizes the laundering of proceeds from any offense punishable by at least one year in prison. Under the Proceeds of Crime Act, financial institutions may report suspicious transactions either to the police or to the Attorney General. However, there have been no such reports, and there are not relevant procedures in place to deal with their possible collection and analysis.

Money Laundering and Financial Crimes

Niue enacted the Financial Transactions Reporting Act (FTRA) in November 2000. The FTRA imposes reporting and record keeping obligations upon banks, insurance companies, securities dealers and futures brokers, money services businesses and persons administering or managing funds on behalf of IBCs. Specifically, the FTRA requires financial institutions to report suspicious transactions, verify the identity of its customers, and keep records of financial transactions for six years. However, the Act contains a number of loopholes that result in inadequate customer identification requirements, among other deficiencies. For example, section 11 of the FTRA requires that financial institutions verify the identity of customers who wish to conduct a transaction. Subsection 11(2) provides a loophole in that a financial institution dealing with an intermediary need establish the identity of the underlying customer only if the transaction exceeds \$10,000.

The FTRA also calls for the establishment of a Financial Intelligence Unit (FIU) within the office of the Attorney General. The FIU has still not been established. Niuean officials have said that the establishment of the FIU will depend upon the outcome of ongoing discussions among the Pacific Islands Forum of a proposed regional FIU for Forum member countries. Niue supports the establishment of a regional FIU to share information among Pacific Island states.

In June 2002, Niue brought into force the International Banking Repeal Act. This Act eliminated Niue's offshore banks. As a result, all offshore banking licenses have been terminated. In addition, Niue now maintains in country a mirror of the IBC registry kept in Panama. All company registration information is kept on island by a registered agent and is accessible to appropriate officials.

Due to these reforms, the FATF decided in October 2002 that Niue has in place an anti-money laundering system that generally meets international standards. Niue was therefore removed from the NCCT list. The U.S. Treasury Department subsequently withdrew its June 2000 advisory to U.S. financial institutions Niue.

Niue is not a member of the United Nations. In November 2001, the government amended the United Nations Act 1946 so as to enable the Cabinet to promulgate regulations giving effect to UN Security Council resolutions. The government of Niue is reviewing its legislation to comply with UN Security Council Resolution 1373. This will include making terrorist financing a criminal offense and authorizing the freezing of assets or accounts. Niue is a member of the Asia/Pacific Group on Money Laundering.

In 1998, Niue passed the Mutual Assistance in Criminal Matters Act, which authorizes the Attorney General of Niue to provide certain types of legal assistance to other countries involved with criminal investigations. Niue has no bilateral cooperation agreements with other countries for the exchange of information on money laundering, though the government has expressed a willingness to cooperate with international efforts to combat money laundering.

Niue should continue to enhance its anti-money laundering legislation. Recent reforms address some of the deficiencies in Niue's anti-money laundering regime; however, the government must finalize and promulgate the necessary regulations to bring the legislation into full force, including the establishment of a FIU. Niue must ensure that the recently enacted reforms are fully and effectively implemented. Additionally, Niue should criminalize terrorist financing.

Norway. Norway is not an important regional financial center; there are 19 commercial banks in the country and approximately 125 savings banks. Money laundering in Norway is related mainly to funds generated by the smuggling of liquor and cigarettes and takes place outside its financial system. However, structuring of deposits still appears to be a problem within the financial system. According to Oekokrim, which serves as Norway's Financial Intelligence Unit, Norway has been experiencing an increase in financial crime such as bank fraud. These types of crimes overshadow narcotics-related money laundering in Norway.

The Norwegian Penal Code includes many criminal offenses as predicates to money laundering. Current money laundering statutes require financial institutions to report large and suspicious transactions to Oekokrim, to verify the identity of their customers, and to keep records of transactions for at least five

years. Large cross-border cash transactions by banks are routinely reported to the Central Bank and kept on file. Individual bankers may be held responsible if their institutions are used to launder money. Norway's anti-money laundering legislation has been strengthened in recent years to conform to the FATF Forty Recommendations.

The Banking, Insurance, and Securities Commission of Norway monitors the financial markets and financial institutions, issues warnings, forwards the consolidated UNSCR 1267/1390 list of terrorist entities and individuals to financial institutions, and issues orders to freeze assets and funds. The Commission conducts on-site inspections to monitor the finance sector and to ensure that the regulations are complied with correctly. The Commission has also taken steps to strengthen reporting requirements of charitable entities.

There were approximately 30 major arrests and/or prosecutions for money laundering in Norway in 2001 and 25 in 2002. Law enforcement officials have the authority to freeze and confiscate assets during money laundering investigations. Suspicious or unusual transaction reports filed by financial institutions have steadily increased over the past four years from 788 reports in 1999 to 992 reports in 2001. There have been 745 suspicious transaction reports filed as of June 30, 2002.

On June 28, 2002, a new bill entered into force, permanently establishing legislative measures against acts of terrorism and the financing of terrorism, and fulfilling the requirements of the UN International Convention for the Suppression of the Financing of Terrorism. Norway ratified this Convention on July 15, 2002. Norway has now ratified all 12 of the International Conventions and Protocols relating to terrorism.

Norway has the authority to identify, freeze, and seize terrorist financial assets. On October 11, 2002, Norway adopted the EU's Common Position on the Application of Specific Measures to Combat Terrorism. No investigations have yet been conducted involving violations of terrorist financing provisions. However, one money laundering and banking case has been associated with the use of the Dahabshil and Al-Barakaat hawala systems.

Norway is a member of the Financial Action Task Force (FATF). Oekokrim is a member of the Egmont Group. Norway is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Norway has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Oman. Oman is not a regional or offshore financial center and does not have a significant money laundering problem. Its small banking sector is supervised by the Central Bank of Oman (CBO), which has the authority to suspend or reorganize a bank's operations. Oman has six commercial banks with 304 Omani and 10 foreign branches. There are also nine foreign incorporated banks with 27 branches in the country. Smuggling trade goods across Oman's long borders and coastline is becoming an increasing concern. Oman may also be vulnerable to forms of trade-based money laundering and customs fraud.

In March 2002, Royal Decree No. 34/2002 was issued promulgating "The Law of Money Laundering." This new law strengthened the existing money laundering regulations by detailing bank responsibilities, widening the definition of money laundering to include funds obtained through any criminal means, and providing for the seizure of assets and other penalties. The new law applies to other types of non-bank financial institutions as well. As of the end of 2002, there had been no arrests under the new law.

The Royal Oman Police (ROP), in coordination with the CBO, is responsible for investigating money laundering activities. Banks are required to know their customers and report all suspicious transactions. Oman has plans to establish a Financial Intelligence Unit (FIU) that will receive suspicious transactions and help coordinate resulting investigations. Oman regulates charitable organizations.

Oman is a party to the 1988 UN Drug Convention, and a member of the Gulf Cooperation Council (GCC), which is a member of the Financial Action Task Force (FATF). In June 2001, Oman underwent a FATF mutual evaluation. Oman has responded to terrorist asset freeze lists by distributing the lists to all

Money Laundering and Financial Crimes

banks and other financial institutions in the country for checking against their accounts. Thus far, the Government of Oman has reported negative results.

Oman should continue to implement its anti-money laundering program, specifically creating a FIU and training criminal investigators to initiate money laundering investigations from the field. Oman also should become more aware of the dangers of alternative remittance systems to launder money and transfer value such as hawala and trade-based money laundering. Oman should also criminalize terrorist financing.

Pakistan. Financial crimes related to narcotics-trafficking, terrorism, smuggling, tax evasion, and corruption remain a significant problem in Pakistan. Production of narcotics in Pakistan is negligible, but Pakistani criminal networks play a central role in the transshipment of narcotics and smuggled goods from Afghanistan to international markets. The proceeds of narcotics-trafficking and funding for terrorist activities are often laundered by means of the alternative remittance system called hawala. This system is also widely used by the Pakistani people for legitimate purposes. A nexus of private, unregulated charities has also emerged as a major source of illicit funds for international terrorist networks.

The Control of Narcotics Substances Act of 1996 criminalizes the laundering of narcotics-related proceeds. The Act contains provisions for the freezing and forfeiture of assets associated with narcotics-trafficking and the reporting of financial transactions believed to be associated with narcotics-trafficking. Pakistan's Ministry of Finance in 2002 drafted anti-money laundering and anti-terrorist financing legislation to bring Pakistan into compliance with international norms. As of late December 2002, this legislation was awaiting consideration by the newly elected National Assembly.

Pakistan's cooperation in Operation Enduring Freedom has brought renewed focus on the role of informal financial networks in financing terrorist activity. In July 2002, the Government of Pakistan (GOP) passed an ordinance regulating hawala moneychangers and facilitating cross-verification of financial transactions between Pakistan and the Gulf States. These measures have led to the registration and formalization of many hawala businesses, but a significant number continue to operate outside the legal framework. A large percentage of hawala transfers to Pakistan consists of the repatriation of wages from the roughly five million Pakistani expatriates residing abroad. There have also been reports of money laundering using gold and gems. Trade-based money laundering is also prevalent. Goods such as foodstuffs, electronics, vegetable oils, and other products that are primarily exported from Dubai to Karachi are then forwarded, at least on paper, to Afghanistan via the Afghan Transit Trade. Through smuggling, corruption, avoidance of customs duties and taxes, and barter deals for narcotics, many of the goods destined for Afghanistan find their way into the burgeoning Pakistani black market. The trading in these goods and commodities is also believed to be used to provide counter-valuation in hawala transactions.

Currently, Pakistan does not have a financial intelligence unit (FIU). Pakistan's National Accountability Bureau, Anti-Narcotics Force, Federal Investigative Agency (FIA), and Customs oversee Pakistan's anti-money laundering efforts. The National Accountability Bureau has been successful in investigating and prosecuting corruption. Pakistan is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. As of January 2003, Pakistan had not signed the UN International Convention for the Suppression of the Financing of Terrorism, but has identified and blocked terrorist assets. Pakistan became a member of the FATF-style regional body, the Asia/Pacific Group on Money Laundering in 2000.

Pakistan should move quickly to enact anti-money laundering and anti-terrorist financing legislation that conforms to international standards. It also should issue financial regulations that mandate the reporting of all suspicious transactions and establish an FIU. In addition, in light of the role that private charities have played in terrorist financing, the GOP should develop a system to regulate charitable organizations and to shut down those charitable organizations that finance violence and terrorism. More emphasis should be put on the misuse of trade to launder money. The misuse of the Afghan Transit Trade should be examined. Customs needs assistance in automation, efforts to control smuggling, and training in how

to recognize money laundering. Law enforcement also needs training in investigating financial crimes. The judicial sector needs to be strengthened and should develop more familiarity with money laundering. Tax reform will also be an essential component in helping to counteract the appeal of hawala.

Palau. An archipelago in the Western Pacific with a population of about 19,000, and per capita GDP of about \$7,000, Palau is not a major financial center. Upon its independence in 1994, Palau entered the Compact of Free Association with the United States. The U.S. dollar is legal tender. 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 commission that recommended financial control legislation to the National Congress in 2001. Following that, Palau took several steps to address financial security through banking regulation and supervision, and the establishment of 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 of 2001 criminalized money laundering and created a Financial Intelligence Unit. This legislation imposes threshold and suspicious transaction reporting, 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 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. This Act also contains provisions allowing the freezing and forfeiture of assets that are the proceeds of a crime.

The Financial Institutions Act of 2001 established the Financial Institutions Commission, an independent regulatory agency that is responsible for licensing, supervising and regulating financial institutions in Palau. 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.

Palau has enacted several legislative mechanisms to foster international cooperation. The Mutual Assistance in Criminal Matters Act (MACA), also 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.

Palau acceded to the UN International Convention for the Suppression of the Financing of Terrorism on November 14, 2001. Palau forwarded to its financial institutions the names of suspected terrorists and terrorist organizations and asked that any assets or accounts belonging to those individuals or entities be immediately reported to the Government and seized. No such assets have been found. Anti-terrorism legislation has been drafted and is expected to be introduced to the National Congress shortly. Additionally, the Task Force on Anti-Terrorism and Homeland Security has been created and is reviewing Palau's efforts to detect and prevent terrorism in the Republic.

Palau is a member of the Asia/Pacific Group on Money Laundering. It has signed Pacific Island Forum anti-money laundering initiatives and has sought to abide by the Honiara Declaration, which calls for Forum countries to implement the Financial Action Task Force 40 Recommendations on Money Laundering.

Palau has taken several steps toward enacting a legal framework with which to combat money laundering. Palau should continue its efforts to implement the broad-based legal reforms already put in place. If the draft of the pending anti-terrorism legislation does not specifically criminalize the support and financing of terrorists, Palau should insert such a provision.

Money Laundering and Financial Crimes

Panama. Despite significant progress to strengthen Panama's anti-money laundering regime since October 2000, money laundering remains a serious problem in Panama and is a potential threat to the stability of the country's legitimate financial institutions. Panama's proximity to major drug-producing countries, its sophisticated international banking sector, its U.S. dollar-based economy, and the Colon Free Zone's (CFZ) role as an originating or transshipment point for goods purchased with narcotics dollars through the Colombian Black Market Peso Exchange make the country particularly vulnerable to money laundering. Panama's financial institutions 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.

Panama's large offshore financial sector includes international business companies (over 370,000 currently registered in Panama), offshore banks (approximately 34 banks), captive insurance companies (corporate entities created and controlled by a parent company, professional association, or group of businesses), and trusts. Captive insurance has become one of the most important sectors of Panama's offshore financial industry, following banking. The high volume of trade occurring through Panama's Colon Free Trade Zone (there are approximately 2,040 businesses established in the Zone) presents opportunities for trade-based money laundering to occur.

In June 2000, the Financial Action Task Force (FATF) identified Panama as a non-cooperative country or territory (NCCIT) in international efforts to fight money laundering. In July 2000, the U.S. Treasury Department issued an advisory to U.S. financial institutions advising them to "give enhanced scrutiny" to financial transactions involving Panama, including transactions involving the CFZ.

These events prompted the Government of Panama (GOP) to engage in coordinated effort to enact and implement laws, executive orders, and regulatory agreements with banks to bring Panama's anti-money laundering program into compliance with international standards. In October 2000, the GOP enacted two laws and issued two Executive decrees to address FATF's concerns about its anti-money laundering regime:

Law No. 41 (Article 389) of October 2, 2000, amended the Penal Code by expanding the number of predicate offenses for money laundering beyond drug 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 established a punishment of 5 to 12 years imprisonment and a fine.

Law No. 42 of October 2, 2000, requires financial institutions (banks, trust companies, money exchangers, credit unions, savings and loans associations, stock exchanges and brokerage firms, and investment administrators) to report the Financial Analysis Unit (UAF)—Panama's Financial Intelligence Unit—currency transactions in excess of \$10,000 and suspicious financial transactions. Law 42 also mandates casinos, CFZ businesses, the national lottery, real estate agencies and developers, and insurance/reinsurance companies to report to the UAF currency or quasi-currency transactions that exceed \$10,000. Furthermore, Law 42 requires Panamanian trust companies to identify to the Superintendent of Banks the real and ultimate beneficial owners of trusts.

Executive Decree No. 163 of October 3, 2000, which amended the June 1995 decree that created the UAF, 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. The Panamanian UAF and the U.S. FIU, the Financial Crimes Enforcement Network (FinCEN), concluded an informal information sharing arrangement and have since shared information through letters of exchange on a case-by-case basis. In 2002 the Panamanian UAF signed memoranda of understanding with seven countries—Mexico, Italy, Guatemala, the Dominican Republic, Croatia, Honduras, and the Principality of Monaco—bringing the total to nineteen. In addition MOUs with Spain, France, Bulgaria, Colombia, Brazil, and El Salvador are awaiting signatures by those respective governments.

Executive Order No. 163 also allows the UAF to provide information related to possible money laundering directly to the Office of the Attorney General for investigation. The UAF continues efforts to raise the level of compliance for reporting suspicious financial transactions particularly by non-bank financial institutions and businesses in the CFZ.

Executive Order 213 of October 3, 2000, amending Executive Order 16 of 1984 relative to trust operations, provides the dissemination of information related to trusts to appropriate administrative and judicial authorities. Furthermore, in October 2000, Panama's Superintendency of Banks issued an Agreement No. 9-2000 that defines requirements that banks must follow for identification of customers, exercise of due diligence, and retention of bank records reporting transactions.

In light of these significant legislative and regulatory reforms and GOP efforts to implement these reforms, the FATF recognized in June 2001 that Panama had remedied the serious deficiencies in its anti-money laundering regime and removed Panama from FATF's list of non-cooperative countries and territories. Similarly, the U.S. Treasury Department withdrew its advisory against Panama in June 2001.

In 2002, the Ministry of Commerce and Industry issued a circular to all finance companies reminding them of the transaction-reporting requirement of Law 42. It also increased the number of inspections on finance companies, and began drafting a law to regulate the operations of pawnshops and exchange houses. The Autonomous Panamanian Cooperative Institute (IPACOO) established a specialized unit for the supervision of loans and credit cooperatives regarding compliance with the requirements of Law 42. The National Securities Commission carried out numerous training sessions and workshops for its personnel and regulated entities. The Colon Free Zone Administration prepared and issued a procedures manual for the users of the Free Zone, outlining their responsibilities regarding prevention of money laundering and requirements under Law 42.

In December 2002, the Panamanian Legislative Assembly approved the Financial Crimes Bill (Law No. 6 of December 6, 2002), which establishes 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 criminalize a wide range of activities related to financial intermediation, including the following: illicit transfers of moneys, accounting fraud, insider trading, and the submission of fraudulent data to supervisory authorities.

With support from the Inter-American Development Bank, the GOP is implementing a Program for the Improvement of the Transparency and Integrity of the Financial System. This Transparency Program is targeted at, through enhanced communication and information flow, training programs, and technology, strengthening the ability of those government institutions responsible for preventing and combating financial crimes and terrorist-financed activities.

Panama has brought cases for domestic prosecution, and the UAF routinely transfers cases to the UIF for investigation. To increase GOP interagency coordination, the UAF and 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 will enable the UAF to begin more timely investigations. In 2002, Panamanian Customs continued an anti-money laundering program at Tocumen International Airport, begun in 2001, to deter currency smuggling by seizing and forfeiting all undeclared funds in excess of \$10,000 from arriving passengers. During 2002, Panamanian customs officers at Tocumen International Airport seized \$3,745,000 in undeclared currency.

GOP cooperation in the investigation of the Hemisphere's largest Black Market Peso Exchange money laundering scheme was instrumental in the U.S. conviction in 2002 of Yardena Hebroni, owner of Speed Joyeros, a CFZ enterprise. The GOP also revoked the Panamanian residency of Hebroni, an Israeli national, after she was ordered deported from the United States. Also notable in 2002 was GOP cooperation in the investigation of large-scale political corruption, theft, and embezzlement of Government of Nicaragua funds, and money laundering by former Nicaraguan president Arnoldo Aleman and members of his government and family. The Panamanian portion of the investigation resulted in the

Money Laundering and Financial Crimes

freezing of \$7 million of the Nicaraguan funds in Panamanian banks and in the freezing of considerable real estate holdings in Panama.

The GOP 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. Also in 2002, the Institute of Autonomous Panamanian Cooperatives, UAF, and the Embassy Narcotics Assistance Section cosponsored a roundtable on money laundering that offered practical training to financial institutions in meeting the reporting requirements under Law No. 42.

In October the UAF, Bank Superintendency and Public Ministry inaugurated a public campaign for the prevention of money laundering that articulated the link between money laundering and terrorist financing and included television commercials co-funded by the Embassy NAS. Also in 2002, the Panamanian Gaming Commission received training on compliance and security issues from the Las Vegas Gaming Commission Seminar earlier in the year.

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 assistance in strengthening their anti-money laundering programs, including Guatemala, Costa Rica, Russia, Honduras, and Nicaragua. Panama also hosted the Sixth Hemispheric Congress on the Prevention of Money Laundering in August 2002. Panama is active in the multilateral Black Market Peso Exchange Group (BMPEG) 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 Organization of American States (OAS) Inter-American Drug Abuse Control Commission (CICAD), the Caribbean Financial Action Task Force (CFATF), and the Offshore Group of Banking Supervisors (OGBS), and the UAF is a member of the Egmont Group. Panama is a party to the 1988 UN Drug Convention.

In response to USG efforts to identify and block terrorist-related funds, the GOP continues to monitor suspicious financial transactions. Panama is a signatory to over eleven United Nations conventions and protocols addressing actions against terrorism, some dating back to 1963. During 2002, the GOP became a party to the UN International Convention for the Suppression of the Financing of Terrorism, and in 2000 signed, but has not ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Panama should criminalize terrorist financing, continue its regional assistance efforts, and continue implementing the significant reforms it has undertaken to its anti-money laundering regime, in order to reduce the vulnerability of Panama's financial sector and to enhance Panama's ability to investigate and prosecute financial crime, money laundering and potential terrorist financing.

Papua New Guinea. Papua New Guinea is not a regional financial center. Its banking sector is relatively small and fairly well-regulated. However, there are no laws against money laundering.

Papua New Guinea is an observer to the Asia/Pacific Group on Money Laundering. Papua New Guinea is not a party to the 1988 UN Drug Convention.

Papua New Guinea should enact a comprehensive anti-money laundering regime that criminalizes terrorist financing and money laundering for all serious crimes. Papua New Guinea should sign the UN International Convention for the Suppression of the Financing of Terrorism.

Paraguay. Paraguay is a principal money laundering center, and although accurate figures are unknown, the National Anti-Drug Secretariat (SENAD) suspects that narcotics-trafficking may generate about 40 percent of money laundering. Money laundering occurs in both the banking and non-banking financial systems.

Money laundering is established as 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 new 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. There have been three convictions for money laundering so far in Paraguay, all under Article 196. All three defendants admitted their guilt and accepted the fine and suspended sentence.

Bank secrecy laws do not prevent banks and financial institutions from disclosing information to bank supervisors and law enforcement entities. Additionally, bankers and others are protected under the anti-money laundering law with respect to their cooperation with law enforcement agencies. Law 1015 also contains “due diligence” and “banker negligence” provisions and applies money laundering controls to non-banking financial institutions, such as exchange houses.

Law 1015 of 1996 requires banks and financial institutions to know and record the identity of customers engaging in significant large currency transactions and to report those suspicious activities to the Financial Intelligence Unit. However the extent to which these requirements are implemented in practice remain in question. The Unidad de Análisis Financiera (UAF) located at the time in the Secretaria de Prevención de Lavado de Dinero o Bienes (SEPRELAD). The UAF is the government entity responsible for receiving and analyzing suspicious activity reports (SARs). The Government, however, lacks a standardized form for SAR reporting, which inhibits the reporting and analysis process. Analysis is also limited because SAR reporting is manual, and the UAF analysts must input the information from the SAR forms into the UAF database. No reporting requirements exist for large currency transactions. As of mid-August 2002, the UAF had received 300 SARs for that year and had referred only ten cases for investigation.

For many years, investigations and prosecution of money laundering cases were also hampered by SEPRELAD’s burdensome bureaucratic structure, budget woes, and the loss of trained personnel. SEPRELAD’s weakness was reflected in the small number of cases presented to the Attorney General’s (AG) office for prosecution. Before 2001, only one went to trial and it was dismissed by the judge on procedural grounds. In the last two years, the USG worked with the SEPRELAD’s UAF to find the means to augment the number of ready-to-prosecute money laundering cases, and to forge more cooperative working relationships between the UAF, the SENAD, the AG, and the Central Bank’s new money laundering unit as well. There were some initial successes such as the FAU’s post 9/11 cases, which showed millions of dollars in wire transfers from Ciudad del Este to Lebanon. Although charges of money laundering were not presented against any individual, part of the information prepared by the UAF helped buttress the criminal case against one suspected fund-raiser for terrorist organizations. He was sentenced to six-and-a-half years in prison for tax evasion. In an effort bring new vitality to the battle against money laundering, the Financial Analysis Unit (FAU) was removed from SEPRELAD’s supervision and commissioned to the AG’s office in July 2002, and a new director assumed charge in December 2002. Taking the FAU out of the ineffective SEPRELAD and putting it under the AG’s authority should enhance cooperation at the working level and improve the AG’s ability to investigate money laundering and terrorist financing. Changing its ineffective director is also expected to infuse new vitality into the unit.

Paraguay continued to experience banking failures, including the closing of the National Worker’s Bank (BNT), and the collapse of Banco Aleman in June 2002. The most spectacular case involved \$16 million diverted from the Central Bank to private accounts apparently linked to the President’s family. The GOP is working with the U.S. Treasury and Justice Departments to trace and account for the missing funds and return them to the Central Bank. The GOP is also suing the U.S. lawyer who handled the funds in the U.S., in an attempt to recover the funds.

The anti-money laundering law of 1996 provides a basic system for forfeiting narcotics-related assets, including bank accounts and a system for forfeiting proceeds derived from narcotics-trafficking. The law

Money Laundering and Financial Crimes

authorizes sharing forfeited assets with other governments. Legitimate businesses can be seized if they are derived from illicit proceeds. Businesses can also be fined or subjected to administrative sanctions if merely used to launder money. The laws only provide for criminal forfeiture.

Paraguay currently has limited resources to investigate and prosecute money laundering cases. Investigations are carried out by a small financial crimes investigative unit, the Unidad de Investigación de Datos Financieros (UIDF). The UAF and the Superintendency of Banks refer analyzed cases to the UIDF for investigation. The UIDF is housed within Paraguay's SENAD, which has adequate police but limited resources to trace and seize assets. Because there are only about 200 prosecutors nationwide for a population of 5.5 million, money laundering investigations in Paraguay are assigned to a single prosecutor. Government corruption is an ongoing problem related to money laundering and money laundering investigations.

Little in the way of personal background information is required to open a bank account or to make financial transactions in Paraguay; therefore there is a high incidence of money laundering activities. Paraguay is an attractive offshore financial center for neighboring countries, particularly Brazil. Foreign banks are registered in Paraguay and non-residents are allowed to hold bank accounts, but current regulations forbid banks from advertising or seeking deposits from outside the country. The Superintendent of Banks, who exercises his right to audit financial institutions, supervises all banks under the same rules and regulations. But there are few effective controls over businesses, and businesses can operate without paying taxes. The large informal economy is outside the GOP's regulatory scope.

The multi-billion dollar contraband re-export trade is centered in Ciudad del Este—the heart of Paraguay's informal economy, and is outside the government's regulatory scope, which also facilitates money laundering in Paraguay. The area is well known for arms and drug trafficking, and international property rights crimes. There are no controls on the amount of currency that can be brought into or out of the country, and there are no cross-border reporting requirements. The area is also suspected by government officials in Paraguay and the U.S. to be a source of terrorist financing. Recent raids in CDE have led to the seizure of arms catalogs, bomb-making materials, extremist Islamic materials, and receipts of wire transfers from Paraguay to the Middle East and the United States. Paraguay has taken some measures to tackle this “gray” economy and to move to a more formal, diversified economy. Paraguay is looking to a “maquila” industry and tourism as alternatives for Ciudad del Este (CDE) and the entire tri-border area.

In the wake of the September 11 attacks, and the call for a crackdown on illicit financial activities that may be fueling terrorist groups, the Central Bank established a complementary money laundering operation to SEPRELAD. La Unidad de Análisis sobre Prevención de Lavado de Dinero o Bienes, or the Analysis Unit for the Prevention of the Laundering of Money or Goods, was originally developed to coordinate the review of the Paraguayan financial institutions' databases for information regarding suspected terrorists. However, the Analysis Unit only has purview over financial institutions, while SEPRELAD has a much broader mandate, to include gambling houses, real estate companies, and many other institutions handling cash and financial transactions. The U.S. Government and the Egmont Group recognize only SEPRELAD's UAF as a financial intelligence unit.

In addition to establishing the Analysis Unit, the GOP has carried out limited efforts to combat terrorist financing. Although there is draft anti-terrorism legislation that was introduced in the Chamber of Deputies in 2002, the GOP currently has no specific laws criminalizing terrorism or terrorist financing. Paraguay has adopted provisions to cover conduct that would be considered terrorist acts, but most of these acts do not carry a sentence of more than five years, nor are they considered predicate offenses for money laundering. The GOP has also signed, but not yet ratified, the OAS Inter-American Convention on Terrorism, which is not in force internationally, and the UN International Convention for the Suppression of the Financing of Terrorism. Paraguay is a member the South American Financial Action Task Force (GAFISUD) and is scheduled to undergo a mutual evaluation on anti-money laundering practices in 2003. Paraguay is also a member of the Egmont Group of Financial Intelligence Units. The GOP has signed the

OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Hemispheric Drug Strategy. Paraguay is party to the 1988 UN Drug Convention, and participates in Summit of the Americas and CICAD-related meetings on money laundering. The GOP has signed, but not ratified, the OAS Inter-American Convention on Mutual Assistance in Criminal Matters and the UN Convention against Transnational Organized Crime, which is not yet in force internationally. It also endorsed the Basel Committee's "Core Principles for Effective Banking Supervision." In 1994, the United States and Paraguay entered into an Agreement to Cooperate in the Prevention and Control of Money Laundering Arising from Illegal Trafficking in Narcotics and Psychotropic Substances, and the GOP also entered into a bilateral agreement with Brazil in 2000 to permit the exchange of money laundering information.

While the GOP took some positive steps in 2002, and provided excellent cooperation in the fight against terrorism, there are other initiatives that should be pursued to increase the effectiveness of Paraguay's anti-money laundering regime. Existing money laundering legislation should be modified to resolve the conflicting aspects of the two laws. The GOP should clearly identify either the UAF or the Analysis Unit as the national financial intelligence unit, or combine the two existing agencies into a single unit to receive, analyze and disseminate information on money laundering. Measures should be taken to expedite the SAR reporting process, such as the development of a standard form that could be sent electronically to the FIU, as well as conducting outreach activities to sensitize financial institutions about reporting requirements. In addition, procedures to file large currency transaction reports should be initiated to further combat illegal financial activity. Paraguay should also adopt legislation that criminalizes and penalizes terrorism and terrorist financing, and establishes terrorist acts and financing as predicate offenses for money laundering.

Peru. Peru is not a major regional financial or offshore money laundering haven. Narcotics-related and other money laundering does occur, but existing laws do not provide reliable or adequate mechanisms to estimate its scale in Peru. Such money laundering may be connected with narcotics-related activity originating in Peru, Colombia or elsewhere in the region, and may involve proceeds of narcotics sales in the United States. Peru's economy is 70-80 percent dollarized, so money laundering is probably conducted primarily in U.S. currency.

A number of former government officials, most from the prior 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. In 2002, the Government of Peru (GOP) continued to make strong efforts at uncovering and recovering the millions of U.S. dollars believed to be the proceeds of money laundering activities carried out by Vladimiro Montesinos, former director of the Peruvian National Intelligence Service.

In 2002, the GOP strengthened its anti-money laundering regime. Prior to 2002, Peru had a limited anti-money laundering legislative and regulatory framework. The previous system criminalized only the laundering of proceeds directly associated with narcotics-trafficking and "narcoterrorism." The new law builds on the 1991 banking law, the 1996 General Law of the Financial and Insurance System and Organic Law of the Superintendency of Banking and Insurance (No. 26702) and 1998 implementing regulations. The new law is very brief, however, and lacks implementing regulations. Furthermore, only certain financial institutions are regulated under the money laundering law, and no regulatory control is exercised over most non-banking enterprises (exchange houses, stock brokerages, etc.). The U.S. Treasury and other outside observers believe that the GOP will need to add detail to the law and develop implementing regulations to make the law effective and applicable in practice. Peru has separate regulations that prohibit laundering money through casinos, but the GOP lacks sufficient resources to adequately supervise this industry.

Money Laundering and Financial Crimes

On April 12, 2002, President Toledo signed into law Bill 27693, which among other things provided for the creation of Peru's first Financial Intelligence Unit, the Unidad de Inteligencia Financiera (UIF). The UIF is an autonomous body responsible for receiving, analyzing, and disseminating suspicious transaction reports. Implementing regulations for the UIF law were issued on October 31, 2002. Prior to the April 2002 law, all unusual or suspicious financial transactions were reported directly to the Office of the Attorney General, and the information was then shared with the Financial Investigative Office of the Peruvian National Police Directorate of Counternarcotics (DINANDRO). Under the new law, the FIU will report information on possible crimes to the Attorney General's office. Also, only banks and financial institutions were required to file suspicious transaction reports under the old legislation. Under the new law, exchange houses, casinos, auto dealers, construction or real estate firms, and other sectors are all required to report suspicious transactions to the UIF. The UIF is also empowered to request financial transaction information from exchange houses, metal and antiques traders, travel agencies and a variety of Peruvian government agencies.

The new legislation also reinstated reporting requirements for large cash transactions. An amendment to the previous anti-money laundering law had required the reporting of currency transactions over 30,000 soles (about \$10,000), but this requirement was suspended in August 1998, one month after the amendment went into effect. This amendment did not apply to institutions other than banks or financial companies. The new money laundering law requires the reporting of individual cash transactions exceeding \$10,000 or transactions totaling \$50,000 in one month. Non-financial institutions, such as exchange houses, casinos, lotteries or others, must report individual transactions over \$2,500 or monthly transactions over \$10,000. Private businesses, banks, and financial companies must report these transactions to the UIF, and major institutions are required to appoint supervisory-level compliance officials to ensure that reporting requirements are met. The 2002 legislation does not address the issue of the transportation of cash or monetary instruments into or out of Peru.

Although the UIF was not yet operational at the end of 2002, the GOP projects that it will be established by early 2003. In October 2002, implementing regulations were issued and the Ministry of Economy and Finance appropriated funds for the initial staffing of the UIF. In early December, the GOP designated a director for the Financial Intelligence Unit.

On June 20, 2002, a new law was passed that expands the predicate offenses from money laundering to include the laundering of assets related to any crime. The penalties for money laundering were also altered. Instead of a life sentence for the crime of laundering money, the new law sets prison terms of eight to fifteen years for convicted launderers, with a minimum sentence of twenty-five years for cases linked to narcotics-trafficking, terrorism, or laundering through banks or financial institutions. In addition, the revised Penal Code criminalizes "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. However, to date, this law lacks implementing regulations, which are necessary to make the law effective and applicable in practice. To date, there have been only two prosecutions and no convictions for money laundering.

Peru currently lacks comprehensive and effective asset forfeiture legislation. The financial investigative office of the Peruvian National Police's Directorate of Counter-narcotics has seized numerous properties over the last several years, but few were turned over to the police to support counternarcotics efforts, and no clear mechanism exists to distribute seized assets among government agencies.

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 UN 1267 Sanctions Committee's consolidated list as being linked to Usama Bin Ladin, 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.

The new legislation, however, fails to provide the GOP with the authority to successfully fight money laundering as a means of terrorist financing. 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 both as a foreign terrorist organization pursuant to section 219 of the Immigration and Nationality Act and pursuant to 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. A final judicial decision is then needed to dispose of or use such assets. Draft legislation that would enable the GOP to do so is currently stalled in the Foreign Affairs Ministry.

Peru ratified the UN International Convention for the Suppression of the Financing of Terrorism on November 10, 2001 and has signed, but not yet ratified, the OAS Inter-American Convention on Terrorism, which is not in force internationally. Peru is a party to the 1988 UN Drug Convention. On January 23, 2002, Peru deposited its instrument of ratification for the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Peru is a member of the Organization of American States Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering, and the South American Financial Action Task Force (GAFISUD) Peru and the U.S. Government signed a new extradition treaty in July 2001. The GOP ratified the treaty in October 2002 and the United States completed its ratification on January 23, 2003. Entry into force is pending the exchange of instruments of ratification. The Peruvian Ministry of Finance and the U.S. Treasury Department exchange financial information for money laundering investigations based on a 1991 Financial Information Exchange Agreement (FIEA).

By establishing a Financial Intelligence Unit and improving existing money laundering legislation in 2002, the GOP made serious advancements in strengthening its anti-money laundering regime. However, much progress is still required. The GOP should proceed with efforts to make the new Financial Intelligence Unit operational, so that the UIF can begin receiving and processing suspicious transaction reports. The Superintendent of Banks and Insurance Companies should appoint a director to the UIF as soon as possible. Training is needed for prosecutors, judges, police, auditors, bankers, and banking supervision officials in identifying suspicious transactions and in carrying out money laundering investigations and prosecutions. Anti-corruption efforts in Peru should be a priority, and the need for strong confidentiality protocols for the UIF should be stressed. The GOP should strengthen procedures to fight money laundering related to non-banking sectors, and should increase efforts to pass legislation criminalizing the financing of terrorists and terrorism and allowing for administrative blocking of terrorist assets. The U.S. Treasury Department is developing an assistance program to strengthen Peru's capabilities in the above areas.

Philippines. The Philippines is a major financial center in the Pacific. In the past few years, the illegal drug trade in the Philippines reportedly has evolved into a billion-dollar industry. Additionally, the Philippines has experienced an increase in foreign organized criminal activity from China, Hong Kong, and Taiwan. Insurgency groups operating in the Philippines fund their activities through narcotics- and arms-trafficking, and engage in money laundering through alleged ties to organized crime. Corruption of government officials is also a source of laundered funds.

In June 2000, the Financial Action Task Force (FATF) placed the Philippines on the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering. The major deficiencies cited by FATF were excessive bank secrecy provisions and lack of a basic set of anti-money laundering regulations, including customer identification and record keeping requirements. Following its placement on the NCCT list, FinCEN, the U.S. financial intelligence unit, issued an advisory to all U.S. financial institutions instructing them to "give enhanced scrutiny" to transactions involving the Philippines.

In June 2001, the FATF determined that the Philippines had made insufficient progress toward remedying the noted deficiencies, and warned that FATF would impose countermeasures by September 30, 2001, if

Money Laundering and Financial Crimes

the Philippines failed to address such deficiencies. In the face of mounting international pressure, the Philippines enacted legislation in September 2001 that addressed many of the FATF's concerns. FATF withdrew its call for countermeasures against the Philippines in September 2001; however, the Philippines remains on the NCCT due to the continued deficiencies relevant to bank secrecy restrictions, provisions in the law that would disallow prosecution for money laundering as a result of crimes committed prior to enactment of the law, and for inhibiting the Central Bank from conducting examinations of specific deposits without obtaining a court order.

The Anti-Money Laundering Act of 2001 (AMLA) criminalizes money laundering, an offense defined to include the conduct of activity involving the proceeds of any unlawful activity, and imposes penalties that include a term of imprisonment of up to seven years. The Implementing Rules and Regulations (IRR) for the Anti-Money Laundering Act were enacted in April 2002.

The AMLA establishes the Anti-Money Laundering Council (AMLC). The AMLC is composed of the Governor of the Bangko Sentral ng Pilipinas as chairman, and the Commissioner of the Insurance Commission and the Chairman of the Securities Exchange Commission as members. The AMLC serves as the Philippines' Financial Intelligence Unit (FIU). Since its establishment, the Government of the Philippines (GOP) reports the AMLC has provided training to other government agencies, financial institutions and private sector organizations. It also participated in a joint initiative to establish anti-money laundering task forces/desks in the Department of Justice, the National Bureau of Investigation (NBI) and the Philippine Center on Transnational Crime (PCTC).

The AMLC is authorized, among other things, to receive suspicious activity reports from covered institutions and to freeze assets alleged to be connected to money laundering. However, the AMLC is unable to instantly freeze bank accounts. By law, the AMLC must wait for Suspicious Transaction Reports (STRs) to be filed, and then establish probable cause. Once probable cause is established, the AMLC is able to freeze an account for a period of 15 days. The AMLC is required to obtain a court order to be able to examine an account. A drawback to this system, especially in connection with terrorist financing, is that terrorism has not yet been defined as a crime. According to the GOP, in its first year of operations, the AMLC received 33 STRs and 32 Covered Transaction Reports (CTRs) and nine Letter-Advices. Additionally, the AMLC issued 27 freeze orders and froze 133 accounts or investments with a total value of \$298,600.

The AMLA builds upon the customer identification and suspicious activity reporting requirements contained in the earlier bank circulars, requiring "covered institutions" – i.e., banks, insurance companies, and broker-dealers in securities – to establish and record the true identity of their clients, based on official documents, and to maintain records of all transactions for five years from the date of such transactions. The AMLA further requires covered institutions to report "covered transactions," which are set at a threshold of PHP 4 million (approximately \$80,000) or an equivalent in foreign currency based on the prevailing exchange rate within five consecutive banking days. Currently, Rule 5(3) in the IRR requires all suspicious transactions with covered institutions, irrespective of the amounts involved, to be reported to the AMLC. This new rule goes beyond what is stated in the AMLA, where there is no obligation to report suspicious transactions outside the definition of "covered transactions," thereby creating possible conflict between the scope of the AMLA and the implementing rules and regulations.

In addition the AMLA relaxes the strict bank secrecy laws of the Philippines. In cases of violation of the AMLA, and upon order of any competent court, the AMLC is able to examine any particular deposit or investment, with any banking institution or non-bank financial institution, when it has been established that there is probable cause that the deposits or investments are in any way related to a money laundering offense. Deposits made before the effective date of the AMLA are not subject to this disclosure.

Currently the Philippine Congress is considering amendments to the AMLA. One proposed amendment would reduce the "covered transaction" threshold amount from P 4,000,000 (approximately \$80,000) to P 500,000 (approximately \$10,000) and provide for mandatory suspicious transaction reporting, regardless of amount. There is a separate provision for suspicious transaction reporting that has no threshold

requirement. The proposed amendments of Section 9(c) would require banks to file reports for both covered and suspicious transactions within five working days from the date of their discovery. The proposed amendment of Section 11 is to give the AMLC the authority to examine deposits and investments without a court order.

The Philippines is a member of the Asia/Pacific Group on Money Laundering and is a party to the 1988 UN Drug Convention. The Philippines and the United States have a Mutual Legal Assistance Treaty that entered into force in 1996. On November 16, 2001, the Philippines signed, but has not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism. The GOP has signed and ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

The Philippines confronts a number of problems in its efforts to counter money laundering. The current threshold for reporting suspicious transactions should be lowered to be effective. The AMLC must be given the authority to retrieve account information relating to deposits or investments made prior to the date of AMLA's enactment and to respond to requests from foreign authorities regarding deposits and investments. Secrecy provisions must be relaxed to allow the Bangko Sentral to supervise and conduct periodic or special investigations without obtaining permission from any other authority and it must be allowed to inquire about and examine any deposit or investment with any banking or non-banking financial institution in the country. The Philippines must address these deficiencies in its current regime, and finalize and implement the necessary regulations. Otherwise, the FATF will recommend that its 29 member states levy countermeasures against the GOP. The Philippines must also criminalize the financing and support of terrorism.

Poland. As a gateway between the former Soviet Union republics and countries of the European Union and lucrative markets beyond, Poland lies directly in the path of narcotics-traffickers and organized crime groups. The burgeoning economy of Europe, and open borders with former socialist countries, have led to a significant growth in transnational crime. Narcotics-trafficking, organized crime activity, auto theft, smuggling, extortion, counterfeiting, burglary, tax fraud, tax evasion, and other crimes generate criminal proceeds in the range of \$2-3 billion yearly, according to Polish government estimates. Poland's banks serve as transit points for the transfer of criminal proceeds. Polish currency exchange businesses and casinos are likewise venues for money laundering activity. The unregistered or gray economy is estimated at approximately 16 percent of GDP. Prosecutors have investigated more than 75 cases involving money laundering since Poland criminalized money laundering in 1997. To date, only one of the cases forwarded to the courts has resulted in a successful prosecution.

In June 2001, the November 2000 Act on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources, often referred to as "the Act of 16 November," came into force. This Law broadened the offense of money laundering to encompass all serious crimes, and increased penalties. The 2000 Law also provided for the creation of a Financial Intelligence Unit (FIU), the General Inspectorate of Financial Information (GIIF), to collect and analyze large and suspicious transactions. GIIF is housed within the Ministry of Finance and became operational in July 2001. In its first year of existence, GIIF received over 350 suspicious transaction reports. More than 38 went to the Prosecutor's Office, and of these, no fewer than 37 prosecutions based on the information from GIIF were initiated. Currently, the Ministry of Justice is preparing between 60 and 70 money laundering cases for trial. 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 three months further, pending a court decision.

A major weakness of Poland's former money laundering regime was that it did not cover many non-bank financial institutions that had traditionally been used for money laundering. Under the new regime, the scope of institutions subject to identity verification, record keeping, and suspicious transaction reporting (SAR) has been widened. Financial institutions subject to the reporting requirements include banks, brokerages, casinos, insurance companies, investment and pension funds, leasing firms, private currency

Money Laundering and Financial Crimes

exchange offices, real estate agencies, and notaries public. In addition, financial institutions are now required to put internal anti-money laundering procedures into effect—a process that is overseen by GIIF. The GIIF is also working with the private sector to develop a better risk profile in Poland, including taking measures to prevent the misuse of charities.

Additional amendments to the money laundering law are expected to come into force in early 2003. These amendments broaden the scope of institutions obligated to report, bring Poland's anti-money laundering legislation up to EU standards regarding the 15,000 euro (approximately \$15,000) reporting threshold, authorize the Ministry of Finance to freeze assets, and give the Polish government authorization to act against terrorism financing. The law authorizes the Ministry of Finance to block suspicious transactions for up to 48 hours. If the Ministry of Finance wants to freeze a transaction for a longer period of time, the case must be referred to a prosecutor, who has the authority to freeze a transaction for an additional three months while an investigation is undertaken. Poland is still working on amendments to the criminal code, which would further improve the government's ability to seize assets. Poland also recently created an office of anti-terrorist operations within the National Police to coordinate and supervise regional anti-terrorism units as well as train local police in anti-terrorism measures.

Poland is a party to the 1988 UN Drug Convention, the European Convention on Extradition and its Protocols, the European Convention on Mutual Legal Assistance in Criminal Matters, and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. In November 2001, Poland ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. In 2002, Poland signed the UN Convention for the Suppression of the Financing of Terrorism, which is expected to be ratified in the first quarter of 2003. Poland also signed and expects to ratify shortly the UN International Convention for the Suppression of Terrorist Bombings.

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, formerly PC-R-EV) and has undergone a mutual evaluation by that group.

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.

Poland has taken a number of steps to put in place a comprehensive anti-money laundering regime to meet international standards, and became one of the newest members of the Egmont Group in June 2002. Poland should pass specific anti-terrorist financing legislation and work to better coordinate investigations between relevant investigating agencies and prosecutors so as to obtain an improved record of prosecutions and convictions.

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. GOP officials also report that bureaux de change, wire transfers, and real estate purchases are used for laundering criminal proceeds.

Portugal has put in place a comprehensive anti-money laundering regime. Money laundering related to narcotics-trafficking and other serious offenses has been criminalized. The cross-border movements of currency that exceed 12,000 euros, approximately \$12,000, must be declared. All financial institutions, including insurance companies, must identify their customers, maintain records for a minimum of ten years, and demand written proof from customers regarding the origin and beneficiary of transactions that exceed 12,000 euros. Non-financial 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 transactions to the Office of the Public Prosecutor.

On February 11, 2002, Act 10/2002 was brought into force. This Act extended the list of entities obliged to report, to include account officers, external auditors, notaries, registrars, and money carriers. It also includes any other entities involved with the purchase and sale of real estate or commercial entities;

operations connected with funds, securities, or other assets belonging to clients; opening or management of savings bank accounts or securities accounts; creation, exploitation, or management of companies, trust funds, or similar structures; and the execution of any financial operation. In addition, according to this Act, the obligated entities have the duty to report any operation which, due to its scope, seems suspicious, independent of the transaction amount.

Act 10/2002 also expands money laundering to include as predicate crimes, trafficking in nuclear materials, trafficking in persons, trafficking in human organs or tissues, child pornography, trafficking in listed species, and tax fraud.

When money laundering is suspected, financial institutions must cease processing the transaction in question and report it to the judicial authority and the Office of the Public Prosecutor. The Public Prosecutor then forwards STRs for analysis to the Central Unit for Money Laundering Investigation (SCIB), which acts as the Financial Intelligence Unit (FIU) for Portugal. Often, reporting entities, usually banks, file their formal report with the Prosecutor's Office while informally reporting the case directly to the SCIB. If money laundering is indicated, the Portuguese Judicial Police (PJP) will conduct an investigation. The SCIB consists of ten criminal investigation officers. The SCIB reported receiving 251 STRs in 2001 and 256 STRs in 2002 (January-October 31)—mainly from banks and other financial entities. A total of 1,013 STRs have been filed since 1998. The SCIB is a member of the Egmont Group.

From January 2002 to November 2002, the PJP conducted 30 investigations of money laundering in connection with narcotics-trafficking. Portuguese laws also call for the confiscation of property and assets connected to money laundering, and authorize the PJP to trace illicitly obtained assets—including those passing through casinos and lotteries—even if the predicate crime is committed outside of Portugal. The GOP reported that 2.5 million euros (\$2.5 million) were seized in 2002 (up to October 31).

More recent legislation to combat organized crime, which came into force in 2002, authorizes police to request files of individuals under investigation. Additionally, with a court order, police are now able to 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.

Public and private sector regulators and organizations play important roles in Portugal's anti-money laundering program. In addition to monitoring compliance, educating the regulated industry, and training officials, a number also alert judicial authorities to evidence of money laundering.

The GOP has comprehensive legal procedures that enable it to cooperate with foreign jurisdictions and share seized assets.

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 entities, of which there are approximately 4,000 registered in Madeira, are similar to international business corporations (IBCs). 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.

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 non-residents or other Madeiran offshore entities, and "international branches" that conduct both offshore and domestic business. Although Madeira has some local autonomy, its offshore sector is regulated by Portuguese and EU legislative rules, and it is supervised by the competent oversight authorities. Bearer shares are not permitted.

Portugal is a member of the Council of Europe, the European Union, and the Financial Action Task Force (FATF). Portugal held the FATF presidency from 1999 to 2000. Portugal is a party to the 1988 UN

Money Laundering and Financial Crimes

Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Portugal is also a party to the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime, and became a party to the UN International Convention for the Suppression of the Financing of Terrorism on October 18, 2002.

Portugal has put into place comprehensive and effective measures to combat money laundering. The GOP's passage of new laws in 2002 will strengthen its ability to investigate and prosecute. The GOP should continue to exercise due diligence over its offshore sector, and closely monitor domestic non-bank financial institutions.

Qatar. Qatar has a relatively small population (approximately 600,000 residents), with an extremely 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 fifteen licensed financial institutions, including two Islamic banks; sixteen exchange houses; and three investment companies. Although Qatar is a cash-intensive economy, cash placement by money launderers is believed by authorities to be a negligible risk due to the close-knit nature of the society in Qatar and the rigorous "know your customer" procedures required.

On September 11, 2002, the Emir of the State of Qatar signed the Anti-Money Laundering Law. According to Article 28 of the law, 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 penalties of imprisonment of five to seven years, in addition to fines. The law expanded the powers of confiscation of proceeds gained from the commission of a crime and instrumentalities used to commit a crime, 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.

The law requires all financial institutions to report suspicious transactions to the QCB and retain records for up to fifteen 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 Qatar to extradite convicted criminals in accordance with international or bilateral treaties.

In addition to reporting suspicious transactions, financial institutions (including businesses conducting hawala transactions) must report all cash transactions of 30,000 Qatari rials (approximately \$11,000) or above to the QCB. The threshold was recently raised to QR 100,000 (approximately \$37,000). All financial institutions also must identify the person entering into a business relationship or conducting a transaction.

All accounts must be opened in person. (Only Qatari citizens, foreign residents, and citizens of other Gulf Cooperation Council [GCC] states are permitted to open bank accounts.) In January 2002, QCB issued Circular Number 9 regarding the Combat of Money Laundering and Financing of Terrorism. This circular was designed 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.

Qatar's charities are under direct supervision of the Ministry of Civil Service Affairs and Housing, as detailed in Law No. 8 of 1998 regarding private associations and institutions. Among the requirements of this law are: 1. registration; 2. regular government audits; 3. government approval for all disbursements; and 4. government inspection of facilities, documents and records.

Article 37 of Law Number 8 of 1998, concerning the establishment and governance of private associations and institutions, stipulates that the Ministry of Awqaf (Endowments) and Islamic Affairs shall oversee and monitor all the activities of private institutions within the boundaries that are regulated by executive provisions. The Ministry may examine the institution's books, records, and documents that are related to its activities, and it may amend its bylaws. The institution shall provide the Ministry with any information, documents, or other data it requests.

According to Article 1 of Law 15 of 1993, banks practicing in offshore business shall be formed either as joint stock companies having their head offices in the State of Qatar or as branches of Qatari or foreign banks.

The QCB, Public Prosecutor and the Criminal Investigation Division (CID) of the Ministry of Interior are the principal entities that have the responsibility for investigating and prosecuting money laundering cases. The QCB receives all suspicious transaction reports and conducts an initial analysis. The QCB obtains additional information from the banks and other government ministries before determining whether to forward the suspicious report to the Ministry of Interior. The Public Prosecutor and CID work closely on all criminal cases, although in financial cases they often seek the assistance of the QCB. There are no specialized units within the Public Prosecutor or CID's offices that initiate or investigate financial crimes. Qatar does not have a Financial Intelligence Unit (FIU). There is little financial crimes investigative experience. There have been no arrests or prosecutions related to money laundering or terrorist financing in 2002. The Government of Qatar (GOQ) is working to increase the ability of local authorities to investigate financial crimes, particularly as outlined in the new money laundering law. Qatar does not yet have any cross-border reporting requirements for financial transactions. Immigration and customs authorities are reviewing this policy and are increasingly interested in expanding their ability to detect trade based money laundering. A recent seizure of approximately \$400,000 of suspect gold entering the country is one example of the government's increased efforts.

The GOQ is currently revising its criminal law to include the crime of terrorism and the financing of terrorism. The current penal code includes a minor punishment for association with "illegal societies" but does not specifically address terrorism. Despite the absence of this law, Qatar has taken steps to combat the financing of terrorism, including requiring banks to freeze the assets of the individuals and entities listed on the UNSCR 1267/1390 consolidated list.

Qatar is a party to the 1988 UN Drug Convention. Qatar is not a signatory to the UN International Convention for the Suppression of the Financing of Terrorism nor the UN Convention against Transnational Organized Crime. Qatar actively participates in the Financial Action Task Force (FATF) as a member of the GCC.

The passage of Qatar's new money laundering law and the drafting of a criminal law to address terrorism finance crimes are indications of Qatar's commitment to combating money laundering and terrorism financing. Implementation and enforcement of the new law and regulations are essential to the success of Qatar's efforts. Training for law enforcement and customs authorities in recognizing and investigating money laundering is also essential. Qatar should sign the UN Convention for the Suppression of Terrorist Financing.

Romania. Romania continues to develop its anti-money laundering regime. Its geographic location makes it a natural transit country for trafficking in narcotics, arms, stolen vehicles, and illegal aliens and, therefore, vulnerable to money laundering. As in other countries in Eastern Europe, corruption and the presence of organized crime activity facilitate money laundering. The proceeds of financial crimes and the smuggling of cigarettes, alcohol, coffee, and other dutiable commodities are also believed to be laundered in Romania.

Romania 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 mandated provisions for customer identification, record keeping, reporting transactions of a suspicious or unusual nature, currency transaction reporting for transactions over 10,000 euros (approximately equivalent to \$10,000), a Financial Intelligence Unit (FIU), and internal anti-money laundering procedures and training for all domestic financial institutions covered by the law. The list of entities subject to the reporting requirements includes banks, non-bank financial institutions, attorneys, accountants, and notaries. There exists some natural discomfort on the part of the banking industry regarding requirements to assist law enforcement, but this has not stopped the Government of Romania (GOR) from establishing further measures, such as Norm No. 3, "Know Your Client." These norms, issued in February 2002 by

Money Laundering and Financial Crimes

the National Bank of Romania, bring Romania's norms into line with the Basel Committee's "Customer Due Diligence for Banks."

Romania's parliament has a new draft law on money laundering. This law revises certain provisions in the former law. First, the new law defines money laundering using the "all crimes" approach, which means that any crime may be a predicate offense rather than the former list of specific crimes. In addition, the new law expands the number and types of entities required to report to the National Office for the Prevention and Control of Money Laundering. Some of these new entities include art dealers, travel agents, privatization agents, postal officials, money transferors, and real estate agents. The new law also provides for both STR and CTR reporting, with the CTR amounts conforming to EU standards. The "Know Your Customer" identification requirements have also been honed so that identification of the client becomes necessary upon both the beginning of a relationship and upon single or multiple transactions meeting or approaching a 10,000 euro standard. This brings Romania into line with Recommendation No. 10 of the FATF 40 Recommendations on Money Laundering.

The National Office for the Prevention and Control of Money Laundering (NOPCML) is Romania's Financial Intelligence Unit (FIU). The NOPCML receives and evaluates suspicious and unusual transaction reports as well as currency transaction reports. Since its establishment the NOPCML has reviewed over 2,000 suspicious transaction reports. The law also provides for feedback to be given, upon request, to NOPCML from the General Prosecutor's Office, and for NOPCML to participate in inspections and controls in conjunction with supervisory authorities. Lastly, it provides for training and for future conferences in conjunction with international partner FIUs, specifically Italy and Austria. The Directorate of Economic and Financial Crimes of the national police also has a mandate to pursue money laundering. There have been 226 money laundering cases investigated since 2001 but none have resulted in arrests.

After 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, legislates that taking of measures, or the production of or acquisition of means or instruments with an intention to commit terrorist acts, are offenses exactly the same as terrorist acts themselves. The ordinance also discusses the character and composition of a terrorist act. These offenses are punishable with imprisonment ranging from five to twenty years. Emergency Ordinance 159, also passed in 2001, sets measures 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. The National Bank of Romania, which oversees all banking operations in the country, also issued Norm No. 5 in support of Emergency Ordinance 159. Emergency Ordinances 153 was passed to strengthen the government's ability to carry out the obligations under UNSCR 1373.

In April 2002, the GOR's Supreme Defense Council of the Country adopted a National Security Strategy, which included 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 Office, the National Bank, and the National Office for the Prevention and Control of Money Laundering.

Romania is a member of the Council of Europe (COE) and participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, formerly PC-R-EV). A mutual evaluation in April 1999 by the PC-R-EV uncovered a number of areas of concern, including the high evidence standard required for reporting suspicious transactions, a potential conflict with the bank secrecy legislation, and the lack of provisions for cases in which the reporting provisions are intentionally ignored. Romania is currently working with EU legal experts to address the PC-R-EV concerns.

The NOPCML is a member of the Egmont Group. The Mutual Legal Assistance Treaty signed in 2001 between the United States and Romania entered into force in October 2001. Romania has demonstrated

its commitment to international anti-crime initiatives by participating in regional and global anti-crime efforts. Romania is a party to the 1988 UN Drug Convention and has signed and ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. With Law No. 263/2002, passed in 2002, Romania ratified the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. During 2002, Romania also ratified the Council of Europe's Criminal Law Convention on Corruption. Romania has signed, but has not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

Romania should continue addressing the concerns of the Council of Europe evaluators as to further improvements in its anti-money laundering regime and should continue its progress on money laundering investigations and prosecutions.

Russia. Russia's ability to transform its economy and implement a new anti-money laundering program is crucial to its efforts to combat laundering of criminal proceeds domestically and internationally. The magnitude of money laundering is considered to be large, given the number and scale of contributing factors. Russia's abundance of natural resources, infiltration of society by organized crime, porous borders, geographic role as a gateway to Europe and Asia, and under-funding of regulatory and law enforcement agencies leave it vulnerable to money laundering. For example, the Russian exclave of Kaliningrad, situated between Poland and Lithuania, has a history of smuggling goods and an active black market economy. As those two countries are expected to join the European Union (EU) in 2004, control of the movement of goods and people has been a thorny issue, only recently resolved between the Russian Federation and the EU.

Capital flight, and the trade fraud often associated with it, use many of the same techniques used in money laundering. Consequently, such irregular and illegal transactions, designed to avoid Russian taxes, and the instability of the Russian economy have obscured the detection of money laundering per se. Central Bank of Russia estimates of the Russian funds that have moved through the banks chartered in Nauru alone (approximately \$70 billion in 1998) give some idea of the enormous size of the problem.

Russia's law on "Combating the Legalization (Laundering) of Income Obtained by Illegal Means" became effective on February 1, 2002. The law requires obligated financial institutions to monitor and report transactions to an authorized agency, keep records, and identify their customers. Russian financial institutions (e.g., credit organizations, securities market professionals, insurance and leasing companies, funds transfer organizations, and pawnshops) must monitor and report to the government covered transactions that exceed 600,000 rubles (approximately \$20,000). Financial institutions must also report transactions that contain certain high-risk features or when money laundering is suspected. Earlier reforms (1999) by the Central Bank of Russia (CBR) instituted regulatory measures to scrutinize offshore financial transactions. In the following six months, wire transfers from Russian banks to offshore financial centers dropped significantly. At the same time the Central Bank curtailed establishing correspondent relations with offshore banks by raising the standards for "eligible" offshore financial institutions and thereby reducing the number. More recently the CBR has been issuing strong guidelines regarding anti-money laundering practices within credit institutions.

The law also calls for an executive agency to be established as a Financial Intelligence Unit (FIU). That agency is the Financial Monitoring Committee (FMC), which is accountable to the Ministry of Finance and is staffed primarily by employees of the Ministry of Finance Currency Control Department, although the FMC is technically independent. The FMC serves as an administrative FIU, having no law enforcement investigative powers. Recent amendments to the anti-money laundering law have increased the FMC's information gathering authority to include activities of investment foundations, non-state pension funds, gambling businesses, and sales of precious metals and jewelry. Moreover, the amendments allow the FMC, in concert with banks, to freeze possible terrorist financial transactions up to one week. (Banks may freeze transactions for two days and the FMC may follow up with an additional five days.) Using encrypted software provided by the FMC, virtually all reporting from credit, securities, and insurance institutions is submitted via electronic means. The FMC anticipates opening seven regional

Money Laundering and Financial Crimes

departments in 2003. A cooperation agreement with Italy's FIU was signed on December 10, 2002. A similar agreement with the French is planned for January 2003. The FMC is a member of the Egmont Group of FIUs.

In light of the reforms to Russia's anti-money laundering regime, FATF withdrew its call for countermeasures against Russia in September 2001 and removed Russia from its list of non-cooperative jurisdictions in October 2002. The U.S. Treasury Department Advisory, which had instructed U.S. financial institutions to "give enhanced scrutiny" to all transactions involving Russia was also lifted. FATF also granted Russia observer status for the FATF plenary in February 2003. A FATF mutual evaluation is planned for 2003.

Russia holds membership in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, formerly PC-R-EV), and underwent a mutual evaluation in June 2000, which was discussed at the January 2001 meeting of the group. 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 has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. The United States and Russia signed a Mutual Legal Assistance Treaty in 1999, which entered into force on January 31, 2002. In November 2002, Russia ratified the UN International Convention for the Suppression of the Financing of Terrorism.

The Russian Federation has enacted new legislation and 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 decree's instructions to relevant agencies to seize assets of terrorist groups. This latter clause, however, conflicted with existing domestic legislation. Accordingly, on September 24, 2002, the Duma approved an amendment to the anti-money laundering law, resolving the conflict, and allowing banks to freeze assets immediately, pursuant to UNSCR 1373. This law came into force on January 2, 2003. The procedures for how this new authority will be implemented in practice are still being discussed within the GOR. Reportedly, no terrorist assets have yet been identified and seized in Russia. Following the Moscow hostage crisis, the Russian legislature took additional steps. 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 (\$100,000,000) in support of federal anti-terrorism programs and improvement of national security.

The enactment of comprehensive anti-money laundering legislation in 2001 marked a milestone in Russia's anti-money laundering regime. Russia's commitment to strengthen that regime has been demonstrated by its aggressive progress this past year. Russia should continue to build on this momentum in analysis and detection of money laundering offenses and should demonstrate its ability and political will to achieve prosecutions and convictions.

Samoa. Samoa does not have major organized crime, fraud, or drug problems. The most common crimes that generate revenue within the jurisdiction would appear to be 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 but insufficiently regulated. The Government of Samoa (GOS) enacted the Money Laundering Prevention Act (the Act) in June 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 December 2002. Under the Act, a conviction for a money laundering offense is punishable by a fine not to exceed WST \$1 million, a term of imprisonment not to exceed seven years, or both.

The Act requires financial institutions to report transactions considered suspicious to a Money Laundering Prevention Authority (MLPA), to be appointed by the Minister of Finance but currently working under

the auspices of the Governor of the Central Bank. The MLPA will receive and analyze these disclosures, and if it establishes reasonable grounds to suspect that a transaction involves the proceeds of crime, it will refer the information to the Attorney General and the Commissioner of Police.

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 exposes the financial institutions to potential abuse. As it is written, financial institutions are under no obligation to maintain any record for single transactions where the amount is under WST \$30,000, so numerous small transactions could avoid detection. Nevertheless, Section 4.3(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 Samoan Tala \$30,000, or the equivalent in another currency.” 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.” The new Regulations and Guidelines also 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 new Money Laundering Prevention Guidelines for the Financial Sector provides that “...If funds to be deposited or invested are being supplied by or on behalf of a third party, the identity of the third party (i.e., 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 Office of the Registrar of International and Foreign Companies, and the MLPA regulate the financial system. There are three locally incorporated commercial banks, supervised by the Central Bank. The Office of the Registrar of International and Foreign Companies has responsibility for regulation and administration of the offshore sector. There are no casinos, but two local lotteries are in operation.

Samoa is an offshore financial center, with eight offshore banks licensed. 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 eight offshore banks, Samoa currently has 7,553 international business corporations (IBCs), five international insurance companies, six trustee companies, and 157 international trusts. Section 16 of the Offshore Banking Act does not prohibit persons who have been sentenced for an offense involving dishonesty from applying to be employed as directors or managers of offshore banks. The Act only requires prior approval, in writing, of the Minister, without setting any criteria to guide the decision. In addition, there is no provision in the Act that specifies the qualifications for an owner/shareholder of an offshore bank. IBCs may be registered using bearer shares and shelf companies that conceal the identity of the beneficial owner and the date of incorporation. Corporate entities may be listed as officers and shareholders because Samoan IBCs have all the legal powers of a natural person. There are no requirements to file annual statements or annual returns. These provisions make IBCs particularly attractive to money launderers, and Samoan authorities have not yet addressed them.

International cooperation can only be provided when 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. The inability of the MLPA simply to exchange information on an administrative level is a material weakness of the current system. The GOS is, however, drafting legislation

to remedy this weakness and seeks to adopt a Mutual Assistance Bill, based on the Commonwealth Secretariat model, that will be request-, not treaty-driven.

Samoa signed the UN International Convention for the Suppression of the Financing of Terrorism in November 2001, and ratified it on September 27, 2002. Consonant with this action, and with Samoa's strong and vocal support for anti-terrorism efforts, was the passage in April 2002 of the Prevention and Suppression of Terrorism Act. This legislation defines and provides for terrorist offenses, including offenses dealing specifically with 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 provide assistance to a criminal to obtain, conceal, retain or invest funds or to finance or facilitate the financing of terrorism.

Samoa is a member of the Asia/Pacific Group on Money Laundering and the Pacific Island Forum. Samoa has not signed the 1988 UN Drug Convention.

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. The GOS should work to ensure that this legislation becomes fully operational. Particular emphasis should be directed toward regulation of the offshore financial sector, principally the establishment of due diligence procedures for owners and directors of banks and the elimination of anonymous accounts for onshore and offshore banks. The GOS should enact 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 should adopt its pending legislation to allow for international cooperation and information sharing.

Sao Tome and Principe. Sao Tome, which has a small economy and only one commercial bank, is not a regional financial center.

Sao Tome is a party to the 1988 UN Drug Convention.

Sao Tome should criminalize money laundering and terrorist financing. Sao Tome should also enact legislation allowing the GOSTP to freeze assets related to money laundering and terrorist financing.

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 narcotics-trafficking and other traditional predicate offenses. There is believed to be some money laundering related to terrorist financing. However, Saudi Arabia has increased its attention on money laundering activity following the September 11 terrorist attacks and has made contributions in the war on terrorist financing. Nevertheless, there are a number of vulnerabilities that need to be addressed.

In Saudi Arabia, money laundering is a crime based on a Quranic passage stating, "Assets arising from illegal acts shall be forbidden and confiscated." It is subject to prosecution based on Sharia (Islamic) law, the Banking Control Law, and Saudi Arabian labor law. Jurisdiction over money laundering offenses lies in the Sharia courts. Saudi Arabia has had a small number of prosecutions for money laundering that originated from the filing of suspicious transaction reports. There is currently a proposal to draft a specific law dealing with money laundering offenses.

Saudi law prohibits non-resident individuals or corporations from opening bank accounts in Saudi Arabia without the specific authorization of the Saudi Arabian Monetary Authority (SAMA). SAMA guidelines correspond to Financial Action Task Force (FATF)'s 40 Recommendations, and specifically require banks to enforce "know your customer rules," maintain records of suspicious transactions, and inform SAMA of suspicious transactions. Saudi Arabia carries out regular inspection of banks to ensure compliance of laws and regulations. SAMA has been active in providing anti-money laundering training to Saudi financial institutions. The GOSA has established an anti-money laundering unit in SAMA and has required Saudi banks to have specialized anti-money laundering units and staff to work with SAMA and law enforcement authorities. The GOSA has also recently created a Financial Intelligence Unit (FIU) in the Security and

Drug Control Department of the Ministry of the Interior. The new FIU is tasked with handling money laundering cases and coordinating its activities with SAMA and appropriate law enforcement agencies.

Saudi Arabia has signed the International Convention for Suppression and Financing of Terrorism based on UNSCR 1373. Saudi Arabia has frozen accounts of individuals and organizations in response to information provided by the U.S. Government. The GOSA signed a multilateral agreement under the auspices of the Arab League to fight terrorism. Saudi Arabia has also invited the FATF to carry out a mutual evaluation in early 2003 against the FATF 40 Recommendations and the Special Eight Recommendations on Terrorist Financing.

Hawala transactions outside banks and licensed moneychangers are illegal in Saudi Arabia. Reportedly, many 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 and created fast, efficient, high quality, and cost-effective fund transfer systems. An important advantage for the authorities is that the senders and users of fund transfers are clearly identified.

Saudi Arabia has established a High Commission for oversight of all charities. Charities in Saudi Arabia are supposed to be licensed, registered, audited, and supervised. Contributions to charities are usually Zakat, which is an Islamic religious duty with specified humanitarian purposes. However, hundreds of millions of dollars in charitable donations leave Saudi Arabia every year and, wittingly or unwittingly, some of these funds have been channeled to terrorist organizations. New guidelines, regulations, and financial control mechanisms have been proposed to help counteract the misuse of charitable donations.

Saudi Arabia should pass specific anti-money laundering and anti-terrorist financing laws. Progress is being made in establishing one centralized FIU. However, as in many countries in the region there is an over-reliance on suspicious transaction reporting to generate money laundering investigations. Law enforcement agencies should take the initiative and proactively generate investigations. More emphasis should be put on the misuse of trade and commodities to launder funds. Saudi Arabia should move rapidly to enforce the new regulations and guidelines established to counteract the misuse of charitable donations.

Senegal. Senegal's banking system and formal and informal money-exchange systems are vulnerable to the laundering of proceeds from corruption, narcotics-trafficking, illegal gems and arms-trafficking, and trafficking in persons, all of which are prevalent in West Africa. Numerous foreign banks, including several French and African banks, have branches in Senegal.

Article 102 of Senegal's 1997 drug code criminalizes narcotics-related money laundering as a misdemeanor punishable by up to 10 years in prison. The last money laundering prosecution under this law was in 1999. The drug code requires banks to report suspicious transactions believed to be linked to narcotics-trafficking. Banks are required to keep records between one and ten years, depending on the type of record. The drug law authorizes the seizure of assets related to narcotics-trafficking. Banking secrecy provisions can only be waived by a judge's order as part of case involving narcotics. There is no requirement to report cross-border currency transactions.

The Government of Senegal (GOS) is considering an anti-money laundering law that would apply to banks, non-bank financial institutions, and intermediaries. The proposed law would criminalize money laundering for many serious crimes. Under the law, banking information could be shared with law enforcement authorities, and individuals could be held legally responsible if they do not report suspicious activity. The law would also expand current asset seizure provisions so that authorities could seize assets related to the laundering of proceeds from many serious crimes. The law would also establish a Financial Intelligence Unit.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA), based in Dakar, Senegal. In November 2002, the

Money Laundering and Financial Crimes

GIABA hosted an anti-money laundering seminar for representatives of 14 of the 15 ECOWAS members, including Senegal. A Senegalese magistrate is the acting head of GIABA.

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): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal, and Togo, all of which use the French-backed CFA franc currency. All bank deposits over approximately \$7,700 made in BCEAO member countries must be reported to the BCEAO, along with customer identification information.

In September 2002, the WAEMU Council of Ministers, which oversees the BCEAO, approved an anti-money laundering regulation applicable to banks and other financial institutions, casinos, travel agencies, art dealers, gem dealers, accountants, attorneys, and real estate agents. The regulation is subject to review by member countries, which would be responsible for implementing many provisions of the regulation. The regulation is expected to go into effect in early 2003.

Under the WAEMU regulation, financial institutions would be required to verify and record the identity of their customers before establishing any business relationship. The regulation would require financial institutions to maintain customer identification and transaction records for ten years. The regulation would also impose certain customer identification and record maintenance requirements on casinos.

All financial institutions, businesses, and professionals under the scope of the WAEMU regulation would be required to report suspicious transactions. The regulation calls for each member country to establish a National Office for Financial Information Process (CENTIF), which would be responsible for collecting suspicious transactions and would have the authority to share information with other CENTIFs within the WAEMU as well as with the Financial Intelligence Units of non-WAEMU countries.

The WAEMU Council of Ministers issued another directive in September 2002 requesting member countries to pass legislation requiring banks to freeze the accounts of any persons or organizations designated by the UN 1267 Sanctions Committee.

In 2001 the BCEAO hosted a conference on money laundering. In July 2002 Senegal participated in the 2002 West African Joint Operation Conference (WAJO) that promotes regional law enforcement cooperation against drug trafficking, terrorism, and money laundering.

Senegal is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the United Nations Convention against Transnational Organized Crime, which is not yet in force internationally.

Senegal should criminalize terrorist financing and money laundering for all serious crimes. The GOS should work with its partners in WAEMU to establish a comprehensive anti-money laundering regime in the region.

Seychelles. Seychelles is not a major financial center, but it does have a developed offshore financial sector, which makes the country vulnerable to money laundering.

The Government of Seychelles (GOS), in efforts to diversify its economy beyond tourism, has taken steps to develop an offshore financial sector to increase foreign exchange earnings. The GOS actively markets Seychelles as an offshore financial and business center that allows the registration of non-resident companies. There are currently over 4,800 registered international business companies (IBCs) in Seychelles that pay no taxes in Seychelles, and are not subject to foreign exchange controls. The Seychelles International Business Authority (SIBA), which acts as the central agency for the registration for IBCs, promotes the fact that IBCs need not file annual reports. The SIBA is part of the Ministry of International Trade, and also manages the Seychelles International Trade Zone. In addition to IBCs, Seychelles permits offshore trusts (registered through a licensed trustee), offshore insurance companies, and offshore banking.

A major weakness of the Seychelles' offshore program is that it still permits the issuance of bearer shares, a feature that can facilitate money laundering by making it extremely difficult to identify the beneficial owners of an IBC. Seychelles officials stated in 2000 that they were reviewing the question of bearer

shares and intended to outlaw them. In the interim, the GOS has indicated that it will not approve the issuance of any more bearer shares.

In 1996, the GOS enacted the Anti-Money Laundering Act (AMLA), which criminalizes the laundering of funds from all serious crimes, requires financial institutions and individuals to report to the Central Bank transactions involving suspected cases of money laundering, and establishes safe harbor protection for individuals and institutions filing such reports. The AMLA imposes record keeping and customer identification requirements for financial institutions, and also provides for the forfeiture of the proceeds of crime. 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 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.

In 1998, the Central Bank of Seychelles issued a comprehensive set of guidance notes that further elucidated and strengthened the provisions of the 1996 Act. The Central Bank of the Seychelles receives and analyzes suspicious activity reports and disseminates them to the competent authorities.

In 2000, the GOS repealed the 1995 Economic Development Act (EDA). The EDA provided concessions (protection from asset seizure and immunity from prosecution for crimes committed abroad and most crimes, other than violent crimes and narcotics-trafficking, committed in the Seychelles) to individuals investing more than \$10 million in the Seychelles.

The Seychelles is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. The Seychelles is a party to the 1988 UN Drug Convention. The Seychelles has signed, but not yet become a party to, both the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

The GOS should criminalize terrorist financing. The GOS should expand its anti-money laundering efforts by moving to immobilize bearer shares and requiring complete identification of beneficial owners of IBCs. The GOS should establish a Financial Intelligence Unit to collect, analyze, and share financial data with foreign counterparts, in order to effectively combat money laundering and other financial crimes. Seychelles should also actively participate in ESAAMLG.

Sierra Leone. Sierra Leone, which has a small commercial banking sector, is not a regional financial center. Loose oversight of financial institutions, weak regulations, rampant corruption, and a prevalent informal money-exchange system create an atmosphere conducive to money laundering. Given the importance of the large diamond sector to the economy, the prevalence of money laundering in the diamond sectors of neighboring countries and the loose oversight of the financial sector, Sierra Leone's diamond sector is particularly vulnerable to money laundering.

There is no specific legislation concerning money laundering. However, the Ministry of Justice is in the process of developing such laws. Banks are required to record the identity of customers engaging in large currency transactions and to maintain adequate records necessary to reconstruct significant transactions in order to respond to government information requests. Banks are also required to report suspicious transactions, although they do not usually adhere to this requirement. Bank secrecy laws prevent the disclosure of client and ownership information except under court order.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA), based in Dakar, Senegal. In November 2002, GIABA hosted an anti-money laundering seminar for representatives of 14 ECOWAS members, including Sierra Leone.

Money Laundering and Financial Crimes

Sierra Leone is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Sierra Leone has signed, but has not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

Sierra Leone should criminalize money laundering and terrorist financing, enforce existing financial laws and regulations, and provide legal authority for the seizure of criminal and terrorist assets.

Singapore. As a significant international financial and investment center, and in particular a major offshore financial center, Singapore is attractive to potential launderers. Bank secrecy laws and the lack of routine currency reporting requirements may make Singapore an attractive destination to foreign drug traffickers, other foreign criminals and terrorist organizations and their supporters seeking to launder their money, and for flight capital. Money laundering occurs mainly in the offshore sector, but may also occur in the non-bank financial system, including extensive moneychangers and remittance agencies. As of December 7, 2002, there were 59 offshore banks, down significantly from 83 in December 2000; all are branches of foreign banks. Singapore does not permit shell banks, either in the domestic or offshore sectors. There are no offshore trusts, although banks may open trust, nominee, and fiduciary accounts. All banks in Singapore, whether domestic or offshore, are subject to the same regulation, record keeping and reporting requirements. There are also hundreds of offshore international and financial service businesses. An offshore company must have a locally registered office with a physical address and a minimum of two directors, at least one of who must be a Singaporean citizen, permanent resident, or employment pass holder. A company incorporated in Singapore has the same status and powers as a natural person. Bearer shares are not permitted. Casinos or Internet gaming sites are illegal in Singapore.

The Corruption, Drug Trafficking, and other Serious Crimes (Confiscation of Benefits) Act of 1999 (CDSA) criminalizes the laundering of proceeds from narcotics and over 150 other offenses. Financial institutions must report suspicious transactions and positively identify customers engaging in large currency transactions. Financial institutions are required to maintain adequate records to respond quickly to Government of Singapore (GOS) inquiries in money laundering cases. However, there are no reporting requirements on amounts of currency brought into or taken out of Singapore.

The Monetary Authority of Singapore (MAS), a semi-autonomous entity under the Ministry of Finance, serves as Singapore's Central Bank and financial sector regulator. MAS performs extensive prudential and regulatory checks on all applicants for banking licenses, including a check to see if the bank is under adequate home country banking supervision. Banks must have clearly identified directors. It is illegal to perform banking transactions without a license. In 2000, MAS issued a series of regulatory guidelines (i.e., "Notices") requiring banks to apply "know your customer" standards, adopt internal policies for staff compliance, and cooperate with enforcement agencies on money laundering cases. Banks must obtain documentation, such as passports or identity cards, from all personal customers so that the bank can verify their names, permanent contact addresses, dates of birth, and nationalities, and conduct inquiries into 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. The guidelines 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. MAS Notice 626 applies to banks, Notice 824 applies to finance companies, Notice 1014 applies to merchant banks, and Notice 314 to direct life insurers and brokers. MAS issued similar guidelines for securities dealers and investment advisors, and futures brokers and advisors.

The Suspicious Transaction Reporting Office (STRO), part of the Singapore Police Force's Commercial Affairs Department, began operating on January 10, 2000, and receives and analyzes suspicious transaction reports filed by financial institutions. It is also authorized to exchange intelligence derived from these reports with foreign counterparts.

The Terrorism (Suppression of Financing) Act, passed in 2002, 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 Act, which supplements and extends interim legislation enacted in November 2001, took effect January 29, 2003.

Separate legislative authority, Section 27A(1)(b) of the Monetary Authority of Singapore Act, as amended in 2002, provides MAS with broad powers to direct financial institutions to comply with international obligations, including UN Security Council Resolutions 1267, 1333, 1373, 1390 and other similar resolutions. Regulations issued by the MAS to implement this authority took effect September 30, 2002. The regulations—S 515/2002, the MAS (Anti-Terrorism Measures) Regulations 2002—bar banks and financial institutions from providing resources and services of any kind which will benefit terrorists and from doing “anything that...assists or promotes” terrorist financing. Financial institutions must notify the MAS immediately if they have in their possession, custody or control any property belonging to terrorists or any information on transactions involving terrorists’ funds. The regulations apply to all branches and offices of any financial institution incorporated in Singapore, or incorporated outside of Singapore but which are located in Singapore.

The MAS, on October 9, 2001, issued Circular FSG 48/2001, instructing financial institutions in Singapore to comply with a series of circulars intended to implement UNSCR 1373, including a freeze on assets possessed or controlled by any person known to have committed or attempted to commit acts of terrorism. MAS previously issued Circular FSG 5/2001 to implement UNSCR 1267, and FSG 6/2001 to implement UNSCR 1333. MAS issued revised circulars updating the freeze order after new names were added to the UNSCR 1267 consolidated list, although the process was not immediate. Singapore officials say they have not identified any assets in Singapore of persons included in the UNSCR 1267 consolidated list.

Alternative remittance systems exist, and are used mainly by the approximately 600,000 foreign workers in Singapore. All remittance agents, formal or informal, must be licensed and are subject to the same laws and regulations, including requirements for record keeping and the filing of suspicious transaction reports. Informal networks that are not licensed are considered illegal.

Charities in Singapore are subject to extensive government regulation, including close oversight and reporting requirements, and restrictions that limit the amount of funding which can be transferred out of Singapore. With a few exceptions, all charities must register with the Government, and must, as part of the registration process, submit governing documents outlining the charity’s objectives and particulars on all trustees. The Commissioner of Charities has the power to investigate charities, including authority to search and seize records, and to restrict the transactions the charity can enter into, suspend charity 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.

Under the “Charities (Fund-raising Appeals for Foreign Charitable Purposes) Regulations 1994,” any charity or person who wishes to conduct or participate in any fund raising for any foreign charitable purpose must apply for a permit. The applicant has to show that at least 80 percent of the funds raised will be used in Singapore, although the Commissioner of Charities has discretion to allow a lower percentage to be applied within Singapore. Permit holders are subject to additional record keeping and reporting requirements, including details on every item of expenditure disbursed, amounts transmitted to persons

Money Laundering and Financial Crimes

outside Singapore, and to whom the money was transmitted. There do not appear to be any restrictions or reporting requirements on foreign donations to charities in Singapore.

Singapore is party to the 1988 UN Drug Convention, and in December 2000 signed, but has not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Singapore signed and ratified the UN International Convention for the Suppression of the Financing of Terrorism. Singapore is a member of the Financial Action Task Force, the Asia/Pacific Group on Money Laundering, the Egmont Group, and the Offshore Group of Banking Supervisors. To bolster law enforcement cooperation and facilitate information exchange, Singapore enacted the Mutual Assistance in Criminal Matters Act (MACM) in March 2000. The MACM provides for cooperation on any serious criminal offense. The provisions of the MACM apply to countries that have concluded treaties, memoranda of understanding, or other agreements with Singapore. 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 in November 2000, the first agreement concluded pursuant to the MACM. This agreement facilitates the exchange of banking and corporate information on drug money laundering suspects and targets, to include access to bank records. The Terrorism (Suppression of Financing) Act provides for mutual legal assistance in cases where there is no treaty, MOU or other agreement in force between Singapore and another country that is a party to the UN International Convention for the Suppression of the Financing of Terrorism. Singapore's FIU has concluded MOUs concerning cooperation in the exchange of financial intelligence with counterparts in Australia and Belgium.

The GOS should continue close monitoring of its domestic and offshore financial sectors. As a major financial center, it should also take measures to regulate and monitor large currency movements into and out of the country to ensure that international criminals, terrorists, terrorist organizations or their supporters do not misuse Singapore's financial system.

Slovakia. 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, arms, stolen vehicles, and illegal aliens. 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 conducting illegal business have been quite problematic for Slovak authorities. Non-bank financial institutions, which have been particularly susceptible to laundering, were brought under the transaction reporting requirements in January 2001.

With the law "On Protection Against the Legalization of Proceeds from Criminal Activities", also known as Act No. 367/2000, Slovakia criminalizes money laundering for all serious crimes and imposes customer identification, record keeping, and suspicious transaction reporting requirements on banks. As noted above, in January 2001, non-bank financial institutions (casinos, post offices, brokers, stock exchanges, commodity exchanges, asset management companies, insurance companies, real estate companies, tax advisors, auditors, and credit unions) became subject to suspicious transaction reporting requirements. New anonymous passbook savings accounts are banned as of October 2000. In 2002, legislative amendments abolished all existing bearer passbooks and extended reporting requirements to art and gem dealers, legal advisors, consultants, and accounting services.

Slovakia's Financial Intelligence Unit (FIU), the OFiS of the Bureau of Financial Police (UFP), has jurisdictional responsibilities over money laundering violations. Established in 1996, the OFiS-UFP receives and evaluates suspicious transaction reports, and collects additional information to establish the suspicion of money laundering. Once enough information has been obtained to warrant suspicion that a criminal offense has occurred, the OFiS-UFP forwards the case to the State Prosecutor's Office for investigation and prosecution. Since its establishment in 1996, through 2001, the UFP has received 1,628 reports alleging suspicious transactions totaling SKK 89.7 billion (\$2.2 billion). Approximately seven

percent of those reports led to criminal prosecutions. Recently, the FIU was divided into three departments. A receptor branch receives and disseminates reports from the obligated entities. A supervisory branch ensures the cooperation of the reporting entities as well as international cooperation. The analytical branch does the actual analysis. OFiS-UFP analysts participate regularly in international and domestic fora related to combating money laundering.

Slovakia ratified the UN International Convention on the Suppression of the Financing of Terrorism on September 13, 2002. The Convention has been incorporated into amendments of the Bank Act, Penal Code and Act No. 367/2000. However, Slovakia elected to pursue several optional terms of the convention that will be fully incorporated no later than March 31, 2003. All competent authorities in the Slovak Republic have full legislative power to freeze or confiscate terrorist assets in accordance with UN Resolution 1373. No terrorist finance related accounts have been frozen or seized in Slovakia.

Slovakia is a party to the European Convention on Mutual Legal Assistance and became a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime in 2001. Slovakia is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. 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 Council of Europe (COE) and participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, formerly known as PC-R-EV). Slovakia sends experts to conduct mutual evaluations on fellow member countries; it also underwent mutual evaluations by this group in 1998 and 2001. As a result, Slovakia has been implementing changes to its money laundering regime based on the recommendations put forth in the reports.

The OFiS-UFP is a member of the Egmont Group. Slovakia has an MOU with the financial intelligence units of Slovenia, Belgium, Poland and the Czech Republic, and a letter of exchange with the FIU of Slovenia. The OFiS-UFP 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 should continue to improve its anti-money laundering legislation. Continued implementation of the provisions of Slovakia's new anti-money laundering legislation will give the Slovak financial system greater protection by helping it prevent and detect money laundering in all financial sectors. Slovakia should also criminalize terrorist financing.

Slovenia. Slovenia's economic stability and location on the Balkan drug route offer attractive opportunities for money laundering. Narcotics-trafficking, which is a growing problem, is the main source of illegal proceeds. Other significant sources of illegal proceeds are fraud, trafficking in weapons, illegal immigration, and currency and securities counterfeiting, as well as extraterritorial offenses such as tax evasion, tax and VAT fraud, and corruption. Organized crime is believed to be involved in both predicate crimes and laundering operations. Money laundering often tends to be undertaken by citizens of the other former state socialist countries, using non-resident accounts. Slovenia's Financial Intelligence Unit, the Office for Money Laundering Prevention (OMLP), is a member of the Egmont Group.

Slovenia's Law on the Prevention of Money Laundering was enacted in 1994 and amended in 2001. The law criminalized money laundering and requires all financial institutions, casinos, and legal persons to report suspicious transactions and currency transactions above 5 million Slovenian Tolars (approximately \$23,000.) Records must be retained for a minimum of five years.

In October 2001, the Slovenian Parliament passed an anti-money laundering law that updated the original 1994 law by, among other provisions, expanding the OMLP's sources of available financial information, extending OMLP's authority to temporarily halt suspect transactions, and requiring mandatory client identification for transactions exceeding 3 million Slovenian Tolars (approximately \$13,699). December 2001 saw the passage of a new law that would increase the power of supervisory authorities to prohibit the

Money Laundering and Financial Crimes

establishment of new bearer passbook accounts, as well as phase out already-existing bearer passbook accounts. Further amendments to the law, which extended reporting obligations to lawyers, law firms, notaries, auctioneers, art dealers, gaming houses, and lottery concessions, were passed and entered into force in July 2002. A special Financial Crime Division was established within the General Police Directorate in 2000 and is in charge of conducting preliminary investigations into money laundering cases, as well as into other economic crimes. Other active financial supervisory bodies include the Bank of Slovenia, the Securities Market Agency, the Insurance Supervisory Agency, and the Office for Gaming Supervision.

Slovenia is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, formerly PC-R-EV) and has undergone a mutual evaluation by the Committee, as well as lending its own experts to evaluate other member countries. Slovenia is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Slovenia is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Slovenia has signed, but not yet become a party to, the UN International Convention for the Suppression of Financing of Terrorism. Slovenia should pass specific anti-terrorist financing legislation.

Solomon Islands. The Solomon Islands is not a regional financial center. The Islands' banking system is small. The country has not criminalized money laundering.

The Solomon Islands is not a party to the 1988 UN Drug Convention.

The Solomon Islands should criminalize terrorist financing and money laundering for all serious crimes. The Solomon Islands should sign the UN International Convention for the Suppression of the Financing of Terrorism.

South Africa. South Africa's position as the major financial center in the region and its relatively sophisticated banking and financial sector make that nation a very attractive target for transnational criminal syndicates. South African officials report that over 150 criminal groups operate within the country. Reports indicate that many of these criminal organizations are of West African and South African origin, along with the Russian Mafia and Chinese Triads. Kidnapping, fraud, stolen vehicles, human trafficking, narcotics, diamond and weapons smuggling, and money laundering are major criminal activities challenging local law enforcement. Reportedly, between \$2 and \$8 billion are laundered through South African institutions every year.

The Proceeds of Crime Act, No. 76 of 1996, criminalizes money laundering for all serious crimes. In 1998, the Prevention of Organized Crime Act, No. 121 (POCA), was promulgated, which supersedes the previous Act. The POCA also criminalizes money laundering, mandates the reporting of suspicious transactions, and provides a "safe harbor" for good faith compliance. Subsequent regulations direct that these reports be sent to the Commercial Crime Unit of the South African Police Service. Both of these Acts contain criminal and civil forfeiture provisions. However, the Government of South Africa (GOSA) has been unsuccessful in its efforts to implement the law. The POCA was amended several times, and several challenges to arrests and seizures are pending.

In November 2001, the National Council of Provinces, the upper chamber of parliament, passed the Financial Intelligence Center Bill (FICB). The FICB provides for the establishment and staffing of a Financial Intelligence Center (FIC) that will coordinate policy and efforts to counter money laundering activities. The FIC will similarly act as a centralized repository of information. The FICB creates new legal categories of accountable and reporting institutions. These include companies and businesses considered particularly vulnerable to money laundering activities, such as banks, life insurance companies, foreign exchange dealers, casinos, and real estate agents. FICB requires these institutions to report suspicious transactions, identify customers, maintain records of transactions for at least five years, and appoint compliance officers to train employees to comply with the law. Suspicious transactions are to be reported

to the FIC. If the FIC has reasonable grounds to suspect that a transaction involves the proceeds of criminal activities, the FIC will forward this information to the investigative and prosecutorial authorities.

The FICB also establishes a Money Laundering Advisory Council to advise the Minister of Finance on policies and measures to combat money laundering. Regulations to implement the FICB have received final approval by Parliament and the Minister of Finance. As a result, accountable institutions will begin reporting to the FIC in February. Officials in South Africa report that the FIC will be operational in early March of 2003.

The GOSA became a signatory to the UN International Convention for the Suppression of the Financing of Terrorism on November 10, 2001. Officials indicate plans to draft anti-terrorism legislation, which are expected to be promulgated by the summer of 2003. In part, this proposed legislation will give the FIC the responsibility to track terrorist funding.

South Africa is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime, which is not yet in force internationally. The United States and South Africa have concluded a bilateral extradition treaty and a Mutual Legal Assistance Treaty, both of which entered into force on June 25, 2001. South Africa is an active member of the Eastern and Southern African Anti-Money Laundering Group.

Although the GOSA has criminalized money laundering for all serious crime, and passed additional legislation necessary to construct a viable anti-money laundering regime, the GOSA should take steps to ensure its implementation of these laws. Additionally, the GOSA should enact legislation criminalizing terrorist financing. Unless it does so, South Africa's financial institutions will remain vulnerable to abuse by organized crime and misuse by terrorist organizations and their supporters.

Spain. Money laundering in Spain results primarily from the proceeds of the cocaine trade. There is also a significant black market for smuggled goods. The laundering occurs primarily in the financial system, although there are indications that money is also laundered through the real estate sector and the informal financial centers sometimes used by the immigrant community as an informal remittance system. Drug traffickers continue to resort to courier networks to remit large amounts of bulk cash to South America and the Middle East.

The Government of Spain (GOS) remains committed to combating narcotics-trafficking, terrorism, and financial crimes. Its 1993 Anti-Money Laundering Law (No. 19) and corresponding 1995 regulations cover money laundering linked to illicit drugs, terrorism, and organized crime. The financial sector is required to identify customers, keep records of transactions, and report suspicious financial transactions. The Commission for the Prevention of Money Laundering and Monetary Offenses coordinates the GOS's anti-money laundering efforts and carries out regulatory and training functions for the financial sector. The financial sector includes banks, mutual savings associations, insurers, financial advisers, postal services, currency exchange outlets, and casinos.

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. Currently, the GOS can freeze terrorist financial assets only if such action has been approved by an international organization such as the United Nations or European Union, or if a judge orders the freezing. The UNSCR 1267 consolidated list of individuals and entities has been distributed to the Spanish financial community. A bill is pending before the Spanish Parliament that would facilitate the administrative freezing of bank accounts of terrorist groups and individuals. Passage is expected in the first quarter of 2003.

The Executive Service of the Commission for the Prevention of Money Laundering (SEPBLAC) serves as Spain's Financial Intelligence Unit. SEPBLAC receives and analyzes suspicious activity reports and forwards those that may indicate money laundering to law enforcement agencies.

Businesses and financial service suppliers operating in Spain or targeting Spanish markets are subject to a new law, Ley de Servicios de la Sociedad de Informacion y de Comercio Electronico (LSSICE), that came

Money Laundering and Financial Crimes

into force on October 12, 2002, for Internet marketing and distribution. The new law requires businesses to register their domain names, company registry, physical address, and other company details. Financial sector businesses such as online banks must still send written contracts to new customers for signature and obtain physical proof of their identity, in order to comply with existing banking regulations.

Spain is a member of the FATF, 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). It ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally, on March 2, 2002, and the UN International Convention for the Suppression of the Financing of Terrorism on April 9, 2002. Spain is also a party to the 1988 UN Drug Convention. SEPBLAC is a member of the Egmont Group.

Spain 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. Spain also has entered into bilateral agreements for cooperation and information exchange on money laundering issues with Bolivia, Chile, El Salvador, France, Israel, Italy, Malta, Mexico, Panama, Portugal, Russia, Turkey, Venezuela, Uruguay, and the United States. Spain actively collaborates with Europol, supplying and exchanging information on terrorist groups.

Spain should continue the strong enforcement of its anti-money laundering program and its leadership in the international arena. It should consider whether additional measures are required to address possible money laundering in the stock market to ensure that the sector is not used for financial crimes.

Sri Lanka. Sri Lanka is neither an important regional financial center nor a preferred center for money laundering. Hawala is practiced as an alternative remittance system. While Sri Lanka recently experienced a failure of a small savings bank due to fraud by senior bank officials, there has been no evidence linking their activities to money laundering or terrorist financing.

As of January 2003, a draft law to deal with money laundering has been approved by the Central Bank and sent to the Ministry of Justice for review and presentation to cabinet and parliament. Currently, financial transactions relating to terrorism and narcotics are illegal under Central Bank regulations and Bank Secrecy laws. In December 2001, the Central Bank introduced regulations on customer due diligence. However, the Central Bank continues to allow the operation of bearer certificates of deposits. Terrorist financing is an offense punishable by imprisonment for a period of five to ten years. The Central Bank of Sri Lanka has circulated the list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list with instructions to identify, freeze and seize terrorist assets. To date no such assets have been identified. Sri Lanka is a party to the UN International Convention for the Suppression of the Financing of Terrorism and to the 1988 UN Drug Convention.

Regulations under the Sri Lankan legislation provide for freezing and forfeiture of assets of individuals and entities involved with the financing of terrorism. There is no specific provision in the law to freeze and forfeit narcotics related assets; however, trafficking, possessing, importing or exporting of narcotics is punishable by death or life imprisonment under the Poisons, Opium and Dangerous Drugs Ordinance (OPDDO).

Draft amendments to OPDDO and a separate draft money laundering bill are expected to include asset forfeiture and seizure provisions for narcotics-related crimes and money laundering. Sri Lanka should pass the draft money laundering legislation, criminalize the financing of terrorism and begin steps to implement an anti-money laundering program, which would include training of law enforcement and customs on how to recognize and investigate money laundering.

St. Kitts and Nevis. The Government of St. Kitts and Nevis (GOSKN) is a federation composed of two islands in the Eastern Caribbean, but each island has the authority to organize its own financial structure. The federation is at major risk for corruption and money laundering due to the high volume of narcotics-trafficking activity through and around the islands and the presence of known traffickers on the islands,

two of whom are the subjects of an important and long-standing U.S. extradition request. An inadequately regulated economic citizenship program adds to the problem.

Most of the financial activity in the federation is concentrated in Nevis, whose economy has become increasingly dependent upon the fees generated by the registration of offshore entities. The Nevis offshore sector has one offshore bank (a wholly owned subsidiary of a domestic bank) approximately 17,000 international business companies and 3,000 trusts. The Nevis domestic structure consists of five domestic banks, four domestic insurance companies (all of which are subsidiaries of St. Kitts companies), one money remitter and 65 trust and company service providers. In St. Kitts, there are four domestic banks, 2 credit unions, four domestic insurance companies, two money remitters and 15 company service providers. There are also 13 trusts and 450 exempt companies. A regional stock exchange, common to the members of the Organization of Eastern Caribbean states (OECS) and supervised by a regional regulator, is located in St. Kitts. There is one casino in St. Kitts and the government is expected to issue two other casino licenses.

Legislation for Internet gaming is in place, but no licenses have yet been issued. The Eastern Caribbean Central Bank has direct responsibility for regulating and supervising the offshore bank in Nevis, as it does for the domestic sector in the entire GOSKN, and for making recommendations regarding approval of offshore bank licenses.

No evidence of terrorist financing has yet been known to be developed in St. Kitts and Nevis. Subsequently, St. Kitts and Nevis enacted the Anti-Terrorism Act #21, effective November 27, 2002. Sections 12 and 15 of the Act criminalize terrorist financing. The Act implements various UN Conventions against terrorism. The GOSKN has some existing controls that apply to alternative remittance systems but has undertaken no initiatives that apply directly to the potential terrorist misuse of charitable and non-profit entities.

In June 2000, FATF placed St. Kitts and Nevis on the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering. The FATF in its report cited several concerns surrounding the anti-money laundering regime of St. Kitts and Nevis. Among the problems identified by FATF were the narrow definition of money laundering as a punishable offense, the absence of mandatory suspicious transaction reporting and the lack of effective supervision of the Nevis offshore sector. In July 2000, the U.S. Treasury Department issued an advisory to U.S. financial institutions, emphasizing the need for enhanced scrutiny of certain transactions and banking relationships in St. Kitts and Nevis to ensure that appropriate measures are taken to minimize risk for money laundering. As a result of the legislative changes addressed below as well as the responsiveness of the GOSKN to requests for mutual legal assistance and other financial sector regulatory inquiries; however, the FATF, with certain on-going follow-up conditions, removed the GOSKN from the NCCT list in June 2002. The U.S. Treasury Department removed its Financial Advisory in August 2002.

In response to the initial FATF 2000 listing of St. Kitts and Nevis, the GOSKN began to take significant steps to address the deficiencies in its anti-money laundering regime as well as to build up its oversight infrastructure. The Proceeds of Crime Act No. 16 of 2000 criminalized money laundering from serious offenses (defined to include more than drug offenses) and imposed penalties ranging from imprisonment to monetary fines. The Act also overrides secrecy provisions that may have constituted obstacles to the access of information with respect to account holders or beneficial owners on the part of administrative and judicial authorities.

In addition, the Financial Intelligence Unit Act No. 15 of 2000 authorized the creation of a Financial Intelligence Unit (FIU). The FIU began operations in 2001 and has a director, deputy director, two legal representatives and five police officers. The FIU is to receive, collect and investigate suspicious activity reports (SARs); it is also charged with liaising with foreign jurisdictions. The FIU continues to receive computers and other assistance from the USG as well as management and asset forfeiture mentoring from the USG and the Caribbean Anti-Money Laundering Program a program jointly funded by the United States, the United Kingdom and the European Union.

Money Laundering and Financial Crimes

Other measures designed to remedy shortcomings in St. Kitts and Nevis' anti-money laundering regime have included the Financial Services Commission Act No. 17 of 2000, Nevis Offshore Banking (Amendment) Ordinance No. 3 of 2000, the Anti-Money Laundering Regulations No. 15 of 2001, the Companies (Amendment) Act No. 14 of 2001, the Anti-Money Laundering (Amendment) Regulations No. 36 of 2001, the Nevis Business Corporation (Amendment) Ordinance No. 3 of 2001 and the Nevis Offshore Banking (Amendment) Ordinance No. 4 of 2001. The GOSKN also issued regulations requiring financial institutions to identify their customers, to maintain a record of transactions, to report suspicious transactions to the FIU and to 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's Regulator is authorized to carry out anti-money laundering examinations. The GOSKN has separated the offshore marketing and regulatory functions. In particular, an offshore Marketing and Development Department, separate from the Financial Services Commission, was established in April 2001. Legislation requires certain identifying information to be maintained about bearer certificates, including the name and address of the bearer of the certificate, as well as its beneficial owner. In addition to these measures, Nevis issued regulations aimed at facilitating the identification of beneficial owners of corporations and corporate shareholders.

Financial Services (Exchange of Information) Regulations were promulgated in 2002. These regulations define the parameters for the exchange of information between domestic regulatory agencies and foreign regulatory agencies. Financial services officials in St. Kitts and Nevis have been seeking to educate relevant stakeholders as to their responsibilities related to anti-money laundering, e.g., using radio, television, newspapers and seminars. The GOSKN encouraged the founding of an association of compliance officers within relevant financial institutions and provided training in anti-money laundering to government financial services personnel.

St. Kitts and Nevis is a member of the Caribbean Financial Action Task Force and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. A mutual legal assistance treaty between St. Kitts and Nevis and the United States entered into force in early 2000. St. Kitts and Nevis is a party to the 1988 UN Drug Convention and in November 2001 signed, but has not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. The GOSKN became a party to the UN International Convention for the Suppression of the Financing of Terrorism on November 16, 2001.

Notwithstanding its recent progress, St. Kitts and Nevis remains vulnerable to money laundering and other financial. St. Kitts and Nevis should continue to devote sufficient resources to effectively implement its anti-money laundering regime.

St. Lucia. St. Lucia is not a major financial center; however, it has developed an offshore financial service center that could potentially make the island more vulnerable to money laundering and other financial crimes. Currently, St. Lucia has one offshore bank, 733 international business companies (IBCs), ten international trusts, ten international insurance companies, seventeen Registered Agents and Trustee (Service Providers), two money remitters, one Mutual Fund Administrator and five domestic banks. Four other parties have applied for offshore bank licenses; two are pending and the other two have been refused.

The Government of St. Lucia (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 Special Branch, the Comptroller of Inland Revenue and others.

The Financial Intelligence Authority Act No. 17 of 2002 authorized the establishment of a Financial Intelligence Unit for St. Lucia, which the GOSL expects will become operational early in 2003. The FIU will receive suspicious activity reports and will be able to compel the production of information necessary

to investigate possible offenses under the 1993 Proceeds of Crime Act and the 1999 Money Laundering (Prevention) Act. 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 Caribbean Anti-Money Laundering Program (CALP), which is funded jointly by the United States, the United Kingdom and the European Union, has trained St. Lucia's FIU personnel and the necessary computer equipment is being provided by the Department of State.

The 1993 Proceeds of Crime Act criminalized money laundering with respect to narcotics. (The GOSL also is drafting legislation to enact a new Criminal Code and Evidence Act.) The Proceeds of Crime Act also provided for a voluntary system of reporting account information to the police or prosecutor when such information may be relevant to an investigation or prosecution. In addition, the Act required financial institutions to retain information on new accounts and details of transactions for seven years.

Many of the 1993 Proceeds of Crime Act provisions were superseded by the 1999 Money Laundering (Prevention) Act, which criminalized the laundering of proceeds with respect to 15 prescribed offenses, including narcotics-trafficking, corruption, fraud, terrorism, gambling and robbery. The Money Laundering (Prevention) Act mandates suspicious transaction reporting requirements and imposes record keeping requirements. In addition, the Money Laundering (Prevention) Act 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. The Act also now 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."

Pursuant to the Act, the Money Laundering (Prevention) Authority was established in early 2000. The Authority consists of five persons "who have sound knowledge of the law, banking or finance." The Authority's functions include receipt of suspicious transactions reports, subsequent investigation of the transactions, dissemination of information within (e.g., to the Director of Public Prosecutions) or outside of St. Lucia, and monitoring of compliance with the law. The Money Laundering (Prevention) Act imposes a duty on the Authority to cooperate with competent foreign authorities. Assistance includes the provision of documents, giving of testimony, undertaking of examinations, execution of search and seizure, and the provision of information and evidentiary items. The Authority has a number of regulatory powers, including the right to enter the premises of a financial institution during normal working hours to inspect transaction records or copy relevant documentation, issue guidelines to financial institutions, and to instruct a financial institution to facilitate an investigation by the Authority.

In 1999, the GOSL also 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 the Registered Agent submitting to the registrar the memorandum and articles of the company, payment of the prescribed fee and the Registrar's determination of compliance with the requirements of the Act. IBCs can be registered online through the GOSL's Pinnacle web page IBCs intending to engage in banking, insurance or mutual funds 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 has neither signed nor ratified the UN International Convention for the Suppression of the Financing of Terrorism. No evidence of terrorist financing has known to have been developed in St. Lucia. The GOSL has not taken any specific initiatives focused on the misuse of charitable and nonprofit entities.

Money Laundering and Financial Crimes

As a member of the Caribbean Financial Action Task Force (CFATF), St. Lucia underwent a first mutual evaluation immediately prior the establishment of St. Lucia's offshore sector. St. Lucia will undergo its Second Round evaluation in March 2003. St. Lucia is a party to the 1988 UN Drug Convention and a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. In February 2000 St. Lucia and the United States brought into force a Mutual Legal Assistance Treaty. On September 26, 2001, St. Lucia signed the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

The GOSL should continue to enhance and implement money laundering legislation and increase supervision of the offshore sector. The GOSL also should take the steps necessary to bring St. Lucia into full compliance with the FATF 8 Special Recommendations. The GOSL should fully establish a Financial Intelligence Unit to allow information exchange with foreign authorities.

St. Vincent and the Grenadines. Until its government fully implements the financial sector and anti-money laundering laws it has recently enacted, St. Vincent and the Grenadines (SVG) will remain vulnerable to money laundering and other financial, as a result of the rapid expansion and inadequate regulation of its offshore sector in recent years.

SVG's offshore sector includes 15 offshore banks (down from 33), 9,734 IBCs (down from over 11,000), two offshore insurance companies, six mutual funds, 400 international trusts, and Internet gaming licenses. SVG's domestic sector comprises five commercial banks, one development bank, two savings and loan banks, one building society, 21 insurance companies, nine credit unions and two money remitters. As with most Eastern Caribbean countries, the Eastern Caribbean Central Bank (ECCB) supervises SVG's five domestic banks. Beginning in October 2001 with an administrative agreement and finalized in the International Banks (Amendment) Act No. 30 of 2002, the Government of SVG (GOSVG) has given the ECCB increasing authority to review and make recommendations regarding approval of offshore bank license applications and to directly supervise SVG's offshore banks in cooperation with the GOSVG's Offshore Finance Authority (OFA). The agreement includes provisions for joint on-site inspections to evaluate the financial soundness and anti-money laundering programs of offshore banks. The OFA alone continues to supervise and regulate the other offshore sector entities. The GOSVG has strengthened the structure and staffing of the OFA by appointing five new members to the OFA board, including a new chairman and individuals bringing it to a total of 12 staff to regulate offshore insurance and mutual funds. However, this staff exercises only rudimentary controls over these institutions.

In June 2000, the Financial Action Task Force (FATF) placed SVG on the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering. The FATF in its report cited several concerns, including the fact that SVG had not put into place anti-money laundering regulations or guidelines with respect to offshore financial institutions, including customer identification, record keeping or suspicious transaction reporting requirements. FATF also cited obstacles to international cooperation and rudimentary licensing and registration requirements for financial institutions in SVG. In July 2000, the U.S. Treasury Department issued an advisory to U.S. financial institutions, warning them to give enhanced scrutiny to all financial transactions originating in or routed to or through SVG, or involving entities organized or domiciled, or persons maintaining accounts in, SVG.

Since July 2000, the GOSVG has acted on a number of fronts to address the concerns of the international community. It has passed substantial legislation, primarily the International Banks (Amendment) Act No. 7 of 2000 that deals with the authorization and regulation requirements for offshore banks as well as with the rules regarding the transfer of shares and beneficial interest. SVG also enacted the International Banks (Amendment) Act of October 2000, which enables the Offshore Finance Inspector to have access to the name or title of an account of a customer and any other confidential information about the customer that is in the possession of a licensee. SVG has enacted the International Business Companies Amendment Act No. 26 of 2002, which became effective on May 27, 2002, immobilizes and registers bearer shares. It has also revoked the Confidentiality Act and passed the Exchange of Information Act No. 29 of 2002 to

authorize and facilitate the exchange of information, particularly among regulatory bodies. It has revoked 16 bank licenses as well as caused the licenses of two others to be surrendered. In April 2001, the GOSVG revoked its economic citizenship program, which provided the legal basis to sell SVG citizenship and passports, although no passports are reported to have been issued.

SVG enacted the Proceeds of Crime and Money Laundering (Prevention) in December 2001 and the Proceeds of Crime (Money Laundering) Regulations in January 2002. Subsequent amendments further strengthened provisions of the Act and the Regulations. Among other measures, this Act criminalizes money laundering and imposes on financial institutions and regulated businesses a requirement to report suspicious transactions suspected of being related to money laundering or the proceeds of crime. The related regulations establish mandatory record keeping rules and limited customer identification/verification requirements. Subsequent to the passage of the Financial Intelligence Unit Act No. 38 of 2001, the GOSVG has established a Financial Intelligence Unit (FIU) that began operation in the summer of 2002. The FIU Act, 2001 allows for the exchange of information with foreign FIUs. An amendment to the FIU Act permits the sharing of information even at the investigative or intelligence stage. The FIU has received approximately eight suspicious activity reports (SARs) during 2002. The FIU has conducted investigations and has forwarded a case to the Director of Public Prosecutions with the recommendation to file a money laundering charge. The case is still pending. The FIU has received initial and ongoing training from the Caribbean Anti-Money Laundering Program, a program jointly funded by the United States, the United Kingdom and the European Union, and Department of State-funded computer and other equipment as well as mentoring in management and asset tracing and forfeiture.

The FATF stated in its October 2002 report that the SVG had enacted most, if not all, legislation needed to remedy deficiencies; however, until the deficiencies are fully addressed and the necessary reforms implemented, the SVG will remain listed. FATF invited the SVG to submit implementation plans that will enable the FATF to evaluate actual realization of the legislative changes in the SVG anti-money laundering regime. The SVG submitted an implementation plan in August 2002. The GOSVG's current progress in implementing anti-money laundering measures will be reviewed at the February 2003 FATF plenary.

Subsequently, St. Vincent and the Grenadines enacted the United Nations Terrorism Measures Act #34, effective August 2, 2002. Sections 3 and 4 of the Act criminalize terrorist financing. The GOSVG is a party to the UN International Convention for the Suppression of the Financing of Terrorism and is deemed to be partially compliant. No evidence has yet been known to be developed of terrorist financing in SVG. Also, the GOSVG has not undertaken any specific initiatives focused on the misuse of charitable and non-profit entities.

The GOSVG is a member of the Caribbean Financial Action Task Force (CFATF), and underwent its Second Round mutual evaluation in November 2002. In addition, SVG is a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering. SVG is a party to the 1988 UN Drug Convention and acceded to the Inter-American Convention Against Corruption in 2001. An updated extradition treaty and a Mutual Legal Assistance Treaty between the United States and SVG entered into force in September 1999.

The GOSVG should address concerns raised by the international community concerning the remaining deficiencies in the GOSVG's anti-money laundering regime. The FIU should strengthen its relationship with its foreign counterparts and join the Egmont Group. The GOSVG also should ensure that it properly supervises the offshore sector and adequately trains regulatory and law enforcement personnel on money laundering operations and investigations.

Suriname. Suriname is not a regional financial center. Money laundering takes place as a result of transnational criminal activity related to the transshipment of Colombian cocaine and European-produced ecstasy through Suriname en route to markets in Europe and the United States. Narcotics-related money laundering is believed to occur primarily through the non-banking financial system and a variety of other means, including the sale of gold purchased with illicitly obtained money and the manipulation of

Money Laundering and Financial Crimes

commercial and state-controlled bank accounts. Suriname's casinos and cambios are also presumed to be used to facilitate money laundering.

Suriname's overall anti-money laundering regime is considered weak, although in September 2002 the Government of Suriname (GOS) brought into force a package of anti-money laundering legislation based on the recommendations of the Caribbean Financial Action Task Force (CFATF). The new legislation defines money laundering and establishes penalties for money laundering activities, requires the reporting of unusual and suspicious financial transactions, establishes a Financial Intelligence Unit (FIU) to track and report on unusual and suspicious financial transactions, and requires financial service providers to confirm the identities of clients, individual or corporate, and to store information on clients for seven years. The FIU, to be administered by the Attorney General's office, is designed to assist in the enforcement of the requirements of the banks and other financial institutions to identify, record and report the identity of customers engaging in significant transactions. The legislation includes a due diligence section making individual bankers responsible if their institution is laundering money and ensures the protection of bankers and others with respect to their cooperation with law enforcement officials. The GOS is receiving technical assistance in establishing the FIU from the EU/US/UK-funded Caribbean Anti-Money Laundering Program. The U.S. is providing equipment and furniture for the FIU.

The new legislation also amends the criminal code to provide for the confiscation of illegally obtained proceeds and other assets obtained partly or completely through criminal offenses, to allow criminal offenses to be filed and penalties to be levied against corporate entities, and to punish persons who participate in an organization that intends to commit crime. The Government of Suriname (GOS) has not criminalized terrorist financing, although current legislation allows assets to be seized under criminal investigative authority. No terrorist-related assets have been identified in Surinamese financial institutions.

Suriname is a member of the CFATF and the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering. Suriname is a party to the 1988 UN Drug Convention.

The GOS should set as priorities the effective implementation of the new anti-money laundering legislation, including establishment of the FIU, and enactment of legislation to criminalize terrorist financing.

Swaziland. Swaziland is a growing regional financial center. International narcotics-trafficking continues to grow in Swaziland, increasing the threat of money laundering. Swaziland's proximity to South Africa, lack of effective counternarcotics legislation, limited enforcement resources, relatively open society, and developed economic infrastructure make it attractive for trafficking organizations and increase the risk for money laundering.

The Money Laundering Act of 2001 criminalizes money laundering for specified predicate offenses, including narcotics-trafficking, kidnapping, counterfeiting, extortion, fraud, and arms-trafficking. The Act establishes a currency reporting requirement, requires banks to report suspicious transactions to the Central Bank, and provides conditions when assets may be frozen and forfeited. The penalty for money laundering is six years imprisonment, a fine amounting to roughly \$2,500, or both. The Act also allows for providing assistance to foreign countries that have entered into mutual assistance treaties with the Government of Swaziland.

Swaziland has an extradition treaty with South Africa, as well as a protocol and mutual understanding on narcotics with Commonwealth Countries.

Swaziland is party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN International Convention against Transnational Organized Crime, which is not yet in force internationally. Swaziland is an active member in the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. In August, 2002, Swaziland hosted the ESAAMLG plenary and Council of Ministers meeting. At the Council of Ministers meeting, Swaziland assumed the one-year presidency of ESAAMLG.

Swaziland should criminalize terrorist financing. Swaziland should also establish a Financial Intelligence Unit capable of sharing information with foreign law enforcement and regulatory officials.

Sweden. Sweden does not appear to have a significant money laundering problem. Swedish anti-money laundering legislation includes all serious crimes. Sweden's money laundering controls allow Sweden to fulfill the recommendations of the Hague Forfeiture Convention.

Swedish law requires financial institutions, insurance companies, currency exchange houses, and money transfer companies to verify customer identification, inquire into a transaction's background, and verify identities for each transaction, particularly in the case of new customers and involving amounts above SEK 110,000 (\$12,300). Swedish law allows for the sanctioning of non-compliant institutions rather than the individual officers of those institutions. Any suspicious transactions are required to be reported to the police Financial Intelligence Unit (FIU). The FIU is entitled to demand customer information from dealers in antiques, jewelry and art; companies buying and selling new and used vehicles; and firms dealing with gambling and the sale of lottery tickets. Swedish law also provides for the seizure of assets derived from drug-related activity.

Although Sweden did not adopt the euro as its country's legal currency, it recognized the potential for money laundering prior to and during the changeover period. Guidelines were issued to the financial sector regarding the scrutinizing of large-scale financial transactions, and the FIU conducted a study on potential problems associated with the changeover.

In 2002, the FIU received approximately 8,000 suspicious transaction reports, almost double the number reported in 2001.

Sweden ratified the UN International Convention for the Suppression of the Financing of Terrorism on June 6, 2002. In July 2002, Sweden adopted a new law on the freezing of assets to combat the financing of terrorism, with the additional purpose of fully implementing UNSCR 1373. Prior to this law, assets could not be frozen. The law also makes it illegal to collect, supply or receive money or other kinds of assets for the purpose of financing terrorist crimes or activities.

Sweden has endorsed the September 1997 Basel Committee's "Core Principles for Effective Banking Supervision." Sweden is a member of the Financial Action Task Force and the Council of Europe. Its FIU is a member of the Egmont Group. Sweden is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. It is also a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

Switzerland. Switzerland's central geographic location; relative political, social, and monetary stability; wide range of available financial services; and long tradition of bank secrecy are all factors that make Switzerland a major international financial center. These same factors make Switzerland attractive to potential money launderers. However, Swiss authorities are aware of this and waive bank secrecy rules in the prosecution of money laundering and other criminal cases.

Reporting indicates that criminals attempt to launder proceeds in Switzerland from a wide range of illegal activities conducted worldwide, particularly narcotics-trafficking and corruption. Switzerland's extensive market in fine arts is also used to launder money. 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. For example, some of the money generated by Albanian narcotics-trafficking rings in Switzerland goes to armed Albanian extremists in the Balkans.

Money laundering is a criminal offense. Switzerland has significant anti-money laundering legislation in place making banks and other financial intermediaries subject to strict Know-Your-Customer and reporting requirements. Switzerland has also implemented legislation for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets.

Money Laundering and Financial Crimes

The current money laundering laws and regulations have been extended to non-bank financial institutions. Consequently, all non-bank financial intermediaries are required to either join an accredited self-regulatory organization (SRO), or come under the direct supervision of the Money Laundering Control Authority (MLCA) of the Federal Finance Administration. The MLCA was formed in 1998 to oversee anti-money laundering laws in the non-banking sector. The SROs must be independent of the management of the intermediaries they supervise and must enforce compliance with due diligence obligations. Non-compliance can result in a fine or a revoked license. About 7,000 fiduciaries operate in this previously unregulated arena. During the summer of 2002, the MLCA shut down three financial management companies, because they were operating illegally and failed to comply with anti-money laundering regulations. This action marked the first time the MLCA took direct action against financial intermediaries in Switzerland.

Additional legislation effective January 1, 2002 is intended to make the prosecution of organized crime, money laundering, corruption and other white-collar crime more effective 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 and white collar crime. During the summer of 2002, the Swiss Federal Council presented a bill to the Nationalrat, Switzerland's National Council, that addressed a number of terrorism issues surrounding ratification of the UN terrorism conventions. This bill also includes legislation for implementation, including a self-standing provision on terrorist financing that introduces criminal liability for legal persons for terrorism financing. The Staenderat was expected to make a decision on this bill in December 2002, and the Swiss House is scheduled consider it in the first half of 2003.

The Money Laundering Reporting Office Switzerland (MROS) is Switzerland's Financial Intelligence Unit (FIU). All financial intermediaries (banks, insurers, fund managers, currency exchange houses, securities brokers, etc.) are legally obliged to establish customer identity when forming a business relationship. They also must notify the MROS, or a government authorized supervisory body, if a transaction appears suspicious. If financial institutions determine that assets were derived from criminal activity, the assets must be reported to MROS and frozen within 5 days until a prosecutor decides whether to take further action. MROS' staff, particularly the non-banking sector staff, increased in 2002, so the FIU now has twice the staff it had at its establishment in 1998.

Switzerland's banking industry offers the same account services for both residents and non-residents. These can be opened through various intermediaries who advertise their services. As part of Switzerland's international financial services, banks offer certain well-regulated offshore services, including permitting non-residents to form offshore companies to conduct business, which can be used for tax reduction purposes.

The Swiss Commercial Law does not recognize any offshore mechanism per se and its provisions apply equally to residents and non-residents. 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.

The Government of Switzerland has made it a key foreign policy goal to correct the country's image as a haven for illicit banking services. In November 2001, the Swiss Federal Banking Commission ordered the dismissal of the Swiss manager of Zurich's Bank Leumi le-Israel because of professional malfeasance in accepting funds from a customer with questionable ties and fund sources. The Commission will also implement a new regulation, starting July 2003, that will significantly increase the banks' diligence rules for "high risk" clients whose political exposure make them vulnerable to corruption. The new regulations call for a systematic recording of new and existing business relationships, the performance of comprehensive, in-depth investigations into "risky" relationships, and electronic monitoring of high-risk transactions.

The Oversight Commission of the Swiss Bankers Association fined Credit Suisse for inadequate due diligence in connection with a total of \$214 million deposited in the bank by former Nigerian dictator Sani Abacha. Swiss press reports put the fine at \$500,000 (SFr. 750,000), making it the largest fine ever imposed by the Commission. The recipient of the fine will be the International Red Cross Committee.

Despite the measures that Switzerland has taken, it continues to come under fire by its neighbors and EU member countries for its continued banking secrecy laws and its refusal to look upon tax evasion as a crime. The EU finance ministers issued a warning to Switzerland in 2002, saying that Switzerland's lack of action is hampering the global crackdown on money laundering and other financial crimes, and threatened sanctions if Switzerland does not change its banking secrecy laws. However, current Swiss law provides for no banking secrecy for suspected fraud, money laundering, or terrorist-related funds, despite Switzerland's steadfast position on maintaining banking secrecy in the face of tax evasion not related to other crimes.

Switzerland ranks among the world's leading art markets. Generating about \$200 billion a year in turnover, the market offers lucrative opportunities for organized crime to transfer stolen art or use art to launder criminal funds. The Swiss art market is especially attractive for unethical transactions since artworks, which may have been smuggled into Switzerland, can legally be re-exported as genuine Swiss artwork after five years. Swiss officials are concerned about the possible abuse of its art dealer market and a new bill against illegal cultural transfers is slated for parliamentary debate next year. The United States is Switzerland's most important art trading partner, importing \$300 million worth of art from Switzerland in 2001.

The soon-to-be amended Swiss penal code makes terrorism financing a predicate offense for money laundering. It has yet to pass the Nationalrat, but it is expected to pass in the spring of 2003, and will be effective immediately upon passage. 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. The banking community cooperates with enforcement efforts. In addition, legislation permits "spontaneous transmittal"—allowing the Swiss investigating magistrate to signal to foreign law enforcement authorities the existence of evidence in Switzerland. For example, the Swiss used this provision in 2001 to signal Peru that it had uncovered accounts linked to former Peruvian presidential advisor Vladimiro Montesinos.

Since September 11, 2001, Swiss authorities have been alerting Swiss banks and non-bank 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 assets of organizations and individuals designated by UN 1267 Sanctions Committee. In 2001, the MROS was notified a record 417 times of suspicious transactions, according to its annual report published in May 2002. This marks a 34 percent increase over the previous year's 311 notifications. The MROS blocked a record \$1.8 billion (SFr. 2.73 billion) during 2001, compared to \$436 million (SFr. 656 million) during 2000. Five international cases account for more than \$1.3 billion (SFr. 2 billion) in assets blocked during 2001. Much of the increase in the number of reported cases was due to the extensive search of terrorist assets following September 11. At least 95 notifications concerning funds totaling \$24.6 million (SFr. 37 million) were linked to the terrorist attacks. In 35 cases, the beneficial owner of the blocked assets was a Saudi-Arabian national, in 33 cases Swiss, and in 5 cases Italian. Others came from Liechtenstein, Afghanistan, France, Egypt, United States, United Kingdom, Bahamas, Syria, Turkey, Bosnia-Herzegovina, Bangladesh, Somalia, United Arab Emirates, Bahrain, and Pakistan. In the year following September 11, 2001, Switzerland froze 72 bank accounts worth \$20 million with suspected links to terrorism. Over 400 money laundering cases, totaling over 2.7 billion Swiss francs, reported during the same time frame.

Switzerland is a signatory of, but has not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Switzerland has ratified the Council of Europe Convention on the Laundering, Search, Seizure, and Confiscation of Proceeds from Crime. Switzerland is expected to soon have ratified all of the UN terrorism conventions. The Federal Council presented, with its bill to Parliament in the summer of 2002, language concerning ratification of the UN International Convention for the Suppression of the Financing of Terrorism and the UN International Convention for the Suppression of Terrorist Bombings. Of the twelve UN Conventions, ten have been ratified, and the Nationalrat is expected to ratify the other two in the spring session. To date, Switzerland has not ratified the 1988 UN Drug Convention.

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 supervisory purposes. Switzerland is a member of the Financial Action Task Force and the Egmont Group. Switzerland is a member of the Basel Committee on Banking Supervision, which established the first international code of conduct for banks. 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.

Switzerland should extend its anti-money laundering program to include dealers in art and high-end goods. Switzerland should continue to work toward full implementation of its anti-money laundering regime.

Syria. Syria is designated by the U.S. Department of State as a State Sponsor of Terrorism. As host to one of the most underdeveloped banking sectors in the world, Syria is not a likely center for money laundering via the formal financial sector. Since private banks were nationalized in the early 1960s, Syria's entire financial system has been owned and operated by the state. The existing public banks are inefficient and highly-regulated, and focus almost exclusively on financing public enterprises. As a result, Syrian businessmen traditionally use banks in neighboring Lebanon and Jordan to receive a full range of banking services. The private sector routinely conducts foreign currency transactions to finance imports, generally by using letters of credit from Lebanon and Europe. Due to foreign exchange controls, the private sector also has restricted access to foreign currency. Illicit proceeds from the narcotics trade may flow through Syria, but it is generally believed they are moved to Lebanon for laundering purposes. As a result, the primary money laundering vulnerability in Syria is not necessarily through financial institutions but via the use of alternative remittance systems such as hawala, trade-based money laundering, gold, and currency smuggling. These money laundering methodologies are known to be used to finance terrorism throughout the region and elsewhere.

The government-controlled banking system in Syria consists of the Central Bank of Syria and five public banks, each specializing in one aspect of economic activity: the Commercial Bank of Syria, the Agricultural Cooperative Bank, the Industrial Bank, the Real Estate Bank, and the People's Credit Bank. These banks employ a rigid interest rate structure that discourages savings deposits, particularly during periods of inflation. Only the Commercial Bank of Syria is permitted to provide commercial banking services. The Commercial Bank, as the sole legal trader of foreign currencies, also effectively controls all foreign trade and all foreign currency transactions. In addition to monopolizing the exchange of foreign currencies, the Syrian government maintains one of the last remaining fixed, multiple exchange rate systems in the world, employing three different rates depending on the nature of the transaction. This inefficient system undoubtedly contributes to alternative methods of transferring value outside the state controlled banking system. There are reports that such transactions occur with the tacit approval, if not involvement, of Syrian government officials. A large percentage of Lebanon's banking services involve Syrian accounts.

In April 2001, Syria enacted new laws on both legalizing private banking (Law No. 28) and establishing rules on banking secrecy (Law 29). However, no private bank has yet been granted permission to open. Much still needs to be done to fundamentally restructure the banking sector, particularly in terms of either suspending or amending existing regulations that would prohibit a newly-licensed private bank from

operating fully. The Syrian government continues to work on detailed regulations that will govern the operation of private banks.

Reportedly, the Syrian government is aware that with the liberalization of its banking sector, measures to prevent such activity must be firmly in place. Therefore, it is preparing draft money laundering legislation that may be passed sometime in 2003. The details of this draft legislation are as yet unclear.

Syria is a party to the 1988 UN Drug Convention. Syria has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

As a first step in crafting an effective anti-money laundering program, Syria should approve comprehensive anti-money laundering and anti-terrorism finance legislation that adheres to world standards. Syria should also be aware that money laundering can easily by-pass financial institutions and take enforcement measures to address these vulnerabilities.

Taiwan. Taiwan's modern financial sector and its role as a hub for international trade make it attractive to money laundering. Its location astride international shipping lanes makes it vulnerable to transnational crimes such as narcotics-trafficking and smuggling. The use of alternative remittance systems or "underground banking" is a money laundering vulnerability. There is a significant volume of informal financial activity through unregulated non-bank channels. According to suspicious activity reports (SARs) filed by financial institutions on Taiwan, the predicate crimes linked to SARs include: financial crimes, corruption, narcotics, and other general crimes, in that order.

Taiwan's anti-money laundering legislation is embodied in the Money Laundering Control Act (MLCA) of April 23, 1997. 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 October 2002, the Executive Yuan approved draft legislation to amend the MLCA and forwarded it to the Legislative Yuan for approval. Among the amendments are provisions for the freezing of assets related to money laundering and terrorism, and for the creation of a system for sharing forfeited assets with domestic and foreign enforcement agencies. The legislation also expands the list of financial institutions to include pawnshops, travel agents, car dealers, and real estate brokers. Other amendments call for stiffer penalties for major or recidivist money launderers, the lifting of immunity from prosecution of conspiring family members or cohabitants, and the introduction of a currency transaction reporting (CTR) requirement for cash transactions. Financial institutions currently have an electronic system in place to identify and record transactions that exceed NT \$1 million (\$30,000); the amendments require financial institutions to report CTRs to an as yet unidentified agency (likely the MLPC). The CTR threshold amount has not yet been determined but will be in the range of NT \$1-1½ million (\$30,000-45,000).

According to statistics published by the MLPC, of the 791 SARs filed in 2001, 28 percent were referred to law enforcement authorities for investigation, 22 percent were under review, and 50 percent were archived with no further action. According to the MLPC, authorities on Taiwan prosecuted 179 individuals in 38 cases for money laundering during 1997-2001. In addition, in 2001 the MLPC provided information to assist 46 domestic and 20 international investigations.

The authorities on Taiwan are actively involved in countering the financing of terrorism. 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. Terrorist financing is not explicitly criminalized, but in accordance with UN Security Council Resolution 1373, the MLCA was amended to allow the freezing of accounts suspected of being linked to terrorism. Under current law the ability of authorities on Taiwan to identify, freeze and seize terrorist-related financial assets is limited, although legislative amendments are pending. At present, authorities on Taiwan must post a bond before freezing or seizing financial assets. No targeted assets have been identified to date.

Money Laundering and Financial Crimes

Alternative remittance systems, or underground banks, are considered to be operating in violation of Banking Law Article 29. Authorities on Taiwan consider these entities unregulated financial institutions, although pending legislation would bring them under the regulatory umbrella. Authorities on Taiwan do not believe that charitable and non-profit organizations in Taiwan are being used as conduits for the financing of terrorism. Taiwan is, however, investigating a number of foreign-owned and operated commercial enterprises that handle remittances by guest workers to their home countries.

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 territories 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 on Taiwan have passed and implemented laws in compliance with the goals and objectives of the Convention. Taiwan is a founding member of the Asia/Pacific Group on Money Laundering (APG) and actively participates in the Group's meetings. The MLPC is a member of the Egmont Group.

Over the past five years Taiwan has created and implemented an anti-money laundering regime within international standards. The APG's May 2001 Mutual Evaluation Report on Taiwan recommended a number of improvements to its anti-money laundering program. The MLCA amendments, introduced in 2002, address a number of these recommendations, especially in the area of asset forfeiture. The authorities on Taiwan should adopt these proposed amendments to continue to strengthen the existing anti-money laundering regime. The authorities on Taiwan should also criminalize the support and financing of terrorism. The authorities on Taiwan should also enact legislation that would result in the issuance of regulations regarding alternate remittance systems.

Tajikistan. Tajikistan is not a financial center, and its underdeveloped banking sector does not make it attractive for money laundering. However, with average monthly income in the country near ten U.S. dollars, the temptation to become involved in narcotics-related transactions remains high for many segments of the society. Further, as the Government of Tajikistan (GOT) continues to pursue financial sector reform, measures to counter money laundering will grow in importance. There are indications that some small-scale money laundering takes place in the country, mostly through the purchase and subsequent import of goods and properties. Trade based money laundering is commonly used in the region.

Tajikistan has criminalized money laundering; the Criminal Code specifies fines ranging from approximately \$700 to \$4,000 (the fines are based on the national minimum wage, currently four Somoni per month or about \$1.30) and a maximum prison term of ten years for the use or masking of funds derived from illegal activities. Tajik law also provides for the seizure of assets used in or derived from narcotics-related activity.

Tajik authorities have been cooperative with U.S. efforts to trace and halt terrorist-related funds, and Tajikistan has signed, but has not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

Tajikistan is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Tajikistan has not yet enacted terrorist financing legislation.

Tanzania. Tanzania is a regional trade center. Police and government officials confirm that Tanzania is vulnerable to money laundering due to poor anti-money laundering controls. Similarly, a weak financial sector and an under-trained, under-funded law enforcement apparatus make such crimes difficult to track and prosecute. Officials have noted that some real estate and used car businesses are used for money laundering purposes. Government officials have also cited drug trafficking and the emerging casino industry as areas of concern for money laundering. The prevalence of money laundering and hawala, and

the threat of terrorist organizations, on the unregulated island of Zanzibar make it an area of concern. Officials indicate that money laundering schemes in Zanzibar generally take the form of foreign investment in the tourist industry and bulk cash smuggling.

The Proceeds of Crime Act of 1991 criminalizes narcotics-related money laundering. However, the Act does not adequately define money laundering, and it has only been used to prosecute corruption cases. The law obliges financial institutions to maintain records of transactions exceeding 10,000 shillings (approximately \$10) for a period of 10 years. If the 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 not required. Financial institution employees are legally protected from liability stemming from reporting suspicious transactions.

In November 2002, Parliament approved the Prevention of Terrorism Act, which the President signed into law on December 14. The Act criminalizes terrorist financing. It also requires all financial institutions to inform the government each quarter of whether any of their assets or any transactions may be associated with a terrorist group, although the implementing regulations for this provision have not yet been drafted. Under the Act, the government may seize assets associated with terrorist groups.

On November 11, 2002, the Parliament ratified the UN International Convention for the Suppression of the Financing of Terrorism, although the Government of Tanzania (GOT) has not yet deposited its instruments of ratification with the UN. Tanzania is a party to the 1988 UN Drug Convention. Tanzania is a member of the East and Southern Africa Anti-Money Laundering Group (ESAAMLG), which was founded in 1999. The GOT continues to play a leading role in the operation of this FATF-style regional body and has detailed personnel to the ESAAMLG Secretariat, located in donated office space in Dar es Salaam. In March 2002, Tanzania hosted the biannual ESAAMLG plenary, and will host it again in March 2003. Tanzania has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Consonant with its commitment to supporting the ESAAMLG, Tanzania should enact comprehensive money laundering legislation that would apply to all serious crimes and include mandatory customer identification. The legislation should also require reporting of suspicious transaction reports to a Financial Intelligence Unit (FIU), which would be empowered to share information with other FIUs and foreign law enforcement agencies.

Thailand. Thailand's location makes it a major risk for money laundering, as it is a transit country for Southeast Asian narcotics. Northern Thailand forms part of the Golden Triangle with Burma and Laos. Although Thailand has taken significant steps toward reducing the production of illicit narcotics, it still serves as a major narcotics-trafficking route for the Golden Triangle, because of its good transportation infrastructure and international connections. Smuggling of narcotics and contraband and evasion of customs duty are significant problems. Thailand is also a major production, transit and distribution country for counterfeit goods. Drug traffickers use Thailand's banking system to hide and move their proceeds. The underground banking system is also widely in use as a money laundering method. Money is transported in bulk from the United States to other Asian countries, and ultimately moved to Thailand. Gambling dens and underground lotteries account for a significant portion of Thailand's underground economy, and remain attractive mechanisms for money laundering. Thailand financial institutions and gem industry are also vulnerable to misuse by terrorist organizations and their supporters. Corruption remains a major problem and several high profile investigations were launched in 2002 concerning the laundering of the proceeds of corruption by public officials.

Thailand's anti-money laundering legislation, the Anti-Money Laundering Act (AMLA) B.E. 2542 (1999) criminalizes money laundering for the following seven predicate offenses: narcotics-trafficking, trafficking in women or children for sexual purposes, fraud, financial institution fraud, , public corruption, customs evasion, extortion, and blackmail. The AMLA requires customer identification, record keeping, and the reporting of large and suspicious transactions, and provides, as well, for the civil forfeiture of property involved in a money laundering offense. Financial institutions are also required to keep customer

Money Laundering and Financial Crimes

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. Thailand does not have secrecy laws that prevent disclosure of client and ownership information of bank accounts to supervisors and law enforcement authorities. The AMLA gives the anti-money laundering office the authority to compel a financial institution to disclose such information.

The AMLA created the, Anti-Money Laundering Office (AMLO) which became fully operational in 2001. AMLO is Thailand's financial intelligence unit. AMLO receives, analyzes, and processes suspicious and large transaction reports as required by the AMLA. Between 1,000 and 1,200 suspicious transactions are reported each month on a regular basis. In addition, AMLO has the responsibility for investigating money laundering for civil forfeiture purposes and has additional responsibility for the custody, management, and disposal of seized and forfeited property. The AMLO is also tasked with providing training to the public and private sectors concerning the provisions of the AMLA. The law also creates 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 Money Laundering Control 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 propose the relevant ministerial regulations.

The anti-money laundering controls apply to financial institutions and the Bureau of Land. The Stock Exchange of Thailand (SET) requires securities dealers to have know-your-customer procedures, however, the SET does not do any anti-money laundering compliance checks during its reviews. There are no anti-money laundering regulations for the insurance industry. Currency exchange dealers are required to be licensed, however, there are no anti-money laundering regulations for exchange businesses.

The Bank of Thailand (BOT) regulates financial institutions in Thailand, however, 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 a financial institution's compliance with the AMLA or BOT regulations. Besides this lack of power to conduct transactional testing, BOT does not examine its financial institutions for anti-money laundering compliance. BOT and AMLO have agreed to jointly undertake this effort which should commence in 2003.

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 2 million baht (approximately \$50,000) and property transactions exceeding 5 million baht (approximately \$125,000) have been in place since October 2000. However, in December 2002, a proposal was made to lower the threshold for reporting cash transactions to 500,000 baht (\$12,000). The proposal is not yet effective. The various land offices are also required to report on any transaction involving property of 5 million Thai baht, or greater, or a cash payment of 2 million Thai baht, or greater, for the purchase of real property.

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. Thailand's 44 BIBFs are now subject to AMLA.

The Royal Thai Government (RTG) recently proposed legislation to establish a new agency, the Special Investigation Department (SID). If the law is passed, it is likely SID will have responsibility for investigating most major financial crimes, including money laundering.

Thailand has not yet criminalized the financing of terrorism. Legislation to make terrorism a serious criminal offense, criminalize terrorist financing, and make it a predicate offense under AMLA is pending approval by the Thai parliament. The RTG issued instructions to all authorities to comply with UN Security Council Resolutions 1267, 1269, 1333, 1373, and 1390, including the freezing of funds or financial resources belonging to the Taliban and the al-Qaida network. To date, Thailand has not identified, frozen and/or seized assets linked to individuals and entities included on the UN 1267 Sanctions Committee consolidated list. The only action taken regarding alternative remittance systems is the general provisions of the AMLA, that make it a crime to transfer, or receive a transfer, that represents the proceeds of a predicate criminal offense.

The U.S.-Thai Mutual Legal Assistance Treaty entered into force in 1993. Thailand also has mutual legal assistance agreements with the United Kingdom, Canada, China PRC, France, and Norway. Numerous bilateral agreements are pending, as well as memoranda of understanding between the Anti-Money Laundering Office and financial intelligence units in other nations. AMLO expects to sign a number of agreements in March 2003 when Thailand hosts the 2nd Pacific Rim Conference on Money Laundering and Financial Crimes. Thailand is a member of the Asia/Pacific Group on Money Laundering (APG). In December 2000, Thailand signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally and is studying its domestic laws to determine what implementing legislation is required. In June 2001, Thailand became a member of the Egmont Group of financial intelligence units. Thailand is a party to the 1988 UN Vienna Convention. The RTG has signed, but not ratified, the UN International Convention for the Suppression of the Financing of Terrorism.

The Royal Thai Government should continue to implement its anti-money laundering program but until the RTG provides a viable mechanism for 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 require the SET to include anti-money laundering compliance checks during its reviews. The RTG should develop and implement anti-money laundering regulations for exchange businesses and should take additional measures to address alternative remittance systems to further strengthen its anti-money laundering regime against crime, particularly by expanding its predicate offenses to include a broader base of serious financial crimes, such as arms/weapons trafficking, alien smuggling, and environmental crimes, as well as making structuring a criminal offense. Thailand continues to suffer problems with asset management and disposition due in part to a lack of resources. This lack of resources could be addressed through the creation of an Asset Forfeiture Fund which could make funds available for money laundering and asset forfeiture investigations. The RTG should create such a fund. Thailand's lack of anti-terrorist financing legislation renders its financial institutions vulnerable to misuse by terrorist organizations and their supporters. The RTG should pass legislation criminalizing terrorist financing and ratify the International Convention for the Suppression of the Financing of Terrorism.

Togo. Togo's poor financial infrastructure makes it an unlikely venue for money laundering through its financial institutions. Its porous borders, however, make it a transshipment point in the regional and sub-regional trade in narcotics. Togo's 1998 drug law criminalizes narcotics-related money laundering and penalizes offenses with up to 20 years in prison. However, there have never been any arrests for money laundering. Financial institutions are required to monitor and report monetary transactions above a threshold appropriate to the local economic situation, and must maintain records of such transactions and supply them to government authorities on request. Financial institutions are legally protected in respect to their cooperation with law enforcement authorities. Due diligence legislation applies to bankers and other professionals, although no arrests have been made for violations of this law.

The Government of Togo (GOT) has the legal authority to seize assets associated with drug trafficking. In 2001, President Eyadema created the national Anti-Corruption Commission to combat corruption and money laundering.

Money Laundering and Financial Crimes

Terrorist financing is a criminal offense in Togo. The GOT has circulated to Togolese financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267/1390 consolidated sanctions list and on additional lists supplied by the U.S. Government. The GOT closely regulates charities and other non-governmental organizations.

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): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal, and Togo, all of which use the French-backed CFA franc currency. All bank deposits over approximately \$7,700 made in BCEAO member countries must be reported to the BCEAO, along with customer identification information. In September 2002, the WAEMU Council of Ministers, which oversees the BCEAO, issued a directive requesting that each member country set up a national committee under their Minister of Finance to deal with financial information as it relates to money laundering. The BCEAO would be in charge of coordinating such committees. Each member country is now responsible for putting legislation in place to implement this directive, and the legislation is expected to be harmonized regionally.

The WAEMU Council of Ministers issued another directive in September 2002 requesting member countries to pass legislation requiring banks to freeze the accounts of any persons or organizations targeted by the UNSCR 1267/1390 consolidated list.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA), based in Dakar, Senegal. In November 2002, GIABA hosted an anti-money laundering seminar for representatives of 14 ECOWAS members, including Togo. In July 2002 Togo participated in the 2002 West African Joint Operation Conference (WAJO) that promotes regional law enforcement cooperation against narcotics-trafficking, terrorism, and money laundering.

Togo is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Togo ratified the UN International Convention for the Suppression of the Financing of Terrorism on February 14, 2002.

Togo should criminalize money laundering for all serious crimes.

Trinidad and Tobago. Trinidad and Tobago has a well-developed and modern banking sector, and is an increasingly significant regional financial center. Consequently, the country suffers increasingly financial crimes, mostly in the form of counterfeiting and credit card fraud. It is likely that money laundering takes place in investment firms, credit unions, banks, insurance companies, casinos, and some retail businesses. Importers under-invoicing imported goods for possible money laundering purposes is a concern as well. In December 2001, a senior customs official was assassinated outside his home. The official was instrumental in investigating allegations of fraud, corruption and under-valuation of goods by customs employees. A police investigation is ongoing.

The Proceeds of Crime Act of 2000 (POCA) expanded money laundering predicate offenses to include all serious crimes, and instituted reporting requirements for suspicious transactions. Failure to comply with POCA's record keeping and reporting requirements can result in a fine of 250,000 TT (approximately \$40,000) and imprisonment for two years for summary conviction, and a fine of 3,000,000 TT (approximately \$500,000) and seven years imprisonment for conviction on indictment. Upon summary conviction for money laundering, an offender can be liable for a fine of 25,000,000 TT (approximately \$4,000,000) and 25 years imprisonment. Furthermore, under the POCA, any officer who aids and abets the money laundering activities of an institution can be convicted of money laundering even if the institution itself has not been prosecuted or convicted. The POCA also enables the courts to seize the proceeds of all serious crimes, although no profits or property have been seized under the Act. Under POCA and the 1987 Prevention of Corruption Act, a former Minister of Finance has been charged, along with others, with offenses ranging from corruption and money laundering to misbehavior in public office and aiding and abetting the same. The Government of Trinidad and Tobago (GOTT) has legislation in

place that allows it to trace, freeze, and seize assets, including intangible assets such as bank accounts. Authorities may seize legitimate businesses if they are used to launder drug money. The GOTT has circulated to its financial institutions the lists of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list as being linked to Usama Bin Ladin, al-Qaida, the Taliban, along with the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 (on terrorist financing) and the relevant EU lists. GOTT customs regulations require that any sum above \$5,000 (in currency or monetary instruments) entering or leaving the country be declared. Cash above \$10,000 may be seized, with judicial approval, pending determination of its legitimate source. The GOTT does not have legislation that specifically authorizes the sharing of forfeited assets with other countries, but has done so in the past on a case-by-case basis through bilateral agreements.

The GOTT has approved a UNDCP plan that involves drafting updated guidelines for anti-money laundering legislation, exchange of information, record keeping, independent regulatory structures, suspicious transaction, reporting, know your customer requirements, and international cooperation.

The Central Bank has set money laundering guidelines, including due diligence provisions that apply to all financial institutions subject to the 1993 Financial Institutions Act. These include banks, finance companies, leasing corporations, merchant banks, mortgage institutions, unit trusts, credit card businesses, and financial services businesses. Credit unions and exchange houses are not subject to the guidelines.

The GOTT has an inter-ministerial counternarcotics/crime task force that investigates narcotics-trafficking and related money laundering.

The U.S. Internal Revenue Service is providing technical assistance to the Trinidad and Tobago Bureau of Inland Revenue to assist them in developing a comprehensive criminal investigations system that would be targeted to reducing corruption and enforcing the criminal statutes concerning tax administration and related financial crimes. This is being done in order to achieve compliance with the GOTT's Income Tax Act.

The GOTT has not become a signatory to the UN International Convention for the Suppression of the Financing of Terrorism, nor is the GOTT deemed to have implemented its principles in accordance with its own FATF self-assessment. There has not yet been any identified evidence of terrorist financing in Trinidad and Tobago.

Trinidad and Tobago is a party to the 1988 UN Drug Convention. Trinidad and Tobago is also a member of the CFATF, which is headquartered in Port of Spain. It underwent a second round CFATF mutual evaluation in 2002, and the report has been endorsed by CFATF's Council of Ministers. Trinidad and Tobago is also a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. In 1999, an MLAT with the United States entered into force. In 2000, the U.S. and GOTT signed a joint statement on law enforcement cooperation, which pledges in part to expand cooperation on the detection and prosecution of money laundering and related criminal activities.

The GOTT should pass anti-terrorist financing legislation that will provide the authority to identify, freeze and seize terrorist assets. The GOTT should also continue its efforts to improve its ability to criminally investigate money laundering.

Tunisia. There is little public information about money laundering in Tunisia. Although it is an offshore financial center, it is not a regional financial center and the government keeps a close hand on the management of the economy. However, the lack of a money laundering law makes Tunisia vulnerable to money laundering. The Ministry of Finance and the Central Bank regulate 12 offshore banks. The Central Bank regularly conducts surprise audits of accounts and transactions of offshore banks. The Ministries of Commerce and Industry and Energy regulate approximately 1,200 offshore manufacturing companies. The Ministry of Commerce also regulates 300 offshore trading companies. The offshore companies may be 100 percent foreign owned. Anonymous directors are not permitted, and the names of all directors and

Money Laundering and Financial Crimes

companies must be listed when the company is organized or when there is a change in directorship. Trading companies, as a rule, operate by matching up third country supply and demand and brokering trade deals, with no goods ever entering or leaving Tunisia. The government closely monitors offshore manufacturing and tightly limits foreign ownership of Tunisian companies.

There is no limit on the amount of foreign currency that may be brought into the country, but amounts over 1,000 Tunisian dinars or its equivalent must be declared (approximately \$750). There are limits on the amount of gold that may be brought into the country. In December 2002, the legislature discussed tightening gold import regulations in light of an emerging parallel gold market.

Tunisia has no specific counter-terrorist financing law, but in November 2001, Tunisia signed the UN International Convention for the Suppression of the Financing of Terrorism. Tunisia is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Tunisia should pass a comprehensive anti-money laundering law as the first step in developing a viable anti-money laundering program. Tunisia should also criminalize terrorist financing.

Turkey. Turkey is an important regional financial center for Central Asia and the Middle East and 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 of funds laundered in Turkey. A substantial percentage of money laundering that takes place in Turkey appears to involve tax evasion. Money laundering takes place in both banks and non-bank financial institutions. Traditional money laundering methods in Turkey involve the cross-border smuggling of currency, bank transfers into and out of the country, and the purchase of high value items such as real estate, gold and luxury automobiles. Turkey is not an offshore financial center and does not have secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement officials. Since the financial crisis of 2000, the Turkish Government has taken over 19 of Turkey's 81 banks, and has significantly tightened oversight of the banking system through an independent regulatory authority.

Turkey criminalized money laundering in 1996 for a wide range of predicate offenses, including narcotics-related crimes, smuggling of arms and antiquities, terrorism, counterfeiting, and trafficking in human organs and in women. The Council of Ministers subsequently passed a set of regulations that mandate the filing of suspicious transaction reports (STRs), and require customer identification and the maintenance of records for five years. These regulations apply to banks and a wide range of non-bank financial institutions, including insurance firms and jewelry dealers. However, the number of STRs being filed is only about 100 per month, a very low number, even taking into consideration the fact that the Turkish economy is a cash-based one. A possible reason for this is the lack of safe harbor protection for bankers and other filers of STRs. Turkish officials indicated in August 2002 that the GOT has drafted a bill that will provide such protection.

Turkey also has in place a system for identifying, tracing, freezing and seizing narcotics-related assets, although Turkish law allows for only criminal forfeiture.

The GOT broadened the definition of money laundering in 2001 through adoption of three conventions of the Council of Europe (CE): the CE Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime; and the CE Criminal Law Convention on Corruption. By becoming a party to these conventions, the Turkish Government agreed to include proceeds of all serious crimes in the definition of money laundering, and to specify corruption as a predicate offense for money laundering. As of December 2002, the GOT had submitted to the Turkish Parliament a draft law that would add bribery to the list of predicate offenses for money laundering.

In July 2001, the Ministry of Finance issued a circular of banking regulations requiring all banks, including the Central Bank, securities companies, and post office banks, to record tax identity information for all customers opening new accounts, applying for checkbooks, or cashing checks. Tax identity disclosure will also be obligatory for cash transfers exceeding \$4,000. The circular also required exchange offices to sign

contracts with their clients and to record tax identity information for all transactions over \$3,000. Financial institutions will have to obtain tax identity information before cashing customers' securities. And non-interest bearing entities such as Islamic financial institutions are required to record tax identity information for all transactions.

The Ministry of Finance also issued a circular mandating that a tax identity number be used in all financial transactions as of September 1, 2001. The circular applies to all Turkish banks and to branches of foreign banks operating in Turkey, as well as other financial entities. The new requirements are intended to increase the government's ability to track suspicious financial transactions.

The 1996 anti-money laundering law established the Financial Crimes Investigation Board (MASAK), which is part of the Ministry of Finance, which receives, analyzes and refers STRs for investigation. MASAK serves as Turkey's financial intelligence unit (FIU). MASAK has a pivotal role between the financial community, on the one hand, and Turkish law enforcement, investigators and judiciary, on the other. In 2002, MASAK received a grant from the European Union to set up a new database system that will give it direct online access to all Turkish government databases. In 1997, the GOT established the Financial Crimes Investigative Board (FCIB). Since that time, the FCIB has pursued more than 500 money laundering cases. Of those, 59 have been prosecuted, with only one case resulting in a conviction. Most of the cases involve non-narcotic criminal actions or tax evasion; roughly 30 percent are narcotics related. It is believed that Turkish-based traffickers collect and transfer money to pay narcotic suppliers in Pakistan and Afghanistan, primarily by using money exchanges in Istanbul. The exchanges in turn wire transfer the funds through Turkish banks to accounts in Dubai and other locations in the Gulf. The money or value is then transferred, often through alternative remittance systems, to narcotics suppliers in Pakistan and Afghanistan.

Turkey cooperates closely with the United States and its neighbors to support the development of a regional anti-crime center in the Balkans under the Southeast Europe Cooperation Initiative (SECI). Turkey and the United States have a MLAT and cooperate closely on narcotics and money laundering investigations.

Turkey is a party to the 1988 UN Drug Convention and is a member of the Financial Action Task Force. MASAK is an active member of the Egmont Group. In December 2000 Turkey signed, but has not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Turkey has traditionally taken a strong stance against terrorism. In May of 2002, Turkey became a party to the UN International Convention for the Suppression of Terrorist Bombings. In February 2002, MASAK issued General Communique No. 3 that detailed a new type of suspicious transaction report to be filed by financial institutions in cases of terrorist financing. Turkey also became a party to the UN International Convention for Suppression of the Financing of Terrorism on June 28, 2002. The GOT has the authority to identify and freeze the assets of terrorist individuals and groups designated by UN 1267 Sanctions Committee, and it froze such assets in several cases during 2002. Although Turkey has not specifically criminalized the financing of terrorism, there are various laws that have provisions which can be used to punish the financing of terrorism. In particular, Article 169 of the Turkish Penal Code prohibits assistance in any form to a criminal organization and any organization which acts to influence public services, media, proceedings of bids, concessions and licenses; to gain votes by using or threatening violence; to commit crimes by implicitly or explicitly intimidating and cowering people is illegal under the provisions of the Law No. 4422 on the Prevention of Benefit-Oriented Criminal Organizations.

Turkey has demonstrated a commitment to fight money laundering and terrorist financing. The GOT should enact its safe harbor bill to protect the filers of STRS, which may result in increased filings. Tax evasion remains a severe problem in Turkey and is directly linked to money laundering. Turkey's 2001 initiative on tax identity numbers should enhance its ability to prosecute tax evaders. Turkey should also regulate and investigate alternative remittance networks for to thwart misuse by terrorist organizations or their supporters.

Turkmenistan. Turkmenistan has only a few international banks and a small, underdeveloped domestic financial sector. Turkmenistan's economy is primarily cash-based. Due to the presence of narcotics-trafficking and organized criminal groups, the country's several foreign-owned hotels and casinos could be vulnerable to financial fraud and money laundering. In addition, the national currency, the manat, has an accepted black market exchange rate that is four times the official rate. These rates create conditions that are favorable to money laundering. Corruption in Turkmenistan is also a source of concern due to the low salaries and broad general powers of Turkmen law enforcement officials. The Government of Turkmenistan did not report any suspected cases of money laundering in 2002.

Article 242 of the Criminal Code imposes liability for the laundering of criminal proceeds. Financial and other transactions using criminal proceeds are punishable by a fine or up to two years imprisonment. Presidential Resolution 0210/02-2 of 1995 gives the Central Bank authority over all international financial transactions. Under this resolution, any entity making an electronic transfer of funds to an account abroad must provide documentation that establishes the source of the funds.

Turkmenistan is a party to the 1988 UN Drug Convention.

Turkmenistan should criminalize terrorist financing and develop a viable anti-money laundering regime.

Turks and Caicos. The Turks and Caicos Islands (TCI) is a Caribbean overseas territory of the United Kingdom (UK). 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. 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 a large offshore financial services sector as well as because of bank and corporate secrecy laws and Internet gaming activities.

The TCI's offshore sector has eight banks (five of which also deal with onshore clientele), approximately 2,500 insurance companies, 1,000 trusts, and 13,000 "exempt companies" that are IBCs, including those formed by the Enron Corporation. 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. The Financial Services Commission employs a staff of 14 and conducts limited on-site inspections. The FSC became a statutory body under the Financial Services Commission Ordinance 2001 and became operational in March 2002, and now reports directly to the Governor.

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 custodian. This applies to all new shares issued and will be phased in for existing bearer shares within 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.

The 1998 Proceeds of Crime Ordinance criminalized money laundering related to all crimes and established extensive asset forfeiture provisions and "safe harbor" protection for good faith compliance with reporting requirements. The Law also established a Money Laundering Reporting Authority (MLRA), chaired by the Attorney General, to receive, analyze, and disseminate financial disclosures such as suspicious activity reports. Its members also include the following individuals or their designees: Collector of Customs, 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 five 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 banking, insurance, trustees, and

mutual funds. 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 non-statutory 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 suspicious activity reports (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 TCI's Financial Intelligence Unit. As of mid-2001, the FCU had received and begun investigating nine SARs.

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 but not all of them. The report noted the need for increased on-site examinations by supervisory authorities, which the government acknowledged, but which still remains a concern. 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, but the Ordinance has not yet been enacted. No legislation has yet 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.

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 new 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 Turks and Caicos have put in place a comprehensive system to combat money laundering with the relevant legislative framework and an established Financial Intelligence Unit. The TCI should move forward with by criminalizing the financing of terrorists and terrorism, and enhancing its on-site supervision program. TCI should expand recent efforts to cooperate with foreign law enforcement and administrative authorities, and join the Egmont Group in order to further ensure criminals do not abuse the TCI's financial sector.

The FSC has made steady progress in developing its regulatory capability and has some experienced senior staff. However, the current regulatory structure is not fully in accordance with international standards. Much progress has been made in enhancing the regulatory framework, with a considerable volume of new legislation passed, but TCI should continue its efforts.

Uganda. Uganda is not a regional money laundering center. Ugandan law enforcement agencies suspect that Uganda's banks and non-bank financial sector are used to launder money, but thus far have been unable to prove their suspicions because of the country's inadequate legal framework. Foreign exchange bureaus and alternative remittance systems are widely used in Uganda and are essentially unregulated.

In 2001, Uganda criminalized narcotics-related money laundering. The Bank of Uganda has issued "Know Your Customer" guidelines; however, it does not have the authority to penalize non-compliance. Uganda lacks a comprehensive anti-money laundering regime.

Money Laundering and Financial Crimes

Uganda established an interagency Anti-Money Laundering Committee in 2000, which was tasked with drafting an anti-money laundering law based on FATF principles. In August 2002, the Committee produced a draft law based on UN models, international standards and South Africa's anti-money laundering law. The draft law, which at the end of 2002 was undergoing comment and revision, contains provisions relating to suspicious transaction reporting, record keeping, legal protection for those who cooperate with law enforcement, the regulation of non-bank financial institutions, international cooperation, and asset forfeiture. As of December 2002, the issue of criminalizing money laundering for all serious crimes through the draft law was still undecided. Uganda is also working on a bill that would provide for an offshore banking sector.

Uganda criminalized terrorist financing in the Anti-Terrorism Act, which was enacted on June 7, 2002.

Uganda has signed the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) MOU and has assumed the rotating chairmanship of ESAAMLG for 2003. Uganda is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the United Nations Convention against Transnational Organized Crime, which is not yet in force internationally. Uganda has signed, but not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

Uganda should enact a comprehensive anti-money laundering regime that criminalizes money laundering for all serious crimes.

Ukraine. The lack of a comprehensive anti-money laundering system seriously impedes Ukraine's ability to combat money laundering and other financial crime. High level and widespread corruption, organized crime, smuggling and tax evasion continue to plague Ukraine's economy. Transparency International has rated Ukraine 2.4, on a scale where 10 means "highly clean." Ukraine's former Prime Minister, Pavlo Lazarenko, is in a U.S. prison awaiting trial on charges that he laundered over \$100 million, which he allegedly obtained illegally while serving as Prime Minister. Ukraine has provided assistance to the United States in connection with this prosecution.

As a member of the Council of Europe, Ukraine underwent a mutual evaluation by that group's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (Moneyval, formerly PC-R-EV) in May 2000. Although Ukraine criminalized drug money laundering in 1995, the mutual evaluation report was highly critical of Ukraine, noting significant deficiencies throughout the law enforcement, legal, and financial sectors. Paramount among the noted deficiencies was the "absence of a comprehensive anti-money laundering preventive law."

Effective September 1, 2001, the Government of Ukraine (GOU) criminalized non-drug money laundering in the Criminal Code of Ukraine. Provisions in the criminal code also address drug-related money laundering offenses and provide for the confiscation of proceeds generated by criminal activities. The GOU enacted the "Act on Banks and Banking Activities" (Act) of January 2001, which imposes counter-money laundering measures 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 Law on Financial Services and State Regulation of the Market of Financial Services" was signed. The law establishes some regulatory controls over non-bank financial institutions that manage insurance, pension accounts, financial loans, or "any other financial services involving savings and money from individuals." Specifically, the law defines financial "institutions" and "services," imposes record keeping requirements on covered entities, and identifies the responsibilities of regulatory agencies. The law created a Committee on Supervising Financial Operations and Markets, which, with the National Bank of Ukraine and the State Commission on Securities and Stock Market, has the primary responsibility for regulating financial services markets.

When the FATF, in September 2001, placed Ukraine on the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering, its report noted that Ukraine lacked (1) a

complete set of anti-money laundering 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, FinCEN, the U.S. Financial Intelligence Unit, issued an advisory to all U.S. financial institutions instructing them to “give enhanced scrutiny” to all transactions involving Ukraine.

On December 10, 2001, the Presidential Decree “Concerning the Establishment of a Financial Monitoring Department” mandated the creation of the Financial Monitoring Department (FMD) by January 1, 2002, to function as an FIU. Under the terms of this decree, the FMD is an independent authority that operates under the Cabinet of Ministers. Under the current law the FMD becomes the Authorized Agency designed to receive and analyze financial information from first line financial institutions. With the new legislation (effective six months after signing), the FMD will have more authority and guidelines for operation.

On November 28, 2002, President Kuchma signed into law an anti-money laundering package “On Prevention and Counteraction to the Legalization (Laundering) of the Proceeds from Crime.” The law calls for customer identification, reporting of suspicious and unusual transactions to an “Authorized Agency,” and five years of record keeping. It also mandates the establishment of anti-money laundering procedures in first-line financial institutions such as banks; stock, securities, and commodity brokers; and insurance companies, among other entities. Non-cash transactions in amounts equal to or greater than 300,000 hryvnyas (approximately \$55,000) and cash transactions equal to or greater than 100,000 hryvnyas (approximately \$18,500) are to be monitored. Any transaction that is suspected of being connected to terrorist activity is to be reported to the appropriate authorities immediately. Corresponding changes to the Criminal Code to establish a money laundering offense in conformity with this law have yet to occur.

The GOU has cooperated with USG efforts to track and freeze the financial assets of terrorists and terrorist organizations. The National Bank of Ukraine (NBU), State Tax Administration, Ministry of Finance, and State Security Service (SBU) are fully aware of Executive Order (E.O.) 13224 and subsequent updates and addenda to the lists of terrorists and terrorist organizations. All agencies have tracked data that was provided, and have exchanged information. The NBU has issued orders to banks to freeze accounts of individuals or organizations listed in the E.O. and later lists. There are, however, problems (which the Ukrainians themselves recognize) of coordination among agencies, and serious gaps in legislation and regulation. Many of the difficulties are directly related to what the FATF had already noted, and the GOU is working to address these issues. The GOU has also taken appropriate steps to implement UN Security Council resolutions relevant to fighting terrorism. The Cabinet of Ministers, on December 22, 1999, issued a resolution ordering agencies and banks to freeze Taliban funds as specified in UNSCR 1267. A Cabinet of Ministers resolution, on April 11, 2001, instructed the NBU to order all banks to comply with UNSCR 1333. In response to these measures, the NBU sent letters to regional departments and commercial banks to execute all applicable provisions of UNSCRs 1267 and 1333.

Ukraine is a party to the 1988 UN Drug Convention as well as the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, which came into force with respect to Ukraine in January 1998. 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 has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. In January 2002, the European Convention on the Suppression of Terrorism was signed. Ukraine ratified the UN International Convention for Suppression of the Financing of Terrorism in December 2002.

FATF gave Ukraine until October 2002 to enact comprehensive, effective anti-money laundering legislation, or it would face the possibility of countermeasures from the FATF member countries. At its September 2002 plenum, FATF extended this deadline until December 15. Nevertheless, Ukraine had not

responded satisfactorily to its listing by FATF. On December 20, the FATF determined that Ukraine's statute did not meet international standards and announced that FATF members would impose countermeasures on Ukraine. Under Section 311 of the USA PATRIOT Act, the United States has designated Ukraine as a jurisdiction that is a primary money laundering concern and has announced possible countermeasures.

By passing its legislation, Ukraine had hoped to forestall the countermeasures threatened by FATF. The FATF Europe Review Group's report to the FATF Plenary, however, highlighted a number of shortcomings and ambiguities, which make the law ineffective. Just one example is Article 8, which states unequivocally that information containing bank secrecy information may not be shared with anyone. This is in direct conflict with Article 13, which mandates turning over relevant materials to the appropriate law enforcement authorities.

Ukraine must demonstrate its political will to combat money laundering by strengthening and clarifying its newly adopted law. It must adopt appropriate regulations, amend its Criminal Code, and criminalize terrorist financing. Additionally, GOU should implement mandatory reporting of suspicious and unusual transactions to the FMD, and allow the FMD to forward cases to the appropriate authorities.

United Arab Emirates. The United Arab Emirates (UAE) is a major financial and trading center in the Gulf region of the Middle East and is located at the crossroads of major narcotics smuggling routes. It has growing ties with financial centers in Europe, Asia, southern Africa, and North America. The financial sector is modern and outward looking. Currently, the UAE financial system has 20 national banks (with 311 branches), 27 foreign banks (with 110 branches), two investment banks, five finance companies, five investment companies and 45 representative offices of foreign banks. There are 100 money exchanges (with 113 branches) operating in the country, along with 45 other financial intermediaries (brokerages) and eight banking, financial, and investment consultation establishments and companies.

The UAE's robust economic development and liberal business environment have attracted a massive influx of people and capital. Approximately 70 percent of the UAE population is comprised of non-nationals. Over 14 million people passed through Dubai's airport in 2000, and 50 million are projected by the year 2010. The UAE, like all countries in the region, is a cash-intensive society. In addition, Dubai is the regional gold center with integrated gold trading ties between Europe and South Asia. Gold is often manipulated by money launderers around the world via trade or as part of alternative remittance systems such as the South Asia-based hawala system of transferring funds. All of these factors suggest that the UAE is at high risk for money laundering. Due to the volume of goods passing through the UAE, the Gulf Arabs' traditional role as business brokers, and lax customs control, the UAE is particularly vulnerable to trade-related money laundering.

In January 2002, the President of the United Arab Emirates promulgated Law No. 4 criminalizing all forms of money laundering activities. All persons, financial institutions, and other commercial and economic establishments will be criminally liable for the offense of money laundering. Such offenses are punishable by imprisonment (up to seven years) and steep fines.

The UAE, and in particular Dubai, is a major international hawala and currency exchange center. The fact that hawala is an undocumented and non-transparent system, and is highly resilient in response to enforcement and regulatory efforts, makes it difficult to control and a highly lucrative mechanism for terrorist and criminal exploitation. The UAE has begun to make progress in publicly accepting its vulnerability and involvement vis-à-vis hawala.

The UAE hosted an International Conference on Hawala in May 2002, which was attended by over 300 delegates including government officials, executives of supervisory institutions, banking experts, and law enforcement officials from 58 countries. The conference concluded with the issuance of "The Abu Dhabi Declaration on Hawala," which calls for the establishment of a sound mechanism to regulate hawala. The Central Bank of the UAE drafted a system for registering and supervising the hawaladars (the hawala brokers). The Board of Directors of the Central Bank approved the system, and it is being implemented.

Advertisements are published in the local press calling on hawaladars to register at the Central Bank and receive a certificate—free of charge—with minimum red tape. They are then required to provide details of remitters and beneficiaries on a special spreadsheet, and deposit such sheets at the Central Bank. They are also required to report suspicious transfers.

The supervision of the UAE banking and financial sector falls under the authority of the Central Bank. The Central Bank issues instructions and recommendations as deemed appropriate and is permitted to take any necessary measure to ensure the integrity of the UAE's financial system. The Central Bank issues licenses to financial institutions under its supervision and may impose administrative sanctions for compliance violations.

UAE anti-money laundering measures can be found in a series of rules and regulations issued by the Central Bank, and thus, are generally applicable to those financial entities that fall under its supervision. There are a number of circulars issued by the Central Bank requiring customer identification and providing for a basic suspicious transaction-reporting obligation. Current regulations require that all cash transactions exceeding 200,000 dirhams (\$54,500) be reported. When suspicious activity is reported from a financial institution, the Central Bank is able to freeze suspect funds, make appropriate inquiries, and coordinate with law enforcement officials.

In July 2000, the UAE established the National Anti-Money Laundering Committee, under the Chairmanship of the Central Bank's Governor, with representatives from the Ministries of Interior, Justice, Finance, and Economy, the National Customs Board, the Secretary General of the Municipalities, the Federation of the Chambers of Commerce, and five major banks and money exchange houses (as observers). It has overall responsibility for coordinating anti-money laundering policy.

Following a review of current practices by the Committee, in November 2000 the Central Bank issued Circular 24/2000, which consolidates and expands anti-money laundering requirements for the financial sector. It is applicable to all banks, money exchanges, finance companies, and other financial institutions operating in the UAE. The Circular provides 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 Circular 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.

With implementation of Law 4/2002 came the establishment of the Anti-Money Laundering and Suspicious Case Unit (AMLSCU), which is located within the Central Bank. Financial institutions under the supervision of the Central Bank are required to report suspicious transactions to the AMLSCU, which is charged with examining them and coordinating the release of information with law enforcement and judicial authorities. It has the authority to request information from foreign regulatory authorities in carrying out its preliminary investigation of suspicious transaction reports. Officials indicate that exchanges with foreign Financial Intelligence Units are possible, provided the exchanges are conducted on a basis of reciprocity. The AMLSCU, which is a member of the Egmont Group, is exploring areas of information sharing with other Financial Intelligence Units. AMLSCU has provided information relating to investigations carried out by international authorities.

The National Anti-Money Laundering Committee issued a Cautionary Notice in the local press to make the general public aware of the possibilities through which terrorist financing could be transacted and has urged avoidance of such possibilities. UAE has extended full support and cooperation to the UN and U.S. authorities in their efforts to track the accounts of terrorists. Under UNSCR 1267/1390, UAE has frozen accounts of certain organizations and individuals with amounts equal to approximately \$3 million.

Four known money laundering cases involving foreign nationals have been referred to courts. Some cases ended in convictions.

Money Laundering and Financial Crimes

The government monitors registered charities and requires the organizations to keep records of donations and beneficiaries. The Ministry of Labor and Social Affairs regulates charities and charitable organizations in UAE.

The UAE is noted for its growing free trade zones (FTZs). There are well over a hundred multinational companies located in the FTZs with thousands of 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 treated as being offshore or outside the UAE for legal purposes.

The UAE is a party to the 1988 UN Drug Convention, and it has entered into a series of bilateral agreements on mutual legal assistance. The UAE is a member of the Gulf Cooperation Council, which is a member of the Financial Action Task Force (FATF). The UAE has been generally receptive to U.S. Government overtures to cooperate on money laundering issues, and has welcomed money laundering-related training and visits by U.S. officials.

The United States and the UAE continue to share information on exchanging records in connection with terrorist financing and other money laundering cases on an ad hoc basis. The AMLSCU has conducted more than 55 workshops in 2002 jointly with U.S., German, UK, and other international banking authorities.

Following the September 11 terrorist attacks in the United States and revelations that terrorists had moved funds through the UAE, Emirati authorities acted to address potential vulnerabilities, and in close concert with the United States, to freeze the funds of groups with terrorist links. The UAE Government has demonstrated that it recognizes the need to implement an effective anti-money laundering system to protect the nation's security and has begun constructing a far-reaching anti-money laundering program. However, there remain areas requiring further action. The UAE should criminalize terrorist financing to ensure that its financial institutions are not misused by terrorist organizations or their supporters. The government should continue with its efforts to examine trade-related and alternative remittance money laundering vulnerabilities. There is currently an over-reliance on suspicious transaction reports to generate money laundering investigations. Law enforcement and customs officials should begin to take the initiative to recognize money laundering activity and proactively develop cases.

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 drugs are still the major source of illegal proceeds for money laundering, the proceeds of other offenses, such as financial fraud and the smuggling of 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. Criminals continue to use bureaux de change (small tourist-type currency exchanges), cash smuggling in and out of the UK, professional money launderers (including solicitors and accountants), and the purchase of high-value assets as disguises for illegally obtained money.

The UK has implemented the provisions of the European Union's Directive on the prevention of the use of the financial system for the purpose of money laundering and the Financial Action Task Force (FATF) Forty Recommendations on Money Laundering. Narcotics-related money laundering has been a criminal offense in the UK since 1986. The laundering of proceeds from all other crimes is criminalized by subsequent legislation. Banks and non-bank financial institutions in the UK must report suspicious transactions.

Bank supervision falls under the Financial Services Authority (FSA). The FSA's primary responsibilities are in areas relating to the safety and soundness of the institutions in its jurisdiction. The FSA also plays an important part 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 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.

The UK's banking sector provides accounts to residents and non-residents, who can open accounts through private banking activities or 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 non-resident accounts for a tax advantage or for investment purposes.

In November 2001, money laundering regulations were extended to money service bureaus (e.g., bureaux de change, money transmission companies). The UK Government plans to bring more areas of the financial services industry into the regulated sector, making them subject to suspicious transactions reporting requirements. These areas of the industry would include attorneys, solicitors, real estate agents, and dealers in high value goods. 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.

On July 24, 2002, the Proceeds of Crime Act 2002 was enacted, and it did not become effective until January 1, 2003. The legislation enhances the efficiency of the forfeiture process, and increases 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 civil asset forfeiture system for the proceeds of unlawful conduct. It also creates the Assets Recovery Agency (ARA), to enhance the 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 related to people who benefit from criminal conduct, and for restraint orders to prohibit dealing with property; and allows the recovery of property that is, or represents, property obtained through unlawful conduct, or that is intended to be used in unlawful conduct.

Further, 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. Additionally, it creates for the regulated sector a new imprisonable offense of failing to disclose suspicious transactions in respect to all crime, not just narcotics- or terrorism-related crimes, as was the case previously. Along with the Proceeds of Crime Act of 2002 came an expansion of investigative powers relative to large movements of cash in the United Kingdom. In light of this, Her Majesty's (HM) Customs has increased its national priorities to include investigating the movement of cash through money exchange houses and identifying unlicensed money remitters.

Suspicious transaction reports (STRs) are filed with the Economic Crime Bureau (ECB) of the National Criminal Intelligence Service (NCIS). The NCIS serves as the UK's Financial Intelligence Unit (FIU). The ECB analyzes reports, develops intelligence, and passes information to police forces and Her Majesty's Customs and Excise for investigation. In 2001, the ECB received approximately 32,000 STRs. The ECB estimates it will receive roughly 65,000 STRs in 2002.

The Terrorism (United Nations Measures) Order 2001 makes it an offense for any individual, without a license from the Treasury, 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.

As a direct result of the events of September 11, 2001, the ECB established a separate Terrorist Finance Team (TFT) to maximize the effect of reports from the regulated sector. The TFT chairs a law

enforcement group to provide outreach to the financial industry concerning requirements and typologies. The operational unit that responds to the work and intelligence development of the TFT has seen a threefold increase in staffing levels directly due to the amount of work that is being produced. The Metropolitan Police responded to the growing emphasis on terrorist financing by expanding the focus and strength of their specialist financial unit dedicated to this area of investigations. This unit is now called the National Terrorist Financing Investigative Unit (NTFIU).

On November 19, 2002, Chancellor Gordon Brown ordered financial institutions in the UK to freeze funds belonging to the Benevolence International Foundation (BIF). BIF's Chief Executive, Enaam Arnaout, a Syrian-born U.S. citizen, was recently indicted in the United States for running a racketeering enterprise, conspiracy to launder money, money laundering, wire and mail fraud, and providing material support to organizations, including Usama Bin Ladin's terror network.

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 is a member of FATF and the European Union. In January 2000, the UK signed the UN International Convention for the Suppression of the Financing of Terrorism and later ratified the Convention on March 7, 2001. In December 2000, the UK signed, but has not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. The NCIS 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 and UK recently negotiated an asset sharing agreement that is merely awaiting signature by the appropriate parties. The UK also has an MLAT with the Bahamas. Additionally, there is an MOU between the U.S. Customs Service and HM Customs and Excise.

The UK should continue the strong enforcement of its comprehensive anti-money laundering program and its active participation in international organizations to combat the domestic and global threat of money laundering.

Uruguay. In the past, Uruguay's strict bank secrecy laws, liberal currency exchange regulations, and overall economic stability made it vulnerable to money laundering, although its extent and exact nature were unknown. In 2002, however, banking scandals and mismanagement, along with massive withdrawals of Argentine deposits led to a near collapse of the Uruguayan banking system, and an end to Uruguay's role as a regional financial center. This probably serves to greatly diminish the attractiveness of Uruguayan financial institutions to money launderers in the foreseeable future. Over the last five years, the Government of Uruguay (GOU) has instituted several legislative and regulatory reforms in connection with the further consolidation of its anti-money laundering program. In May 2001, it enacted Law 17,343, which extended the predicate offenses for money laundering beyond narcotics-trafficking and corruption to include terrorism, smuggling (above the threshold of \$20,000); illegal trafficking in weapons, explosives and ammunition; trafficking in human organs, tissues or medications; trafficking in human beings; extortion; kidnapping; bribery; trafficking in nuclear and toxic substances; and illegal trafficking in animals or antiques. The courts have the power to seize and later confiscate property, products or financial instruments linked to money laundering activities.

The deputy chief of staff of the President works with the National Drug Board, which is the senior authority directing anti-money laundering policy. The Center for Training on Money Laundering serves as a forum for discussion and advice on policy as well as allowing private sector input. The Financial Information and Analysis Unit (UIAF), which works with Central Bank personnel, acts as a Financial Intelligence Unit, receiving, analyzing, and remitting to judicial authorities suspicious transaction reports. The Ministry of Finance and Economics, 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 private sector has also 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 (in 1997), the Association of Exchange Houses (2001), and the Securities Market (2002).

According to GAFISUD, Uruguay's laws and regulations meet most of the FATF 40 Recommendations on Money Laundering. Money laundering is considered a crime separate from underlying crimes such as narcotics-trafficking, administrative corruption, terrorism or smuggling, which are formally listed in the legal statutes. The GOU can confiscate or preventively impound assets, proceeds or instruments used or intended to be used in money laundering crimes. However, real estate ownership is not registered in the name of the titleholder, which makes tracking money laundering in this important sector difficult, particularly in the partially foreign-owned tourist industry around Punta del Este. Safeguarding the financial sector from money laundering activities is a priority for the GOU. A series of Central Bank regulations require banks (including offshore), currency exchange houses, and stockbrokers to implement anti-money laundering policies, including the recording in internal databases transactions over \$10,000, and the reporting of suspicious transactions. In addition, the insurance and reinsurance sector, stock market, and currency exchange houses must know and thoroughly identify their customers, and report suspicious financial transactions to UIAF. The UIAF was created in December 2000, within the Superintendency of Financial Intermediation Institutions, to coordinate all anti-money laundering efforts. The UIAF, receives, analyzes, and remits to the judicial authorities, when appropriate, suspicious transaction reports. The Central Bank Circular 1722 that created the UIAF also generally provides UIAF the ability to respond to requests for international cooperation.

The insurance sectors are further required to maintain a registry of "relevant" transactions, such as payments of insurance premiums of \$10,000 or more, while stock and investment fund administrators must maintain a registry of individuals and entities exchanging currency or other valuables in amount greater than \$10,000. There are twelve offshore banks and six offshore mutual fund companies. The offshore banks are subject to the same laws and regulations as local banks, and are required to be licensed by the GOU—a process involving background checks on license applicants. There are no records of the number of Uruguayan offshore firms or shell companies, although, a large number are believed to exist. 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.

Uruguay remains active in international anti-money laundering efforts. It is a party to the 1988 UN Drug Convention. Uruguay is a member of the Financial Action Task Force for South America (GAFISUD) and the deputy chief of staff of the President, has been named President of the GAFISUD for 2003. Uruguay is also a member of the OAS Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering. The USG and the GOU are parties to an extradition treaty and a mutual legal assistance treaty that entered into force in 1984 and 1994, respectively. Uruguay has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Uruguay has also signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism.

The GOU should take steps necessary to bring it into compliance with the FATF Special Eight Recommendations on Terrorist Financing. Effective implementation and enforcement of these anti-money laundering measures must remain a priority for the GOU in order to eliminate the potential for money laundering and terrorist financing activities throughout its financial sector.

Uzbekistan. Uzbekistan is not considered an important regional financial center and does not have a developed financial system. Reportedly, Uzbek citizens and residents attempt to avoid using the official banking system for transactions, except when required by law. There is little trust in current financial controls. In Uzbekistan, the majority of the population hold savings in the form of cash dollars stored at home. There is a significant black market for smuggled goods in Uzbekistan. Since the Government of Uzbekistan (GOU) imposed a restrictive trade and import regime in mid-2002, the smuggling of consumer goods increased dramatically. Many Uzbek citizens make a living by shuttle-trading goods from neighboring countries, Iran, the Middle East, India, Korea, Europe, and the United States. The basically un-reported and un-monitored trade is very susceptible to trade-based money laundering. It is thought that narcotics traffickers exchange their proceeds on the black market, allowing small-scale business people access to drug dollars. As in neighboring countries, narcotics can also act as a commodity, and they

Money Laundering and Financial Crimes

are frequently bartered or traded for desired goods. Illicit proceeds are often carried across Uzbekistan's borders for deposit in other countries' banking systems, such as in Kazakhstan, Russia, or the United Arab Emirates.

Foreign exchange controls formally limit the availability of foreign currency in the economy. The controls also inadvertently encourage the use of alternate remittance systems. Cash proceeds of crime denominated in the local currency, the soum, can easily be converted into other currencies on the black market. Residents and non-residents may bring the equivalent of \$10,000 into the country tax-free. Amounts in excess of this limit are assessed a one percent duty. Non-residents may take out as much currency as they brought into the country. However, residents are limited to the equivalent of \$1,500. Nonetheless, foreign currency is readily available to criminals, via the thriving black market.

There appears to be little money laundering through formal financial institutions in Uzbekistan in large part due to the extremely high degree of supervision and control exercised by the Central Bank of Uzbekistan, the Ministry of Finance, and the state-owned and controlled banks. The GOU has anti-money laundering legislation. 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 4.5 million soum (\$4,000 at the black market rate) must be tracked and reported to the authorities. Institutions must report suspicious transactions immediately, via phone call and follow up memorandum to the Central Bank of Uzbekistan. Non-bank institutions such as jewelry stores and auto dealers are not required to report suspicious transactions. Banks are required to maintain records for only two years, generally not an adequate period to reconstruct suspect transactions.

Article 41 of the Law on Narcotic Drugs and Psychotropic substances (1999) stipulates that any institution may be closed for performing a financial transaction for the purpose of legalizing (laundering) proceeds derived from illicit traffic in narcotic drugs and psychotropic substances. Penalties for money laundering are from five to ten years imprisonment. Article 243 of the Criminal Code imposes penalties for the legalization of proceeds derived from criminal activity, i.e. five to ten years of imprisonment. This article also defines the act of money laundering. It includes transfer, conversion, exchange, as well as concealing of origin, true nature, source, location, disposition, movement and rights with respect to the assets derived from criminal activity as punishable acts.

In accordance with Uzbekistan's Code of Criminal Procedure, investigation of money laundering offenses falls under the jurisdiction of the Ministry of Internal Affairs. The Department of Investigation of Economic Crimes within the Ministry conducts investigations of all types of economic offenses. There are also specialized structures within the National Security Service and the Department on Combating Economic Crimes and Corruption in the Office of the Prosecutor-General, which are also authorized to conduct investigation of, inter alia, money laundering offenses.

Uzbekistan's Law Number 167 "On Fighting Terrorism", of 15 December, 2000, criminalizes terrorist financing. The law is designed to provide for the security of individuals, society, and the state from terrorism; protection of territorial integrity and state sovereignty; preserving civil peace; and preventing ethnic strife. The law names the National Security Service (NSS), the Ministry of Internal Affairs (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 anti-terrorist 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. The banking community, which is entirely state controlled and, with few exceptions, state-owned, generally cooperates with efforts to trace funds and seize accounts. Uzbekistan is a party to the UN International Convention for the Suppression of the Financing of Terrorism. The GOU has blocked terrorist assets.

Uzbekistan is a party to the UN 1988 Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally.

Vanuatu. Vanuatu's offshore sector is vulnerable to money laundering, as it has historically maintained strict 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, 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.

Vanuatu's financial sector includes five licensed banks (that carry on domestic and offshore business) and 60 credit unions, regulated by the Reserve Bank of Vanuatu. The Financial Services Commission (FSC) regulates the offshore sector that includes 55 offshore banks and approximately 2,500 "international companies" (i.e., international business companies or IBCs), as well as offshore trusts and captive insurance companies. IBCs 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.

The Serious Offenses (Confiscation of Proceeds) Act 1989 criminalizes the laundering of proceeds from all serious crimes and provides for seizure of criminal assets and confiscation after a conviction. The Financial Transaction Recording Act of 2000 requires financial institutions to identify customers and beneficial owners when establishing business relations or account accommodations. Regulatory agencies in Vanuatu have instituted stricter procedures for issuance of offshore banking licenses, and continue to review the status of previously issued licenses. This legislation requires all financial institutions, both domestic and offshore, to report suspicious transactions and to maintain records of all transactions for six years, including the identities of the parties involved. Safe harbor provisions are provided under this legislation to all suspicious transactions reported in good faith.

The Financial Transaction Reporting Act 2000 provides for the establishment of a Financial Intelligence Unit (FIU) within the State Law Office. The FIU receives suspicious transaction reports filed by financial institutions 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. These records must be kept for a period of six years after the completion of the transaction.

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 restraining of 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.

Additionally, in December 2002, Vanuatu passed the Proceeds of Crime Act of 2002. The act criminalizes the financing of terrorism. The E-Business Act No. 25 of 2000 and the Interactive Gaming Act No. 16 of 2000 regulate e-commerce. Section 5 of the E-Business legislation permits the establishment of a Vanuatu-based website where business can be conducted without residency, directors, shareholders, or a registered office. Reportedly, the E-Business Act requires online operations to maintain stringent customer

Money Laundering and Financial Crimes

identification and record-keeping requirements, as well as reporting suspicious transactions. The Financial Transaction Reporting Act of 2000 applies to e-commerce or businesses by defining any company listed under the Vanuatu Interactive Gaming Act 2000 as a financial institution.

Vanuatu is a member of the Asia/Pacific Group on Money Laundering, the Offshore Group of Banking Supervisors, the Commonwealth Secretariat, and the Pacific Island Forum. The Financial Intelligence Unit became a member of The Egmont Group in June 2002. Vanuatu has not signed the UN International Convention for the Suppression of the Financing of Terrorism or the Convention against Transnational Organized Crime, which is not yet in force internationally. Vanuatu is not a party to the 1988 UN Drug Convention. The Financial Action Task Force reviewed Vanuatu in 2000 and determined not to designate Vanuatu as non-cooperative in the fight against money laundering.

Vanuatu should immobilize bearer shares and require complete identification of the beneficial ownership of IBCs and implement all provisions of its newly enacted Proceeds of Crime Act.

Venezuela. Venezuela is not considered a regional financial center, nor does it have an offshore financial sector. The relatively small but modern banking system (71 financial institutions of which 58 are classified as banks) primarily serves the domestic market. Venezuela's proximity to drug-source countries, weaknesses in the anti-money laundering system, and corruption, continue to make it a prime target for money laundering. The main source of money laundering in Venezuela stems from proceeds generated by Colombia's cocaine and heroin trafficking organizations and anecdotal evidence suggests that some money is laundered through the real estate market in its Margarita Island free trade zone.

The 1993 Organic Drug Law provides the only legal mechanism for the investigation and prosecution of money laundering crimes. Under this law, a direct connection between the illegal drugs and the proceeds must be proven to establish a money laundering offense. The Government of Venezuela (GOV) freezes assets of individuals charged in international drug trade or money laundering cases directly related to narcotics-trafficking. If a conviction is obtained, the frozen assets are turned over to the Ministry of Finance for use in drug demand reduction programs. After the introduction of a new Code of Criminal Procedure in 1999, responsibility for initiating these actions shifted from judges to prosecutors. Due to prosecutorial unfamiliarity with the new accusatory judicial system as well as assuming the burden of tens of thousands of backlogged cases, the number of cases resulting in seizure of trafficker assets has decreased.

To expand the predicate offenses for money laundering beyond activities involving the illicit drug trade, the GOV introduced the Organic Law against Organized Crime bill. Under this bill money laundering is made a separate, autonomous offense, with no drug nexus required, and those who cannot establish the legitimacy of possessed or transferred funds and who have awareness of the illegitimate origins of those funds would be guilty of money laundering. The bill broadens assets forfeiture and sharing provisions, and provides law enforcement with stronger investigative powers by authorizing the use of modern investigative techniques such as the use of undercover agents. The bill is in its final reading in the National Assembly, but over the past six years similar legislation was never ultimately passed and the current Organized Crime bill, after years of effort, has still not been passed or enacted.

Since 1997, the Superintendence of Banks and Other Financial Institutions (SBIF) has implemented controls to prevent and investigate money laundering, including stricter customer identification requirements and the reporting of currency transactions and suspicious activity. These controls apply to all banks (commercial, investment, mortgage, private), savings and loan institutions, currency exchange houses, money remitters, money market funds, capitalization companies, and frontier foreign currency dealers.

The institutions are also required to report currency transactions of more than \$10,000 (or local currency equivalent), and suspicious transactions to a National Financial Intelligence Unit (UNIF) created in 1998 under the SBIF. The UNIF analyzes suspicious activity reports (SARs) and refers those deemed appropriate for further investigation to the Office of the Public Prosecutor, which subsequently opens and

oversees the criminal investigation. Since 1998, the UNIF has received 8,545 SARs. The UNIF is a member of the Egmont Group (since 1999) and has signed bilateral information exchange agreements with counterparts worldwide. The Venezuelan Constitution guarantees the right to bank privacy and confidentiality, but in cases under investigation by the UNIF, the Superintendence of Bank and Other Financial Institutions, or the Office of the Prosecutor, or by order of the Judge of Control, bank secrecy may be waived. Comprehensive financial and law enforcement information is available to the UNIF.

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 including the reporting of suspicious transactions and has conducted a number of training initiatives for its members. The AVCC also drafted and distributed an extensive operations manual entitled "System for the Prevention and Control of the Serious Crime of Money Laundering." Each currency exchange house in the country has and employs systems to electronically transmit transaction reports to SBIF.

Lacking the legal basis to employ modern investigative techniques, with appropriate legal safeguards, Venezuelan law enforcement authorities find it difficult, if not impossible to investigate and prosecute sophisticated criminal organizations and complex crimes such as money laundering. Indeed, there have only been a few money laundering convictions in Venezuela and all of them are narcotics related. On June 20, 2002, two Venezuelan citizens were sentenced to 15 and 25 years, respectively, for drug-related money laundering. This builds upon the single arrest and prosecution of one Venezuelan citizen in 2001, who was sentenced to 20 years in prison.

Current Venezuelan law does not specifically mention crimes of terrorism. The Organized Crime Bill would rectify this by defining terrorist activities and establishing punishments of up to 20 years in prison. The Bill's expanded definition of money laundering would also make it possible to prosecute those engaged in terrorism financing and to freeze and seize their assets.

Venezuela participates in the Organization of American States Inter-American Commission on Drug Abuse Control (OAS/CICAD) Experts Group to Control Money Laundering, the Caribbean Financial Action Task Force (CFATF), and the Multilateral Working Group against the Black Market Peso Exchange System. Venezuela is a party to the 1988 UN Drug Convention and has signed and ratified the UN Convention against Transnational Organized Crime, which is not yet in force internationally. This Convention was ratified by the National Assembly, made into a Law of the Republica Bolivariana of Venezuela on December 15, 2000, and published in the Official Gazette No. 37.357 on January 2002. On November 16, 2001, the GOV signed, but has not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

The GOV continues to share money laundering information with U.S. law enforcement authorities under the 1990 anti-drug money laundering agreement. The information shared has supported U.S. domestic operations, resulting in the seizure of significant amounts of money and several arrests in the United States.

The GOV should enact measures such as the criminalization of the financing of terrorists and terrorism and institute measures to be able to expeditiously freeze terrorist assets, in order to implement the FATF Special Eight Recommendations on Terrorist Financing. The GOV should enact the Organic Law Against Organized Crime to provide law enforcement and judicial authorities the much-needed tools for the effective investigation and prosecution of money laundering and other financial crimes.

Vietnam. Vietnam is not an important regional financial center. The Vietnamese banking sector is underdeveloped and the Government of Vietnam (GVN) controls the flow of all U.S. dollars in official channels. The nature of the banking system makes it unlikely that major money laundering or terrorist financing is currently occurring in financial institutions. The "drug economy" exists in Vietnam's informal financial system. Vietnam has a large "shadow economy" in which U.S. dollars and gold are the preferred currency. Due to the limited size of Vietnam's banking system and currency exchange controls, even

legitimate businesses carry on transactions in this “shadow economy.” In addition, Vietnamese regularly transfer money through gold shops and other informal mechanisms to remit or receive funds from overseas. Officially, expatriate remittances account for one billion U.S. dollars and unofficially the number may be more than double that amount. There is speculation that a percentage of intra-familial transactions in this alternative remittance system may result from narcotics proceeds.

Vietnam does not yet have a separate law on money laundering or terrorist financing. However, 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 counternarcotics agency the authority to require disclosure of financial and banking records when there is a suspected violation of the law. However, the implementing regulations have not yet been promulgated. The State Bank of Vietnam, which has the lead on countering terrorist financing, can also request the disclosure of information when it believes that a transaction might fall within this category. Furthermore, the State Bank requires banks to report suspicious transactions of any kind.

The World Bank is working with the GVN on draft banking legislation. This legislation may also include a section on money laundering. The GVN is also working with international agencies to increase its banking supervision capabilities.

The GVN is a party to the UN International Convention for the Suppression of the Financing of Terrorism. The GVN should pass separate terrorist financing legislation if it is not included in the current anti-money laundering draft legislation that is expected to cover all serious crimes. The GVN should also establish cross border currency controls and regulate the use of gold as an alternative remittance system.

Yemen. Yemen has no anti-money laundering legislation. Though the extent of money laundering is not known, the lack of legislation and the prevalence of hawala make Yemen vulnerable to money laundering. Yemen’s banking sector is relatively small with 14 commercial banks, including three Islamic banks. The Central Bank of Yemen (CBY) supervises the country’s banks. Local banks accounted for approximately 62 percent of the total banking activities, while foreign banks covered the other 38 percent.

In April 2002, the CBY issued Circular 22008, informing 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 through banks at which they have no accounts. The same provision applies to beneficiaries of such transfers. Banks must also take every precaution when transactions appear suspicious, and report such activities to the CBY. The circular was distributed to the banks along with a copy of the Basel Committee’s “Customer Due Diligence for Banks,” concerning “Know Your Customer” procedures.

At the end of 2002, the parliament was in the process of enacting anti-money laundering legislation. The governor of the CBY has prepared a primary draft that has been presented to the bankers’ association and other financial bodies for recommendations. The proposed anti-money laundering law – which has been also reviewed and approved by the Ministry of Legal Affairs – criminalizes money laundering for a wide range of crimes including narcotics offenses, kidnapping, embezzlement, bribery, fraud, tax evasion, illegal arms trading, and money theft, and imposes penalties of three to five years’ imprisonment. There is no specific legislation relating to counter-terrorist financing in Yemen. But terrorism is covered in various pieces of legislation that treat terrorism and its financing as serious crimes.

The proposed law requires banks, financial institutions, and precious commodity dealers to verify the identity of persons and entities that want to open accounts or deal with them, keep records of transactions for up to ten years and report suspicious transactions. In addition the draft law requires that reports be submitted to an information-gathering unit within the CBY. The unit will act as the Financial Intelligence

Unit (FIU), which in turn will report to an Anti-Money Laundering Committee (AMLC). Under the proposed law the AMLC – which will have representatives from the Ministries of Finance, Justice, Interior, and Industry and Commerce, the CBY, and the Board of Banks – is authorized to issue regulations and guidelines and provide training workshops related to combating money laundering efforts.

The proposed law grants the AMLC the right to exchange information with foreign entities. The head of the committee can ask local judicial authorities to enforce foreign court verdicts based on reciprocity. Also, the proposed law will permit the extradition of criminals in accordance with international treaties or bilateral agreements. CBY states that although the law is expected to pass in 2003, banks have begun applying its money laundering combating provisions in anticipation of its passage.

In response to UNSCR 1267/1390 and Yemen's Council of Ministers directives, CBY issued a number of circulars to all banks operating in Yemen directing them to freeze accounts of 144 persons, companies, and organizations, and to report any finding to CBY. As a result, one account was immediately frozen with a balance equal to \$33.

A law was passed in 2001 governing charitable organizations. This law entrusted the Ministry of Pensions and Social Affairs with overseeing their activities. The law imposes penalties of fines and/or imprisonment on any society or its members for carrying out activities or spending funds for other than the stated purpose for which the society in question was established.

Yemen is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Yemen is a member of the Arab Convention for the Suppression of Terrorism.

Although the Government of Yemen has made some attempts to improve the country's domestic anti-money laundering program and to cooperate internationally with criminal investigations, serious deficiencies remain. As a crucial first step to address these deficiencies, Yemen should pass, implement, and enforce the proposed anti-money laundering legislation. This would constitute a significant step toward meeting international standards. Yemen should also enact specific legislation with respect to the financing of terrorism and terrorists.

Yugoslavia, Federal Republic of. Narcotics-trafficking, smuggling, money laundering, and other criminal activities are continuing at a noticeable level in the Federal Republic of Yugoslavia. Yugoslavia is a transit country for illegal drugs moving along the Balkan route from Asia to Europe and the Americas. Yugoslav officials maintain that the majority of criminal proceeds from drug trafficking laundered in Yugoslavia are derived from illegal activities of the Kosovar Narco-Mafia. Since 1999, the Government of Yugoslavia has had no jurisdiction over Kosovo, based on UNSCR 1244, so Yugoslav authorities must rely on cooperation with UNMIK police and KFOR to combat these activities. Officials estimate that up to half of all financial transactions in Yugoslavia may be connected with money laundering.

In 2002, Yugoslavia decided to divide into a looser confederation of Serbia and Montenegro. This has had an impact in some ways on the laws and regulations on corruption and money laundering. Montenegro has decided to use the euro as its standard of currency, while Serbia has stayed with the dinar. In early 2003, a new constitutional charter will be ratified and implemented that will re-define relations between Serbia and Montenegro. When this charter becomes effective, it will affect ministries and departments currently under federal jurisdiction, and transfer them to or establish them in the governments of the respective states.

The year 2002 saw Yugoslavia, and then Serbia, concentrate on removing restrictions on current account transactions to enable the dinar to be declared convertible. It was proposed that Yugoslav individuals be allowed to transfer up to 5,000 euros each in cash abroad and Yugoslav companies be able to provide advance hard-currency payments for imports from abroad, borrow abroad, and make hard-currency repayments on loans. However, the government also determined that all transfers abroad must be strictly monitored to guard against money laundering. In addition, some restrictions remain: individuals may not borrow, open accounts, or buy real estate abroad, and companies cannot lend or invest abroad.

Money Laundering and Financial Crimes

The Yugoslav Federal Assembly adopted an Anti-Money Laundering Law in September 2001. In March 2002, Yugoslavia divided into Serbia and Montenegro, and the law that went into effect became the law for the Serbia portion of Yugoslavia. The Serb Law came into effect in July 2002 and brings Serbia into line with the FATF Forty Recommendations. The law defines money laundering to mean depositing, or introducing into the financial system in any manner, money that has been acquired through illegal activity. This includes money derived from the gray market economy and arms and narcotics-trafficking. Among the entities required to take actions and measures aimed at uncovering and preventing money laundering under the law are: commercial and savings banks, other financial credit institutions, the postal savings bank, the post office, commercial enterprises, all government entities, the National Bank of Yugoslavia and its clearing and payments department, foreign exchange bureaus, casinos, pawnshops, stock exchanges, and national lottery organizers.

The covered entities are required to identify persons opening an account “or establishing any other kind of lasting business cooperation with the client” and report on every transaction exceeding 600,000 dinars (about \$10,000). Criminal penalties for money laundering violations range from six months to five years in prison, while civil penalties range from 45,000 to 450,000 dinars (\$750 to \$7,500) per offense. This law, when taken with the penal code and criminal procedure law, provides for the temporary seizing and permanent confiscation of assets derived from or used for criminal activities. It also authorizes the government to revoke business licenses and ban business activities of legal entities and natural persons involved in criminal activities.

The anti-money laundering law also provides for the establishment of a Financial Intelligence Unit (FIU). The Serb FIU, called the Federal Commission for the Prevention of Money Laundering (FCPML), became operational in July 2002, as mandated by the law. The Commission functions as an administrative unit. Currently, the staff of the FCPML numbers 18, but it expects to hire another ten analysts when the unit is transferred from federal jurisdiction to that of the Serbian Finance Ministry, probably in Spring 2003.

The Republic of Montenegro also prepared a law against money laundering, which is expected to be adopted in early 2003 and when effective will compel covered entities to report transactions meeting or exceeding 15,000 euros, the EU standard. As interim measures in 2002, Montenegro amended its penal code to criminalize money laundering and enable the government to seize and confiscate assets involved in criminal activity. In addition, the Central Bank began to require financial institutions to report suspicious transactions, establish anti-money laundering programs and train personnel in relevant matters. The Republic of Montenegro also required offshore banks to re-register, post a \$1 million Eurobond, and establish themselves as regular banks. No offshore institutions have done this, and Montenegro considers them to be dissolved.

The new law, when effective, is expected to bring Montenegrin standards into line with the European Convention definition of money laundering as well as the FATF Forty Recommendations. Under the law, covered entities include all banks, savings-credit unions, any legal entities that have been entirely or partially financed from state funds, investment and pension funds and other financial institutions, post offices, telecommunication companies, other companies and unions, the Privatization Council, insurance companies, stock exchanges and other financial institutions authorized to perform operations related to securities, offshore companies, exchange offices, pawnbrokers, gambling houses, bookmakers, slot machine clubs, and organizers of all lotteries and games of chance. Like the Serb law, the Montenegrin law also provides for the establishment of an FIU, known as the Office for the Prevention of Money Laundering. The FIU, to be housed in the Ministry of Finance, will function as an administrative unit.

In March 2002, Article 234 of the Law on Criminal Procedure was introduced, which authorizes an investigating judge to order financial institutions to release information about business and personal accounts at the request of a state prosecutor. This law is expected to give more power to the state to detect terrorism financing because the information can be obtained faster and with less bureaucracy.

The Government of Yugoslavia also submitted a Bill on the Amendment of the Criminal Law that would sanction terrorist financing as a separate offense in line with the UN International Convention for the Suppression of the Financing of Terrorism, which Yugoslavia signed on November 12, 2001 and became a party to on October 10, 2002. The law has yet to be adopted, however.

Also proposed by Serbia but yet to be signed is a special counter-terrorism law that will upgrade legislative and institutional frameworks for combating terrorism. It takes its cue from the successes of other countries and is intended to bring Serbia into compliance with UNSCR 1373. Among the FCPML's duties is to work on fighting terrorism and terrorism financing. The FCPML is currently tracing the names on the E.O. 13224 asset freeze list. Under discussion is the idea of having a separate department within FCPML specifically charged with combating terrorism financing. The Montenegrin FIU will also track terrorism financing as well as money laundering.

Yugoslavia is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. In 2002, Yugoslavia ratified the Council of Europe Convention on the Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime, and participated in bilateral and multilateral fora to improve its analytical and seizure capabilities. Yugoslavia established a Belgrade office of Interpol to contribute to the fight against trafficking and terrorism. The Serbian and Montenegrin finance ministers joined finance ministers from Albania, Bulgaria, Croatia, Macedonia, and Republika Srpska in establishing a regional group to fight (among other economic corruption problems) money laundering.

FCPML has bilateral agreements on cooperation and information exchange with Macedonia, and expects to enter into agreements with Russia, Slovenia, Romania, and Bosnia-Herzegovina shortly. Yugoslavia also has mutual assistance agreements signed with over 20 other countries. Although there is no legislation to authorize the sharing of confiscated assets with other countries, and none is under consideration at this time. There is also no prohibition against it—leaving Serbia free to enter bilateral agreements.

Yugoslavia or its constituent parts should criminalize terrorist financing. Yugoslavia or its constituent parts still need to implement domestic legislation to support the international conventions signed in 2002. Laws should also be amended to enable the freezing and seizing of funds kept within the country by persons or entities located outside of it who have connections with international terrorist or narcotics activities. Both jurisdictions within Yugoslavia should participate in international fora that offer training and technical assistance for police, customs, and judiciary officials involved with combating transnational organized crime.

Zambia. Zambia is not a major financial center. Law enforcement officials report that cash smuggling may be occurring in connection with the trade in illicit diamonds.

The Drug Enforcement Commission has the responsibility for investigating money laundering offenses. In 2001, the National Assembly passed the Prohibition and Prevention of Money Laundering Bill, which makes money laundering a criminal offense, stiffens penalties for financial crimes, and increases the investigative and prosecutorial powers of the Drug Enforcement Commission. The law also requires financial institutions to report suspicious transactions to regulators and to retain transaction records for ten years. The law authorizes investigators to seize assets related to money laundering. The Minister of Home Affairs has reported that there are plans to form an anti-money laundering authority, which will enforce the Prevention of Money Laundering Act No. 14 of 2001.

Although Zambia participates in meetings of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), Zambia has not formally joined the group.

Zambia is not a signatory to the UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Zambia is a party to the 1988 UN Drug Convention.

Zambia should create a Financial Intelligence Unit, criminalize terrorist financing and sign the ESAAMLG Memorandum of Understanding.

Money Laundering and Financial Crimes

Zimbabwe. Zimbabwe is not a regional financial center and is not considered to be at significant risk for money laundering.

Zimbabwe's Anti-Money Laundering Act criminalizes narcotics-related money laundering. In October 2002, the Government of Zimbabwe submitted the Anti-Money Laundering and Proceeds of Crime Bill to Parliament. The bill would require banks to maintain records sufficient to reconstruct individual transactions for at least six years. The bill would also mandate a prison sentence of up to five years for a money laundering conviction.

Zimbabwe is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the United Nations Convention against Transnational Organized Crime, which is not yet in force internationally.

Zimbabwe should enact a comprehensive anti-money laundering regime that criminalizes terrorist financing and money laundering for all serious crimes. Zimbabwe should join the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), the FATF-style regional body. Zimbabwe should also sign the UN International Convention for the Suppression of the Financing of Terrorism.