

[*Text as released to Congress; see [revised version](#)]

Jordan

Jordan is not a regional or offshore financial center and is not considered a major venue for international criminal activity. The banking and financial sectors, including moneychangers, are supervised by competent authorities according to international standards. The Central Bank of Jordan, which regulates foreign exchange transactions, issued anti-money laundering regulations designed to meet the Financial Action Task Force (FATF) Forty Recommendations on Money Laundering in August 2001. Under Jordanian law, money laundering is considered an “unlawful activity” subject to criminal prosecution.

An October 8, 2001 revision to the Penal Code criminalized terrorist activities, specifically including financing of terrorist organizations. Jordan has checked for assets of individuals and entities identified by the UNSCR 1267 Sanctions Committee, although no such assets have been identified to date. In December 2004, the United States and Jordan signed an Agreement regarding Mutual Assistance between their Customs Administrations that provides for mutual assistance with respect to customs offenses and the sharing and disposition of forfeited assets.

Jordan has neither enacted a comprehensive anti-money laundering law, nor established an independent Financial Intelligence Unit (FIU). However, a draft anti-money laundering law is nearing completion for approval by the cabinet and presentation to Jordan’s parliament. Anti-money laundering efforts are handled by an anticorruption agency within the Jordanian Intelligence Services. However, Jordanian officials report that financial institutions file suspicious transactions reports and cooperate with prosecutors’ requests for information related to narcotics-trafficking and terrorism 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 (as amended in 2003) waives banking secrecy provisions in any number of criminal cases, including suspected money laundering and terrorism financing.

Jordan is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. Jordan has signed, but not ratified, the UN Convention against Transnational Organized Crime. Jordan is a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004. The MENAFATF is a FATF-style regional body. The creation of the MENAFATF is critical for pushing the region to improve the transparency and regulatory frameworks of its financial sectors.

The Government of Jordan has taken steps in constructing an anti-money laundering and terrorist financing program, but much remains to be done. Specific anti-money laundering legislation should be passed recognizing all types of predicate offenses. Jordan should establish a Financial Intelligence Unit (FIU) that receives, analyzes and disseminates suspicious transaction reports to law enforcement agencies. Jordan should ratify the UN Convention against Transnational Organized Crime. Jordanian law enforcement and customs should examine forms of trade-based money laundering.

Kazakhstan

Kazakhstan, with its developed, modern banking system has become the financial center for Central Asia. Unfortunately, the lack of adequate banking regulations, widespread corruption, regular incidents of money laundering and cash smuggling, mostly related to economic crimes, and Kazakhstan’s status as a major transit hub for narcotics-trafficking from Afghanistan, also make this country a potential regional money laundering center. The Government of Kazakhstan (GOK) is a willing partner in the fight against terrorism, but weak laws, corruption, ill-trained financial police and a lack of modern equipment hamper its efforts. It is, however, taking steps to remedy these problems.

Money laundering was first criminalized in Kazakhstan by Article 30 of the 1998 counternarcotics law, which makes it illegal to launder money in connection with the sale of illegal drugs. The definition of money laundering used in the act, however, is narrow and the sanctions against it relatively light (a maximum of three years imprisonment, rising to five for multiple offences). 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 GOK has been aware for several years of problems with its policing of financial crimes and is proactively taking corrective measures. In January 2004, the State Agency for Economic Crimes and Corruption was established. The agency is an amalgam of the former Financial Police Agency and the Ministry of Internal Affairs' 9th Department on Economic Embezzlement. The newly created Agency for the Regulation and Inspection of the Financial Market and Financial Organizations is authorized to supervise all aspects of financial markets. In the past, supervision of financial markets was carried out by various state bodies and coordinated by the National Bank. The establishment of a new body, separate from the National Bank, demonstrates the government's intentions to ensure that the country's financial system is consistent with the best international practices. While the head of the new agency reports directly to the president of Kazakhstan, the agency itself continues to operate under the auspices of the National Bank with which it shares regulatory functions. The overall effectiveness of the agency is also limited by a lack of training and the absence of any legal mechanisms to ensure law enforcement's access to the information related to illegal financial operations, such as money laundering, corruption, terrorism financing and other crimes.

The Prosecutor General's Office is the lead agency in drafting new anti-money laundering and counterterrorist financing legislation and in the formation of the proposed Financial Investigative Unit (FIU). The Office of the Prosecutor General expects the legislation to be passed by the end of the first quarter (April 1, 2005), and that the FIU should be fully operational by the end of 2005. The latter is contingent on requisite funding of the FIU being provided by the Parliament during the annual GOK budget process. The Office of the Prosecutor General has the responsibility within the GOK to ensure that the provisions of the law and the function of the FIU will meet international standards and become an effective means of combating money laundering and related financial crimes.

Only one-half of 242,000 registered business entities in the country are in fact operational. In addition, it is estimated that over 93,000 businesses do not report their tax incomes. Since the beginning of 2004, the State Agency for Combating Economic Crimes and Corruption reported 421 registered money laundering cases in Kazakhstan totaling \$107 million. In early January 2004, the Almaty Prosecutor's Office charged two companies with bank fraud. The two companies were charged with illegal operations resulting in the laundering of \$7 million over a period of five months. According to the Prosecutor's Office, these crimes were conducted with the help of bank employees, making them especially difficult to detect. According to the Prosecutor General of Kazakhstan the detection of crimes involving money laundering companies is fairly low, and the above figures probably do not reflect the true scope of these crimes in Kazakhstan. Moreover, even when such crimes are detected, they often are not prosecuted. According to the Prosecutor's Office, approximately only one out of ten criminal proceedings is actually brought to court.

Kazakhstan is not an offshore financial center. There are no offshore companies or banks. Existing legislation does not favor offshore banks and financial centers. Foreign banks, including American, Dutch, Turkish, and Russian-based financial institutions have offices in Kazakhstan.

The GOK cooperated in circulating the E.O. 13224 list among Kazakhstani banks.

Kazakhstan acceded to the 1988 UN Drug Convention in 1997, and in December 2000 the country signed the UN Convention against Transnational Crime. On February 24, 2003, Kazakhstan ratified the UN International Convention for the Suppression of the Financing of Terrorism. In 2000, the GOK signed, but has not yet ratified, the UN Convention against Transnational Organized Crime.

Kazakhstan is considering acceding to the Council of Europe's Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime. Kazakhstan is a signatory of the Central Asian Agreement on Joint Fight Against Terrorism, Political and Religious Extremism, Transnational Organized Crime and Illicit Drug Trafficking, signed in April 2000 by Kazakhstan, the Kyrgyz Republic, Tajikistan and Uzbekistan. Kazakhstan is a charter member of the newly organized Eurasian Group on Combating Money Laundering and Financing of Terrorism.

The Government of Kazakhstan is still in the process of developing some of the key legal and institutional frameworks necessary to establish a viable anti-money laundering/counterterrorist financing regime. The Kazakhstan should enact comprehensive legislation, to include criminalizing terrorist financing, and implement due diligence and reporting requirements that meets international standards. Kazakhstan should continue its efforts to provide training and adequate resources to the bodies tasked with enforcing its laws and regulations.

Kenya

As a regional financial and trade center for East, Central, and Southern Africa, 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. As such, Kenya is vulnerable to money laundering. Recently Kenya has taken steps to trace millions of dollars of public funds that were laundered abroad; corruption facilitated the removal of such funds.

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, though up to now no clear instances of laundering of funds from narcotics-trafficking appear to have come to light. The Central Bank is the regulatory and supervisory authority for Kenya's deposit-taking institutions and has responsibility for over 51 entities. The Kenyan Parliament enacted legislation at the end of 2004 that strengthens the Central Bank's supervisory authority, but it makes no specific reference to money laundering.

In October 2000, the Central Bank issued regulations that require deposit institutions to verify the identity of customers wishing to open an account or conduct a transaction. The regulations also require that these institutions report suspicious transactions. Under the regulations, banks must maintain records of large transactions and report them to the Central Bank. These regulations do not cover non-bank financial institutions such as money remitters, casinos, or investment companies, and there is no enforcement mechanism behind the regulations. Some banks do file suspicious transaction reports voluntarily, but they run the risk of civil litigation, as there are no adequate "safe harbor" provisions for reporting such transactions to the Central Bank. The trigger amount is also very high: on a daily basis, all commercial banks are required to submit reports detailing all transactions greater than \$100,000. Controls on money laundering as such are rarely, if ever, applied to financial institutions or intermediaries outside the banking sector.

Kenya has little in the way of cross-boundary currency controls. Kenyan regulations require that any amount of cash above \$5,000 be disclosed at the point of entry or departure. In reality this provision is rarely enforced. Central Bank guidelines call for currency exchange firms to furnish reports on a daily basis on any single foreign exchange transaction above about \$10,000, and on cumulative daily foreign exchange inflows and outflows of about \$100,000. Under September 2002 guidelines, foreign exchange dealers are required to ensure that cross-border payments are not connected with illegal financial transactions.

The Banking Act amendment of December 2001 authorizes disclosure of financial information by the Central Bank of Kenya to any monetary authority or financial regulatory authority within or outside Kenya. 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, and only a handful of suspicious transactions have been reported so far.

Kenya is a party to the UN International Convention for the Suppression of the Financing of Terrorism. It has cooperated with the United States and the United Kingdom, but lacks the institutional capacity, investigative skills, and equipment to conduct complex investigations independently. In April 2003, the Government of Kenya (GOK) introduced the Suppression of Terrorism Bill into Parliament. The bill contains provisions that will strengthen the GOK's ability to combat terrorism, but the legislation is opposed by many for fear of human rights violations, though not because of the bill's counterterrorism aspects as such. A GOK official stated in October 2004 that the bill was in the process of being re-drafted. The public does support the government's attempts to increase transparency and to combat corruption, which include its efforts related to money laundering.

There is no legislation permitting the seizure of the financial assets of terrorists. All charitable and nonprofit organizations are registered with the Government and have to submit annual reports. Noncompliance with the annual reporting could lead to de-registration; however, this is rarely enforced. The government did de-register some non-governmental organizations with Islamic links in 1998 in the wake of the bombing of the U.S. Embassy in Nairobi, although they were later re-registered.

Kenya is a party to the 1988 UN Drug Convention. Kenya is an active member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. Kenya has an informal arrangement with the United States for the exchange of information regarding narcotics, terrorism financing, and other serious crime investigations.

At present the government entities responsible for tracing and seizing assets include the Central Bank of Kenya Banking Fraud Investigation Unit, the Kenya Police through the Anti-Narcotics Unit and the Anti-Terrorism Police Unit, and the Kenya Revenue Authority.

The passage of anti-money laundering legislation and the creation of a financial intelligence unit (FIU) by Kenya would help to formalize its relationship with the United States and with other countries. In 2001, the Government of Kenya formed the Anti-Money Laundering Task Force with the mandate of drafting a comprehensive anti-money laundering law, sensitizing the public and government to money laundering issues, and addressing terrorist financing. After the inception of the task force, a bill on money laundering was drafted, but not introduced. Relevant authorities claim that the bill, entitled the Anti-Money Laundering and Proceeds Bill, will be introduced to Parliament in 2005.

The key points of the legislation include tracing, seizing, and freezing suspect accounts, including those involved in the financing of terrorism; confiscation of the proceeds of crime; declaration of the source of funds; outlawing of anonymous bank accounts; and introduction of mandatory reporting of suspicious transactions above a certain amount. The proposed legislation is not explicit on seizing legitimate business used to launder money. The draft legislation provides for criminal forfeiture only. Actual seizure of assets and forfeiture under current law is rare.

Kenya should expedite the passage of the Anti-Money Laundering and Proceeds Bill and the Suppression of Terrorism Bill as first steps in building a comprehensive anti-money laundering regime. It should also establish a financial intelligence unit (FIU) to serve as a vital part of this regime.

Korea, Democratic Peoples Republic of

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.

The Government of North Korea should enact a comprehensive anti-money laundering regime and take steps to stop financial crimes originating in North Korea and the funding of terrorism.

Korea, Republic of

South Korea is not considered an attractive location for international financial crimes or terrorist financing, partly because of existing foreign exchange controls. However, such activities do exist. As law enforcement authorities have gained more expertise investigating money laundering and financial crimes, they have also become more cognizant of the problem. In general, however, the still fairly strict foreign exchange controls in place make it difficult for drug-related or terrorism-related money laundering to flourish.

Most money laundering appears to be associated with domestic criminal activity or corruption and official bribery. Still, criminal groups based in South Korea maintain international associations with others involved in human and contraband smuggling and related organized crime. On the whole, the South Korean government has been a willing partner in the fight against financial crime, and has pursued international agreements toward that end. The Financial Transactions Reports Act (FTRA), passed in September 2001, requires financial institutions to report suspicious transactions to the Korea Financial Intelligence Unit (KoFIU), which operates within the Ministry of Finance and Economy. The KoFIU was officially launched in November 2001, and is composed of 60 experts from various agencies, including the Ministry of Finance and Economy, the Justice Ministry, the Financial Supervisory Commission, the Bank of Korea, the National Tax Service, the National Police Agency, and the Korea Customs Service. KoFIU analyzes suspicious transaction reports (STRs) and forwards information deemed to require further investigation to domestic law enforcement and the Public Prosecutor's office.

In January 2004, the government tightened its requirements for STRs by lowering the monetary threshold under which they are required to file reports to 20 million won (approximately \$19,000) from the previous 50 million won. Improper disclosure of financial reports is punishable by up to five years imprisonment and a fine of up to 30 million won (about \$25,000). In December 2004, the government also adopted, through a revision of the FTRA, a currency transaction reporting (CTR) system requiring financial institutions to report all currency transactions exceeding a monetary threshold to be set by Presidential Decree. The threshold must be under 50 million won (approximately \$47,250). The FTRA revision also set customer due diligence requirements stipulating that financial institutions must identify and verify customer identification data such as address and income status. The revision will take effect in 2005, on the one year anniversary of the law's promulgation.

Between November 2001 and August 2004, KoFIU has received a total of 4,661 STRs from financial institutions, with a marked increase coming in the past year. It has completed analysis of 4,038 of them, and provided 959 reports to law enforcement agencies as of August 2004. Results were disseminated to law enforcement agencies such as the Public Prosecutor's Office (PPO), National Police Agency (NPA), National Tax Service (NTS), Korea Customs Service (KCS), and the Financial Supervisory Commission (FSC). Another 639 STRs were still under the FIU's analysis. The Korean

Customs Service reported on October 4, 2004, that it had found 23 cases of illegal financial transfers overseas (including money laundering) worth 734.8 billion won (\$639 million) as the result of a special investigation conducted between June 14 and September 30. In December 2004, local police arrested several brokers who arranged for undocumented foreign workers to send illegal remittances abroad via the illegal underground “hawala” system. Additionally, the managing directors of the SK Group, a major conglomerate, were prosecuted for laundering 10 billion won (\$8.4 million), in checks and securities, in November 2003.

KoFIU supervises and inspects the implementation of internal reporting systems established by financial institutions. KoFIU is also charged with coordinating the efforts of other government bodies, and the Policy Coordination Committee held meetings in November 2003 and March 2004 to discuss policies and revisions of the FTRA. Officials charged with investigating money laundering and financial crimes are beginning to widen their scope to include crimes related to commodities trading and industrial smuggling, and continue to search for possible links of such illegal activities to international terrorist activity. On December 1, 2004, KoFIU introduced a new online electronic reporting system, through which financial institutions can report suspicious transactions more quickly.

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.

Money laundering related to narcotics-trafficking has been criminalized since 1995, and financial institutions have been required to report transactions known to be connected to narcotics-trafficking to the Public Prosecutor’s Office since 1997. All financial transactions using anonymous, fictitious, and nominee names have been banned since the 1997 enactment of the Real Name Financial Transaction and Guarantee of Secrecy Act. The Act also requires that, apart from judicial requests for information, persons engaged in financial institutions 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.

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.

South Korea still lacks specific legislation on terrorism financing. Two versions of a new counterterrorism bill are working their way through the legislative process, though previous attempts to pass similar bills have not succeeded. Many politicians and nongovernmental organizations (NGOs), recalling past civil rights abuses in Korea by the government, oppose the pending counterterrorism legislation because of fears about possible misuse by the National Intelligence Service. The proposed legislation is crafted to allow the Republic of Korea Government (ROKG) additional latitude in fighting terrorism, though general financial crimes and money laundering have already been criminalized in previously enacted laws.

The pending counterterrorism bill, if passed, would permit the ROKG to seize legitimate businesses that support terrorist activity. Currently, under the special act against illicit drug trafficking and other related laws, legitimate businesses can be seized if they are used to launder drug money, but businesses supporting terrorist activity cannot be seized unless other crimes are committed. At this

time, there are no known charitable or nonprofit entities operating in Korea that are used as conduits for the financing of terrorism.

Through KoFIU, the ROK circulated to its financial institutions the list of individuals and entities that have been included in the UNSCR 1267 Sanctions Committee's consolidated list as being linked to Osama bin Laden or members of the al-Qaida organization or the Taliban, or which the U.S. Government (USG) or the European Union have designated under relevant authorities. The ROK implemented regulations on October 9, 2001, to freeze financial assets of Taliban-related authorities designated by the UN Security Council. The government then revised the regulations, agreeing to list immediately all U.S. Government-requested terrorist designations under U.S. Executive Order 13224 of December 12, 2002. Due in part to Korea's remaining restrictive foreign exchange laws, which persist despite some recent liberalization, and which render the country unattractive as an offshore financing center, no listed terrorists are known to be maintaining financial accounts in Korea at this time. Korean banks have not identified any terrorist assets. There have been no cases of terrorism financing identified since January 1, 2002.

ROK authorities are just beginning to assess whether the hawala system is an area of concern. Currently, gamblers who bet abroad often use alternative remittance and payment systems; however, government authorities have already criminalized those activities through the Foreign Exchange Regulation Act and other laws. Hawala-type vendors do exist in South Korea and operate primarily among the country's small population of approximately 30,000 foreigners from the Middle East.

The ROK actively cooperates with the United States and other countries to trace and seize assets. The Anti-Public Corruption Forfeiture Act of 1994 provides for the forfeiture of the proceeds of assets derived from corruption. In November 2001, 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 \$9.5 million worth of drug-related assets in the first 10 months of 2004, compared to a similar amount over the same period in 2003. The ROKG established six additional new bank account tracking teams in 2004 to serve out of the District Prosecutor's offices in the metropolitan cities of Busan, Daegu, Kwangju, Incheon, Daejeon, and Ulsan, to expand its reach. Its legal framework does not allow civil forfeiture.

The ROK continues to address the problem of the transportation of counterfeit international currency. The National Intelligence Service's (NIS) International Crime Center indicated on November 24, 2004, that there were 141 reported cases of counterfeit dollars worth \$66,525 in the first nine months of 2004. This represented the same number of cases noted in the same period of 2003, but the dollar amount increased by some 47 percent compared with a year earlier. Based on the amount of counterfeit currency actually uncovered, the NIS estimated that \$500,000 to one million dollars of fake currency may be in circulation in South Korea.

South Korea has a number of thriving free trade zones (FTZs) that enjoy certain special privileges. However, companies operating within them are subject to the same general laws on financial transactions as companies operating elsewhere, and there is no indication these FTZs are being used in trade-based money laundering schemes or for terrorist financing. The ROK mandates extensive entrance screening to determine companies' eligibility to participate in FTZ areas, and firms are subject to standard disclosure rules and criminal laws. As of November, 2004, the ROK had seven FTZs, as a result of the June, 2004 recategorization of the three port cities of Busan, Incheon, and Kwangyang as FTZs. They were recategorized from their previous designation of "customs-free areas" in order to avoid confusion from the earlier dual system of production-focused FTZs, and logistics-oriented "customs-free zones." Incheon International Airport is slated to become the eighth FTZ. In

2004, the Ministry of Commerce, Industry, and Energy expects the addition of the three new FTZs to boost 2004 exports through the FTZs to over \$12 billion, and expects imports into the FTZs to reach \$10 billion by 2008.

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. In October 2001, the ROK signed the UN International Convention for Suppression of the Financing of Terrorism, and it ratified the convention on February 17, 2004. The ROK also signed in December 2003, but has not ratified, the UN Convention against Corruption. The ROK is an active member of the Asia/Pacific Group on Money Laundering (APG), and in 2004 hosted the APG annual meeting.. The ROK also 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 addition, the FIU continues to actively pursue information-sharing agreements with a number of countries. KoFIU signed memoranda of understanding with Belgium (March 2002), Poland (October 2002), the United Kingdom (October 2002), Brazil (February 2003), Australia (May 2003), Indonesia (October 2003), Colombia and Venezuela (November 2003), Japan (December 2003), Finland (January 2004), Canada (June 2004) and the United States (November 2004) to facilitate the exchange of information on money laundering. These agreements are expected to enhance the government's asset tracing and seizure abilities.

The Government of the Republic of Korea should criminalize the financing and support of terrorism and should continue to move forward to adopt and implement its pending legislation. The Republic of Korea should extend its anti-money laundering regime to financial intermediaries. The Republic of Korea should continue its policy of active participation in international anti-money laundering efforts, both bilaterally and in multilateral fora. Spurred by enhanced local and international concern, the Republic of Korea law enforcement officials have begun to fully grasp the negative potential impact such activity has on their country, and to take steps to combat its growth. The Republic of Korea should also accede to the UN International Convention for the Suppression of Terrorism.

Kuwait

Kuwait is not a major regional financial sector. It has nine commercial banks, including two Islamic banks, all of which provide traditional banking services comparable to Western-style commercial banks. Kuwait also has two specialized banks, the Kuwait Real Estate Bank, which is in the process of converting to an Islamic bank, and the government-owned Industrial Bank of Kuwait. Both of these banks provide medium and long-term financing. Regulators do not believe that money laundering is a significant problem, and most money laundering operations are generated as a byproduct of local drug and alcohol smuggling into the country.

On March 10, 2002, the Emir (Head of State) of Kuwait 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, and that banks must require proper identification of regular and occasional clients. The law also requires banks to keep all records of transactions and customer identification information for a minimum of five years, conduct training and establish internal control systems, and report any suspicious transactions.

Law No. 35/2002 designates the Office of Public Prosecution (OPP) as the sole authority to receive reports and take appropriate action on money laundering operations. Reports of suspicious transactions are then referred from the OPP to the Central Bank of Kuwait (CBK) for analysis. 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. Moreover, banks and financial institutions may face a steep fine

Money Laundering and Financial Crimes

(approximately \$3.3 million) if found in violation of the law. Law 35/2002 does not cite terrorist financing as a crime; however, the definition of criminal activity is broad.

The law includes articles on international cooperation, and on monitoring cash and precious metals transactions. Currency smuggling into Kuwait is also outlawed under Law No. 35/2002, although reporting requirements are not enforced at ports of entry. Provisions of Article 4 of Law No. 35/2002 state that every person shall, upon entering the country, inform the customs 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). However, the law does not require individuals to file customs declarations when carrying cash or precious metals out of Kuwait. The law authorizes the Minister of Finance to set forth the resolutions necessary to ensure its implementation. The Minister of Finance, as stipulated by Law No. 35/2002, can issue resolutions to enhance combating money laundering operations, without actually amending the legislation. Several cases have been opened under Law No. 35/2002, but the majority of them were closed after investigations did not disclose prosecutable offenses. Only two cases have gone to courts. The cases reportedly involve money smuggling and failure to report currency transactions, and do not involve banks.

In addition to Law No. 35/2002, anti-money laundering reporting requirements and other rules are contained in the CBK's instructions No. (2/sb/92/2002), which took effect on December 1, 2002, superseding instructions No. (2/sb/50/97). The revised instructions provide for, inter alia, customer identification and the prohibition of anonymous or fictitious accounts (Articles 1-5); the requirement to keep records of all banking transactions for five years (Article 7); electronic transactions (Article 8); the requirement to investigate transactions that are unusually large or have no apparent economic or lawful purpose (Article 10); the requirement to establish internal controls and policies to combat money laundering and terrorism finance, including the establishment of internal units to oversee compliance with relevant regulations (Article 14 and 15); and, the requirement to report to the CBK all cash transactions in excess of \$10,000 (Article 20). In addition, the CBK distributed detailed instructions and guidelines to help bank employees identify suspicious transactions. The CBK is currently working on updating its anti-money laundering instructions to accommodate new international standards.

Kuwait has two Islamic banks, Kuwait Finance House (KFH) and Bubiyan Islamic Bank, which are both licensed and supervised by the CBK. As of May 31, 2004, KFH came fully under the supervision of CBK, and has been cooperative with its offices, as have all other Islamic investment companies. The Bubiyan Islamic Bank was established by the Kuwaiti Investment authority (KIA) and is in the process of being formed, after its May 2004 initial public offering. The Kuwait Real Estate Bank, which has been one of Kuwait's two "specialized banks," is in the process of converting to an Islamic bank. The CBK has been working on bringing Islamic financial institutions under its supervision since before the terrorist attacks of September 11, 2001.

In addition, CBK issued circular No. (2/sb/95/2003) in 2003, which is directed toward money changing companies, and which contains similar instructions with respect to combating money laundering and suspicious activities reporting guidelines. A similar order (31/2003) was issued by the Kuwait Stock Market to all companies under its jurisdiction. There are about 130 money exchange businesses (MEBs) operating in Kuwait, none of which are companies, and therefore, are not under the supervision of the CBK but rather under the Ministry of Commerce and Industry. The CBK has reached an agreement with the Ministry of Commerce and Industry to enforce all anti-money laundering (AML) laws and regulations in supervising such businesses. Furthermore, the Ministry will work diligently to encourage the MEBs to apply for and obtain company licenses and register with the CBK.

The Ministry of Commerce and Industry supervises insurance companies, exchange bureaus, gold and precious metals shops, brokers in the Kuwait Stock Exchange, and all other financial brokers. Since

September 2002, these firms must abide by all regulations concerning customer identification, record keeping of all transactions for five years, establishment of internal control systems, and the reporting of suspicious transactions.

In April 2004, the Ministry of Finance issued Ministerial Decision No. 11 (MD No. 11/224), which transferred the chairmanship of the National Committee for Anti-Money Laundering and the Combating of the Financing of Terrorism, formerly headed by the Minister of Finance, to the Governor of the CBK. The Committee is comprised of representatives of the Ministries of Interior, Foreign Affairs, Commerce and Industry, and Finance; Office of Public Prosecution; Kuwait Stock Exchange; General Customs Authority; and the Union of Kuwaiti Banks. The decree expanded the membership of the Committee to include the Ministry of Labor and Social Affairs in an apparent move to oversee charities and non-governmental organizations.

According to the MD 11/2004, the Committee shall be entrusted, *inter alia*, with drawing up the country's strategy and policy with regard to anti-money laundering and terrorist financing; drafting the necessary legislation, along with pertinent regulations; coordinating between the concerned ministries and agencies in matters related to combating money laundering and terrorist financing; following up on domestic, regional, and international developments, and making needed recommendations in this regard; setting up appropriate channels of communication with regional and international institutions and organizations; and representing Kuwait in domestic, regional, and international meetings and conferences. In addition, Article Seven entrusts the Chairman of the Committee with issuing regulations and procedures that he deems appropriate for the Committee duties and responsibilities and the organization of its activities.

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. However, there is no indication that such activities occurred with the knowledge of the Kuwaiti head office, which remains undesignated; U.S. authorities have only designated the branches in Pakistan and Afghanistan as having been used to funnel funds to terrorist organizations. The RIHS is under the supervision of the Ministry of Labor and Social Affairs, which has become the newest member of the National Committee for Anti-Money Laundering and the Combating of the Financing of Terrorism.

In August 2002, the Kuwaiti Ministry of Social Affairs and Labor issued a ministerial decree creating the 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 has established guidelines to charities explaining donation collection procedures and regulating financial activities. The new Department is also charged with conducting periodic inspections to insure that they maintain administrative, accounting, and organizational standards according to Kuwaiti law. Further, the Department mandates the certification of charities' financial activities by external auditors. Banks may not transfer any money outside of Kuwait without prior permission from the Ministry. In addition, such wire transactions must be reported to the CBK.

On June 23, 2003, the CBK issued Resolution No. 1/191/2003, establishing the Kuwaiti Financial Inquiries Unit (KFIU) as an independent entity within the Central Bank. The goals of KFIU, which acts as a Financial Intelligence Unit (FIU), are to receive and analyze reports of suspected money laundering from the Office of Public Prosecution (OPP), to establish a database of suspicious transactions, to conduct anti-money laundering training, and to carry out domestic and international exchanges of information in cooperation with the OPP. Law No. 35/2002 did not establish the FIU as the central unit for the receipt, analysis, and dissemination of the suspicious transaction reports (STR) information; instead, these critical functions were divided. Now, STRs are received in the CBK, while

the Public Prosecutor has the authority to disseminate STRs and assess international requests for information. Kuwaiti officials agree that the current limits on information sharing by the FIU are a problem that requires amending of the law.

Kuwait is a member of the Gulf Cooperation Council (GCC), which is itself a member of the Financial Action Task Force (FATF). In November 2004, Kuwait signed the memorandum of understanding governing the establishment of the Middle East and North Africa Financial Action Task Force (MENAFATF). Kuwait is one of the fourteen charter members of this FATF-style regional body that was inaugurated in Bahrain to promote best practices to combat money laundering and terrorist financing in the region.

Kuwait has signed the 1988 UN Drug Convention. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. It has not yet signed the UN International Convention for the Suppression of the Financing of Terrorism.

Kuwait is making progress in enforcing its anti-money laundering program. The issuance of the Ministry of Finance Decree 11/2004 concerning the new duties of the National Committee for Anti-Money Laundering and the Combating of the Financing of Terrorism represents a significant improvement. Kuwaiti officials acknowledge the need for extensive training for all involved sectors.

The Government of Kuwait should take steps to strengthen its anti-money laundering law, improve the sharing of financial information, and criminalize terrorist financing. Kuwait should also make outbound currency and precious metals declarations mandatory. More interagency cooperation and coordination between the Kuwaiti Financial Inquiries Unit and other concerned parties could yield significant improvements in proactive investigations and international information exchange. The Kuwaiti Financial Inquiries Unit should be able to independently share financial information with its foreign counterparts, and receive, analyze, and disseminate suspicious transaction reports without obtaining prior authorization from the Office of the Public Prosecutor. Kuwait should 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.

Kyrgyz Republic

The Kyrgyz Republic is not a regional financial center. Money laundering is still not classified as a crime under present Kyrgyz legislation. The Kyrgyz banking system remains comparatively underdeveloped. Like other countries in this region, the Kyrgyz Republic's alternative remittance systems are susceptible to money laundering activity or trade-based fraud. The smuggling of consumer goods, tax and tariff evasion, official corruption and narcotics-trafficking continue as the major sources of illegal proceeds within the Kyrgyz Republic.

In 2004 the Kyrgyz legislature drafted a fairly comprehensive law on "Combating Terrorism and Illicit Money Laundering". On December 9, 2004, the bill passed its first reading in the Parliament. It will need to pass an additional reading before being sent to the President for signature. The proposed law defines predicate offenses and criminalizes income obtained as a result of a criminal action. It also includes the mandatory reporting of suspicious transactions by all Kyrgyz financial institutions. Because of Parliamentary elections scheduled for late February, it is expected that the second reading will not take place until the second quarter of 2005. At present, the Kyrgyz Republic has no other laws or draft laws on money laundering.

The National Bank has provisions that require customer identification procedures and make an exception to bank privacy rules for suspicious transaction reporting, but these provisions are reported to be mostly ignored by the commercial banks. Currently, several National Bank restrictions prohibiting banking operations with certain offshore financial institutions and a number of identified suspicious organizations serve to regulate the anti-money laundering process. Oversight of the banking

sector, however, remains generally weak, and Kyrgyz law enforcement agencies lack the expertise and resources necessary to effectively monitor and investigate financial irregularities.

On October 6, 2004 the Kyrgyz Republic, along with Russia, China, Belarus, Tajikistan, and Kazakhstan, formed the Eurasian Group for Counteraction to the Legalization of Illegal Incomes and Terrorism Financing. The Kyrgyz Republic is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism. The Kyrgyz Republic has signed, but not yet ratified, the UN Convention against Corruption.

The Kyrgyz Government has agreed to participate in a United States-sponsored "Needs Assessment" on money laundering and financial investigations scheduled for February 2005. This review is designed to identify the vulnerabilities or deficiencies in legislation to combat money laundering and financial crimes. It will also identify training needs for all Kyrgyz law enforcement agencies responsible for investigations of these crimes.

The Government of the Kyrgyz Republic should adopt the legislation necessary to implement a comprehensive anti-money laundering regime capable of thwarting terrorist financing and should provide the necessary resources to implement such a program. The Kyrgyz Government should also remain vigilant in its efforts to combat money laundering activities that circumvent the financial institutions.

Laos

Laos, a major drug-producing and transit country, is on the fringe of the region's banking network. Its banking sector is dominated by state-owned commercial banks in need of extensive reform. The small scale and poor financial condition of Lao banks may make them more likely to be venues for certain kinds of illicit transactions. However, Lao banks are not optimal for moving large amounts of money in any single transaction, due to the visibility of such movements in a small, low-tech environment. What money laundering does take place through Lao banks is likely to have been from illegal timber sales or domestic criminal activity, including drug trafficking. In a recent high-profile case involving a foreign-owned company accused of securities fraud, Lao customs authorities seized \$300,000 in cash a businessman was transporting to Thailand, in contravention of Lao law. Subsequent investigation indicated that this business had transferred several million dollars from abroad through the Lao banking system in the past year, much of which was reportedly withdrawn in cash. The case revealed the weakness of the Lao banking system in monitoring suspicious transactions.

Laos has drafted a money laundering law with counterterrorism finance components, based upon a model law provided by the Asian Development Bank. The legislation was proposed during the second half of 2004 and has passed through the Ministry of Justice. It awaits prime ministerial approval and is expected to be passed by the National Assembly in April 2005, perhaps with changes. The law will criminalize money laundering and terrorist financing. A Financial Intelligence Unit (FIU) will also be established, to supplant the small and informal one currently in place. Reportedly, a provision will be made for the freezing of suspect transactions and forfeiture of laundering proceeds. The Bank of Laos currently has a very small Banking Supervision Department, and it is thought that the Department will be augmented and used to help implement the new legislation. Provision will be made for mutual assistance in criminal matters between Laos and other countries.

Lao law prohibits the export of the national currency, the Kip. It is likely that the currency restrictions and undeveloped banking sector encourage the use of alternative remittance systems.

The GOL is a party to the 1971 UN Convention on Psychotropic Substances and the 1988 UN Drug Convention. GOL sends its officials to relevant Association of Southeast Asian Nations (ASEAN)

regional conferences on money laundering. Laos also has observer status in the Asia Pacific Anti-Money Laundering Group, and plans to join fully once its anti-money laundering law is enacted.

The Government of Laos should pass anti-money laundering and counterterrorism financing legislation. Laos should also become a party to the UN International Convention for the Suppression of Financing of Terrorism and the UN Convention against Transnational Organized Crime.

Latvia

Latvia's role as a regional financial center, its large number of commercial banks, and those banks' sizeable non-resident deposit base continue to pose significant money laundering risks in Latvia, even as Latvian financial institutions, regulators, and law enforcement and judicial authorities seek tighter adherence to legislative norms, regulations, and "best practices" designed to fight financial crime. Sources of laundered money include counterfeiting, corruption, white-collar crime, extortion, financial/banking crimes, stolen cars, contraband smuggling, and prostitution. Organized crime is thought to account for a significant portion of laundered proceeds. Latvian consumers are increasingly comfortable with the use of electronic, credit, and other non-cash payments. At the same time, there are no restrictions in Latvia on cross-border currency movement (cash or non-cash, domestic or foreign) or the physical movement of other financial instruments. However, in November 2004, a package of drafted acts was finalized, in anticipation of a forthcoming European Union (EU) Directive, to enact cash declaration requirements (over 15,000 euros) on the external borders of the EU. This will affect Latvia's border crossings with Russia and Belarus, and passengers traveling to Latvia by air from non-EU countries. The proposal will be sent to the Latvian Parliament for review in 2005. Latvia's accession to the European Union occurred on May 1, 2004.

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 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 Law on the Prevention of Laundering of Proceeds Derived from Criminal Activity (the anti-money laundering law (AML)) requires all institutions engaging in transactions to report suspicious activity. On February 1, 2004, the amendments to meet the requirements of the Second EU Directive of 2001 became effective. Amendments to the AML law expand the scope of reporting institutions, and include auditors, lawyers, and high-value dealers, as well as credit institutions.

The law lists four categories of entities obligated to report suspicious activities: participants in financial and capital markets (credit institutions, insurance companies, private pension funds, stock exchanges, brokerage companies, investment companies, credit unions, and investment consultants); organizers and holders of lotteries and gambling enterprises; companies engaged in foreign currency exchange; and individuals and companies who perform professional activities and services associated with financial transactions (money transfer services, tax consultants, auditors, auditing companies, notaries, attorneys, real estate companies, art dealers, and commodities traders).

Another amendment to the AML law recognizes all offenses listed in the criminal law, including terrorism, as predicate offenses for money laundering. The amendments also provide the FIU with authority to stop transactions for up to 45 days. The supervisory and control authorities have begun to amend their guidelines for the additional institutions the amendments have brought under their supervision.

The AML law requires all institutions engaging in transactions to report suspicious activity. Individual banks and other financial institutions have discretion in establishing internal protocols for identifying suspicious transactions. The law also mandates institutions to report unusual transactions, based on a

list of indicators that the GOL established in 2001 as part of its AML regime. According to the list of unusual indicators, Latvian banks are mandated to report cash transactions in excess of 40,000 lats (approximately \$80,000). Additionally, banks are required to record the identity of any customer engaging in a transaction exceeding 15,000 euros. There are no bank secrecy laws that prevent law enforcement agencies from identifying account holders during criminal investigations. Financial and credit institutions submit suspicious transaction reports (STRs) and unusual activity reports to the Control Service.

The Control Service operates under the oversight of the Prosecutor General's Office. Approximately 40 percent of all reports filed with the Control Service are STRs; the other 60 percent consist of unusual currency transaction reports. The Control Service received 7,902 reports in 2002, 15,371 reports in 2003, and 16,128 in 2004. The growth in the number of reports for the year 2003 is due to the more pro-active efforts on the part of most banks to report unusual activity above the mandatory threshold requirements, and the additional research conducted by the financial institutions to trace the funds. In 2003, nine new criminal cases were opened and nine additional cases were updated with information provided by the FIU. In 2004, ten new criminal cases were opened and six additional cases were updated with information provided by the FIU.

Prior to Latvia's accession into the European Union, the EU's 2001 Report on Latvia's Progress characterized the perceived level of corruption in Latvia as relatively high. Latvia continues to take steps to combat both real and perceived corruption. In 2002, the Parliament adopted the Law on Prevention of Conflict of Interest of Public Officials.

In January 2002, the government formally established the Anti-Corruption Bureau (ACB), an independent agency whose specific charter is to prevent and combat corruption. The ACB started operating in February 2003. In 2004 the ACB reviewed 734 Latvian officials' asset declarations and sanctioned 63 officials for violations. In addition, in 2004, the number of cases the ACB forwarded to the prosecutor's office for criminal prosecution nearly doubled to 35. The ACB and the Control Service, cooperate on cases of suspected public corruption. In 2004, the Ministry of Justice prepared draft amendments on corruption concerning the coercive measures and criminal liability of legal entities, to be presented to Parliament in 2005.

Since July 2001, the Finance and Capital Market Commission (FCMC) has served as the GOL's unified public financial services regulator, overseeing commercial banks and non-bank financial institutions, the Latvian Stock Exchange, and insurance companies. The Bank of Latvia supervises the currency exchange sector. The FCMC conducts regular audits of credit institutions and will apply sanctions to companies that fail to file mandatory reports of unusual transactions. The Control Service also checks to insure that it receives matching STRs on transactions that occur between Latvian banks. The FCMC has approved guidelines for identifying customers and unusual and suspicious transactions, as well as guidance on the internal control mechanisms that financial institutions should have in place. While the FCMC has pressed financial institutions to pay closer attention to suspicious transactions, particularly those involving jurisdictions on the Financial Action Task Force (FATF)-designated list of Non-Cooperative Countries and Territories (NCCTs), the FCMC is limited in its regulatory powers to take strong public action against offending banks.

In 2004, the FCMC conducted 35 on-site inspections of 19 banks where it assessed the banks' internal controls for preventing money laundering. In one instance, the FCMC fined the bank for non-compliance with AML guidelines. The FCMC placed five additional banks under an enhanced supervisory regime. These banks must address, within a prescribed time period, any non-compliance with legal and FCMC guidelines on preventing money laundering, or face sanctions. By December 2004, 13 Latvian banks were still under enhanced FCMC supervision. The FCMC notified two of these banks that board members responsible for preventing money laundering faced removal. An additional two banks face the removal of all of their board members. The FCMC warned one bank

during 2004 that it would revoke the bank's license if it failed to comply with FCMC recommendations by the imposed deadline.

The FCMC conducted 13 inspections of seven insurance companies during 2004. It fined two companies for failure to comply with requirements stemming from the "Law on the Prevention of Laundering of Proceeds Derived from Criminal Activity." The FCMC removed the managements of four insurance companies in 2003 and 2004 due to reinsurance operations that likely involved tax evasion and/or money laundering.

Financial institutions have the ability to freeze accounts for an unlimited amount of time. If a financial institution finds the activity of an account questionable, it may close the account on its own initiative. If the institution considers the activity unusual but not suspicious, there is no obligation to file a suspicious transaction report with the Control Service. Latvia still lacks clear legal authority for asset seizures and forfeitures associated with financial crimes. The law enforcement authorities under the Ministry of Interior have proposed a program for combating organized crime, which is under consideration by the government. The program recommends creating a unit under the State Police that would be in charge of addressing issues and legislation concerning the confiscation of proceeds derived from criminal activity issues.

Latvia continues to address the issue of offshore investments. Information on offshore company owners had been confidential, but a law enacted in January 2002 requires more information on the branches of offshore companies in Latvia. The law requires that at least half the board members of such companies 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.

In 2004, the FCMC notified all Latvian banks that they were to cease and desist from advertising their services on websites that publicize offshore financial services. Non-residents represent approximately half of Latvian banks' account holders. Latvian law mandates that banks must collect information on the identity of all account holders, and FCMC regulations require that AML officers must approve new accounts. However, ongoing law enforcement investigations suggest that beneficial account holders sometimes use false identities to open accounts at Latvian banks.

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 evidence-gathering processes need streamlining. There are three specialized units, one at the Financial Police (Latvian Finance Ministry), one at the Economic Police (Latvian Interior Ministry), and one at the Office to Combat Organized Crime, which are responsible for money laundering investigations, and one unit at the Prosecutor's Office which specializes in bringing charges against suspected individuals. To date, there have been no forfeitures of illicit proceeds based on money laundering. In 2004, the Prosecutor's Office tried two money laundering cases that resulted in acquittals; one of those cases is on appeal by the prosecution.

The GOL has initiated a number of measures aimed at combating the financing of terrorism, and became a party to the UN International Convention for the Suppression of the Financing of Terrorism on November 14, 2002. Latvia is also a party to 11 other international conventions designed to prevent arms trafficking, terrorism on public transportation, and hostage taking. The GOL has implemented regulations to apply sanctions imposed by UNSCR 1267 and 1333 under Cabinet of Ministers' Regulation No. 437 "On the Sanction Regime of the United Nations Security Council against the Afghan Islam Emirates in the Republic of Latvia." On October 14, 2004, Regulation No. 840 "On the Countries and International Organizations Whose Lists Include Persons Suspected of Committing Acts of Terrorism or Complicity Therein" entered into force, replacing Regulation 387 of July 2003. In accordance with Regulation No. 840, the FIU electronically provides credit and financial institutions and their supervisory and control authorities with consolidated terrorist lists. The Regulation allows

the FIU to order a credit or financial institution to freeze suspected terrorist funds. Latvia also has a mechanism for freezing financial resources or other property not involving terrorism.

The Law on Credit Institutions enables police to obtain information from credit institutions in cases of suspected terrorism during the operative stage, prior to the initiation of a criminal case. In October 2004, the FCMC updated its guidelines for financial and credit institutions' internal controls to prevent money laundering and terrorist financing. These updated guidelines incorporate all of the FATF recommendations.

In November 2004, the Prime Minister's Crime Prevention Council approved a new national action plan outlining a strategy to target money laundering, based on the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) recommendations. The Cabinet has not yet formally adopted the new measures, but individual ministries affected by the plan have begun to implement the new procedures.

Amendments to the AML law 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 counterterrorism 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, and have invested considerable effort in tracing transactions executed by terrorists or their accomplices. Other practical measures include organizing relevant training courses for personnel in financial institutions, creating a special counterterrorism information network within the financial system, nominating a person to deal with counterterrorism issues at the FIU, and establishing an FIU reporting system and procedures concerning terrorist finances.

Latvia has a growing legal gambling industry. Through September 2004, the gaming industry accounted for 51,000,000 lats (approximately \$100,000,000) of revenue, compared to 36,500,000 lats (approximately \$71,568,000) during the first nine months of 2003. In 2004, Latvia enacted a new law that restricts slot machines to defined gaming halls (places that have greater than ten gaming machines). Bars and cafes with slot machines that have been in operation prior to June 2002 are permitted to maintain their gaming operations provided they have no more than five slot machines. This rule change caused the number of gambling places to drop from 1,487 to 688 during 2004. The number of gaming halls increased from 508 in 2003 to 638 in 2004. As of December 2004, there were 12,125 gaming machines in Latvia, compared to 10,597 in 2003. The number of casinos dropped from 20 in 2003 to 15 in 2004.

The Ministry of Finance's Department of Lotteries and Gambling Supervisory Inspection regulates the gaming industry in Latvia. There are ten casino inspectors who preside over daily cash-out operations at each of the country's casinos. There are seven slot machine inspectors. All casino customers must register and show proof of identification prior to entering the casino premises. Casinos and gaming halls must provide information about winnings of greater than 5,000 lats (approximately \$10,000) to the Ministry of Finance and the FIU. In January 2004, the GOL mandated new bookkeeping procedures for casinos that allow for easier supervision and regulation. The Ministry of Finance has statutory authority to inquire about all casino owners and officers, and works with the FIU to review licensing applications.

There are four special economic zones in Latvia that provide a variety of significant tax incentives for manufacturing outsourcing, logistics centers, and trans-shipment of goods to other free trade zones. These zones are located at the free ports of Ventspils, Riga, and Liepaja, and in the inland city of Rezekne near the Russian and Belarusian Borders. There have been instances of smuggling involving cigarettes and meat products related to warehouses located in the free trade zone.

Latvia participates in MONEYVAL, and, as a member, underwent a mutual evaluation in March 2000 that resulted in many of the changes to its AML law and procedures. Latvia's second round of evaluations was completed in 2002, and the results were discussed during the MONEYVAL committee in May 2004. Latvia is now working to implement these measures as part of a National AML Action Plan.

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 1988 UN Drug Convention, and in December 2001, ratified the UN Convention against Transnational Organized Crime.

The Control Service, Latvia's FIU, has been a member of the Egmont Group since 1999 and has cooperation agreements on information exchange with FIUs in Belgium, Bulgaria, Canada, the Czech Republic, Estonia, Finland, Guernsey, Italy, Lithuania, Malta, Russia, Slovenia, and Poland. In addition, Latvia has signed multilateral agreements with 10 accession countries for automatically exchanging information between the EU financial intelligence units using FIU.NET.

The GOL should continue to explore ways to improve cooperation between Latvian law enforcement agencies at the working level, and to strengthen its capacity and record in aggressively prosecuting and convicting those involved in financial crimes. The Financial and Capital Markets Commission must take tough, public action against those banks that have consistently shown themselves unable or unwilling to apply proper AML procedures. 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, pass asset seizure and forfeiture legislation, and more aggressively regulate its bureaux de change and its gaming industry. Although the GOL believes its existing laws are adequate to prosecute terrorist financing cases, this belief has not been tested. The GOL should therefore specifically criminalize terrorist financing to ensure that adequate legal tools are in place to successfully prosecute such offenses.

Lebanon

Lebanon is a financial hub for banking activities in the Middle East. It has one of the more sophisticated banking sectors in the region. The banking sector continues to record an increase in deposits. As of September 2004, 63 banks (53 commercial banks and ten investment banks) operated in Lebanon, with total deposits of \$53.5 billion. Three U.S. banks' also have representative offices operating in Lebanon: American Express Bank, the Bank of New York, and JP Morgan Chase Bank. The Central Bank (Banque du Liban) (CBL) regulates all financial institutions and money exchange houses. Banking sources emphasize that Lebanon is not a significant financial center for money laundering; however, Lebanon's free market economy, combined with the tradition of bank secrecy and the extensive use of foreign currency (particularly dollars), allows for an environment conducive to laundering money from illicit sources due to a general lack of accountability and enforcement. The narcotics trade is not a principal source of proceeds in money laundering. Lebanon imposes no controls on the movement of capital. It has a substantial influx of remittances from expatriate workers and family members.

Lebanon has continued to make progress toward developing an effective money laundering and terrorism finance regime incorporating the Financial Action Task Force (FATF) Forty Recommendations, which culminated in the FATF's removal of Lebanon from the list of Non-Cooperative Countries or Territories (NCCTs) in June 2002. With Lebanon's removal from the NCCT list, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) lifted its advisory, which had instructed all U.S. financial institutions to "give enhanced scrutiny" to all transactions involving Lebanon. In October 2003, the FATF ended the monitoring period to which Lebanon had been subjected since June 2002.

In 2004, Lebanon passed a law requiring diamond traders to seek proper certification of origin for imported diamonds; the Ministry of Economy and Trade would be in charge of issuing certification for re-exported diamonds. This law, designed to prevent the traffic in conflict diamonds, will allow Lebanon to join the Kimberly Process, a voluntary joint government, international diamond industry, and civil society initiative to stem the flow of rough diamonds—that are used by rebel and terrorist movements to finance their operations—through imposing extensive requirements on participants to certify the legitimate origin of rough diamonds. In August 2003, Lebanon passed a decree prohibiting imports of rough diamonds from countries that are not members of the Kimberly Process.

In April 2001, Lebanon adopted Law No. 318, which created a framework for lifting bank secrecy, broadening the criminalization of money laundering beyond drugs, mandating suspicious transaction reporting, requiring financial institutions to obtain customer identification information, and facilitating access to banking information and records by judicial authorities. Under this law, money laundering is a criminal offense and punishable by imprisonment for a period of three to seven years and by a fine of no less than twenty million Lebanese pounds (\$13,267). The provisions of Law No. 318 expand the type of financial institutions subject to the provisions of the Banking Secrecy Law of 1956, to include institutions such as exchange offices, financial intermediation companies, leasing companies, mutual funds, insurance companies, companies promoting and selling real estate and construction, and dealers in high-value commodities. In addition, Law No. 318 requires companies engaged in transactions for high-value items (precious metals, antiquities) and real estate to report suspicious transactions.

These companies are also required to ascertain, through official documents, the identity and address of each client, and must keep photocopies of these documents as well as photocopies of the operation-related documents for a period of no less than five years. The CBL regulates private couriers who transport currency. Western Union and Money Gram are licensed by the CBL and subject to the provisions of this law. Charitable and nonprofit 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 CBL. Law 318 (2001) clarified the CBL's powers to require financial institutions to identify all clients, including transient clients, maintain records of customer identification information, request information about the beneficial owners of accounts, conduct internal audits, and exercise due diligence in conducting transactions for clients.

Law No. 318 also established a Financial Intelligence Unit (FIU), called the Special Investigation Commission (SIC), which is an independent entity with judicial status that can investigate money laundering operations and monitor compliance of banks and other financial institutions with the provisions of Law No. 318. The SIC serves as the key element of Lebanon's anti-money laundering regime and has been the critical driving force behind the implementation process. The SIC is responsible for receiving and investigating reports of suspicious transactions. The SIC is the only entity with the authority to lift bank secrecy for administrative and judicial agencies, and it is the administrative body through which foreign requests for assistance are processed. The SIC circulates to all financial institutions the list of individuals and entities that have been included on the UNSCR

1267 Sanctions Committee's consolidated list. The SIC also circulates the list of individuals and entities that the U.S. Government and the European Union have designated under their relevant authorities. The SIC has signed a number of memoranda of understanding with other FIUs concerning international cooperation in anti-money laundering and combating terrorist financing. The SIC cooperates with competent U.S. authorities on exchanging records and information within the framework of Law 318.

During 2003, Lebanon adopted additional measures to strengthen efforts to combat money laundering and terrorism financing, such as establishing anti-money laundering units in customs and the police. In July 2003, Lebanon joined the Egmont Group of financial intelligence units. SIC reported increased inter-agency cooperation with other Lebanese law enforcement units such as Customs and the police. The cooperation led to an increase in the number of reported suspicious transactions reports (STRs), and as a result SIC initiated several investigations in 2004. Article 12 of Law 318 provides for immunity from prosecution for the chairman, staff, and delegates of the SIC, as well as for the financial institutions' money laundering reporting officers.

Since its inception, the SIC has been active in providing support to international case referrals. From January through November 2004, the SIC investigated over 176 cases involving allegations of money laundering and terrorist financing activities. Out of these cases, 13 were originated from U.S. Government (USG) requests. Seventeen of these cases were related to terrorist financing. Bank secrecy regulations were lifted in 68 instances, and three cases relating to money laundering were transmitted by the SIC to the State Prosecutor General to determine if these cases would be referred to the criminal court for trial. The Prosecutor General reported four cases to the SIC to freeze the suspects' assets. These cases involve 24 persons, 19 convicted in drug cases, four in currency counterfeiting, and one in theft. The Prosecutor General has also referred to the criminal court three cases involving four persons, two on drug-related charges and two on embezzlement charges, as well as a family of four persons facing terrorism charges based on a USG list of designated individuals. Total dollar amounts frozen by the SIC in all these cases is about U.S. \$3.2 million.

In October 2003, in order to more effectively combat money laundering and terrorist financing, Lebanon adopted two laws, Numbers 547 and 553. Law 547 expanded Article One of Law 318 (2001), criminalizing any funds resulting from the financing or contribution to the financing of terrorism or terrorist acts or organizations, based on the definition of terrorism as it appears in the Lebanese penal code (which distinguishes between "terrorism" and "resistance"). Law 547 also criminalized acts of theft or embezzlement of public or private funds, or their appropriation by fraudulent means, counterfeiting, or breach of trust, for banks and financial institutions, or falling within the scope of their activities. It also criminalized counterfeiting of money, credit cards, debit cards, and charge cards, or any official document or commercial paper, including checks. Law 553 added an article to the penal code (Article 316) on terrorist financing, which stipulates that any person who voluntarily, either directly or indirectly, finances or contributes to terrorist organizations or terrorists acts is punishable by imprisonment with hard labor for a period not less than three years and not more than seven years, as well as a fine not less than the amount contributed but not exceeding three times that amount.

Offshore banking is not permitted. Lebanon has no offshore trusts or offshore insurance companies. Legislative Decree No. 46, dated June 1983, governs offshore companies. It restricts offshore companies' activity to negotiating and signing agreements concerning business carried outside Lebanon or in the Lebanese Customs Free Zone; thus, offshore companies are barred from engaging in activities such as industry, banking, and insurance. All offshore companies must register with the Beirut Commercial Registry, and the owners of an offshore company must submit a copy of their identification. Moreover, the Registrar of the Beirut Court keeps a special register, in which all documents and information issued by the offshore company are to be retained.

There are currently two free trade zones operating in Lebanon, at the Port of Beirut and at the Port of Tripoli. The free trade zones fall under the supervision of Customs. Exporters moving goods into and out of the free zones submit a detailed manifest to Customs. If Customs suspects a transaction to be related to money laundering or terrorism finance, it will report it to the SIC. Lebanon has no cross-border currency reporting requirements. However, since January 2003, Customs checks travelers randomly and notifies SIC when large amounts of cash are found.

Lebanese law allows for property forfeiture in civil as well as criminal proceedings. The Government of Lebanon enforces existing drug-related asset seizure and forfeiture laws. Current Lebanese legislation provides for the confiscation of assets the court determines to be related to or proceeding from money laundering or terrorist financing. In addition, vehicles used to transport narcotics will be seized. Legitimate businesses established from illegal proceeds after passage of Law 318 are also subject to seizure.

Lebanon was one of the founding members of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-styled regional body that promotes best practices to combat money laundering and terrorist financing in the region. It was inaugurated on November 30, 2004, in Bahrain, by 14 Arab countries. Lebanon will host the first MENAFATF plenary in the first quarter of 2005. Lebanon's SIC Secretary was elected to a one-year term as the first President of MENAFATF.

Lebanon has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision" and is compliant on 24 out of the 25 "Core Principles." Compliance with the pending "Core Principle" is being addressed, and a draft law providing legal protection to bank supervisors awaits the cabinet's approval. Banks are compliant with the Basel I capital accord and are preparing to comply with Basel II recommendations concerning capital adequacy.

Lebanon is a party to the 1988 UN Drug Convention, although it has expressed reservations to several sections relating to bank secrecy. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. It has not yet signed the UN International Convention for the Suppression of the Financing of Terrorism. Lebanon has expressed reservations on Article 11 of the UN International Convention for the Suppression of Terrorist Acts by Bombs, concerning the "extradition for political crime," claiming that it conflicts with Lebanon's penal code.

The Government of Lebanon continues to improve its efforts to develop an effective anti-money laundering and terrorism finance regime. It should encourage more efficient cooperation between financial investigators and other concerned parties, such as police and customs, which could yield significant improvements in initiating and conducting investigations. It should ratify both the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of Terrorist Financing.

Lesotho

Lesotho is not a financial center and does not have a significant money laundering problem. There is currently no legislation criminalizing money laundering or terrorist financing. In 2003, the Government of Lesotho (GOL) drafted a comprehensive "Money Laundering and Proceeds of Crime" bill; the bill was revised in 2004. As of early 2005, the revised draft bill was being reviewed before presentation to the Cabinet.

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 \$16,000) to the Central Bank. Financial institutions are also required to maintain, for a period of ten years, all necessary records to enable them to comply with information requests from competent authorities.

No cases of money laundering were reported within the past year.

The GOL created a multi-agency committee to assist in its implementation of UNSCR 1373. The Commonwealth Secretariat is assisting members of the committee to formulate national policy and draft legislation on terrorism, and intends to sponsor related training for countries of the region.

Lesotho is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Lesotho is a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. However, it has not yet signed the ESAAMLG Memorandum of Understanding (MOU).

The Government of Lesotho should criminalize money laundering and terrorist financing and should develop a viable anti-money laundering regime. It should sign the MOU for ESAAMLG.

Liberia

Liberia is not a regional financial center. However, Liberia is vulnerable to money laundering because it has been a major transshipment point for illegal diamond smuggling and illegal arms trading. Liberia is also a growing transit country for narcotics on their way to Europe from Nigeria. Liberia is also a fertile haven for drug cultivation, but it appears that most of the locally grown drug crop is used for domestic consumption. Liberian National Police (LNP) routinely stop shipment of marijuana moving from the interior to the Atlantic coast in order to extract bribes from the drivers, but then the shipments are allowed passage. During the Liberian civil war, which was declared officially over on August 11, 2003, Liberia was also a major transshipment point for illegal diamond smuggling, exploitative timber, and illegal arms trading. There were numerous allegations that the profits from these industries were being used to fund local militias and international terrorist activities. The connection to local militias has been documented. The international terrorist nexus may have existed to some degree, but its extent and sustainability is not well known.

There was a major shift in this activity after the end of the Liberian civil war. In September 2003, the UN adopted sanctions on arms, travel, diamonds and timber. With the arrival of UN peacekeepers in 2003, the illicit arms trade has virtually disappeared. UN timber sanctions have limited legal exports, but an illegal timber industry still existed in 2004. UN sanctions on diamonds have limited the ability of smugglers to use Liberia for operations. The National Transitional Government of Liberia (NTGL) has now met the conditions for becoming a participant in the Kimberley Process Certification Scheme, which requires that certain minimum standards be met in order to assure that diamonds being traded are not conflict diamonds and their origin is known. As of the end of 2004, however, the NTGL had yet to begin implementation of the certification scheme. Until that is done, diamond traders, including Eastern Europeans and Lebanese, can travel to Monrovia to purchase rough diamonds on the black market and then smuggle and export them out of Liberia, documenting them as coming from some other source, in violation of a UN Security Council Resolution prohibiting all trade in Liberian rough diamonds. The under valuation of diamond exports and use of double invoicing are common tactics employed to transfer value out of the country, often in conjunction with other illicit activities. There continue to be press allegations that al-Qaida has exploited the West African diamond trade, but such a connection has not been conclusively established. Cash in excess of \$10,000 must be declared to customs officers upon entering the country, and amounts over \$7,500 must be declared on departure. However, these regulations are not regularly enforced, and there is widespread corruption in Liberia's customs administration.

Money laundering is a criminal offense in Liberia, but there are no strong laws to prosecute persons who might be engaged in financing traffickers or terrorist organizations. Businesses may be seized for laundering money, and the government receives the proceeds of such seizures. The banking sector is

thought to be complicit in money laundering, given the unregulated financial environment. There were no arrests and/or prosecutions for money laundering or terrorist financing during 2003 or 2004. Liberia suffers from institutional damage from 14 years of civil war and a weak UN civil police (UNMIL) mandate, which provides no arrest authority for the force. A weak transitional authority comprised of ex-combatant leaders, the NTGL is confronted by a host of problems and lacks the political will and the policing structure to deal with the issue of money laundering. The police force is ineffective, although UNMIL is attempting to restructure and reform the force. Border security is effectively non-existent. The judiciary is notoriously corrupt, and allegations of verdict buying are rampant. This can be considered a primary form of economic crime, as businesses operating in Liberia face the constant threat of state-enabled financial pressure and/or extortion. This corruption does not operate on any organized level and enriches only the officer, judge or minister who manages to extract payment. Given the poorly supervised financial environment, private economic crime is considered to be widespread.

In November 2004, the Central Bank of Liberia (CBL) learned through Interpol of the circulation in Monrovia of counterfeit Liberian \$100 notes. At about the same time, there was an unverified report of counterfeit U.S. dollar notes in small denominations sighted in rural Liberia. The CBL contacted the Interpol West African Representative at Interpol Headquarters in Lyon, France, seeking further details, but no response has been received. One possible solution to this threat would be movement toward dollarization of the Liberian economy, an option promoted by many senior Liberian officials. The Governor of CBL is also considering the printing of newly designed notes as one of the ways to address the counterfeit bills problem.

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 2004, Liberia signed an accord with the U.S. Government giving the U.S. Navy and Coast Guard the right to search Liberian-flag vessels on the high seas.

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. Liberia is not a party to the 1988 UN Drug Convention. In March 2003, Liberia became a party to the UN International Convention for the Suppression of the Financing of Terrorism. In September 2004, Liberia became a party to the UN Convention against Transnational Organized Crime.

The Government of 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, take steps to properly regulate its diamond industry, and implement and carry out its responsibilities as part of the Kimberley Process.

Liechtenstein

The Principality of Liechtenstein's well-developed offshore financial services sector, relatively low tax rates, loose incorporation and corporate governance rules, and tradition of strict bank secrecy have contributed significantly to the ability of financial intermediaries in Liechtenstein to attract funds from abroad. These same factors have historically made the country attractive to money launderers. Rumors and accusations of misuse of Liechtenstein's banking system persist in spite of the progress the principality has made in its efforts against money laundering.

Liechtenstein's financial services sector includes 16 banks, three non-bank financial companies, and 16 public investment companies, as well as insurance and reinsurance companies. The three largest banks cover ninety percent of the market. Liechtenstein's 230 licensed fiduciary companies and 60

lawyers serve as nominees for, or manage, more than 75,000 entities (mostly corporations, Anstalts, or trusts) available primarily to nonresidents of Liechtenstein. Approximately one third of these entities hold controlling interests in other entities, chartered in countries other than Liechtenstein. Laws permit corporations to issue bearer shares.

Like many of its neighbors, Liechtenstein has bearer passbook accounts as well. Although the owners were identified at the opening of the account, and due diligence practices should force any bearer to identify him/herself at the counter, there is still the possibility of transferability. The Government of Liechtenstein (GOL) has decided that bearer accounts will no longer be opened. Total assets under management in Liechtenstein banks increased by Swiss francs (CHF) 7.32 billion to CHF 103.415 billion (an increase of 7.6 percent). Due to outsourcing of business units, the number of banking staff decreased from 1,718 to 1,527 (a decrease of 11.1 percent)

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 applies some money laundering controls to financial institutions and intermediaries operating in Liechtenstein, the anti-money laundering regime at that time suffered from serious systemic problems and deficiencies.

In response to international pressure, beginning in 2000, the GOL took legislative and administrative steps to improve its anti-money laundering regime. 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. In addition, financial intermediaries must set up profiles of their clients, which go beyond identification to include their assets and how the clients obtained them. These laws also address the independence of accountants reporting on anti-money laundering compliance.

The GOL continues to make progress in strengthening its anti-money laundering regime and implementing recent reforms. Liechtenstein has increased the resources, both human and financial, devoted to fighting money laundering. Domestically, an inter-ministerial body called the Money Laundering Coordination Group meets quarterly to work on coordination between agencies. Attorneys have become covered entities, as have dealers in high-value goods; and the practice of "tipping off" is prohibited. The GOL has committed all financial institutions (banks and non-bank intermediaries) to obtain full identification of accounts' beneficial owners. The list of predicate offenses for money laundering has been expanded through Article 165 of the Criminal Code. Article 165 also criminalizes laundering one's own funds, and imposes higher penalties for money laundering. However, negligent money laundering is not addressed.

On August 18, 2004, the GOL announced its intention to intensify its fight against money laundering by undertaking a full revision of its Due Diligence legislation. The scope of the revision goes beyond the mirroring of European Union (EU) money laundering guidelines. The proposed revisions address issues such as implementing stronger know your customer regulations and procedures for risk-based monitoring. The revisions also call for the termination of existing relationships with shell banks, as well as the expansion of covered institutions to include casinos, auctioneers, dealers in precious goods, and auditors. The GOL believes the amended Due Diligence Law will increase the attractiveness and stability of the financial center of Liechtenstein. The revisions are expected to become effective on February 1, 2005.

Originally, the Financial Supervision Authority (FSA) was responsible for supervising all banks and fiduciaries licensed to operate in Liechtenstein. The FSA had the authority to conduct on-site spot checks and to request information as required. To remedy problems that arose with the implementation of the laws, a Due Diligence Unit (SSP) was also established to supervise compliance with anti-money laundering regulations. In 2002 the GOL assigned the SSP to handle all supervisory responsibilities, removing it entirely from the FSA. Currently, supervisory responsibility is split between SSP and the

Financial Intelligence Unit (FIU). The SSP has completed over 80 audits covering over 25,000 banking relationships, and works effectively and closely with the FIU, the Office of the Prosecutor, and the police. The GOL is currently working on reorganizing this system via the establishment of an integrated regulatory unit, combining all sectors under one roof.

Liechtenstein's FIU, the Einheit fuer Finanzinformationen (EFFI), became operational in March 2001, and a member of the Egmont Group in June 2001. 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 EFFI's authority. The EFFI has developed a system for suspicious transaction reporting (STR) analysis that involves internal examination, 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 and has access to various governmental databases, although it cannot seek additional financial/bank information unrelated to a filed STR. Currently, banks, insurers, financial advisers, postal services, bureaux de change, attorneys, financial regulators, and casinos are required to file STRs. The GOL also reformed its STR system to permit reporting for a much broader range of offenses and 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." Another problem is that if a transaction is not completed, it is at the institution's discretion whether to report it. EFFI also has responsibility for analysis and transactions in the countering of terrorism financing.

In 2003, STR notifications dropped by 14.9 percent from the year before to 172. Of these 172 cases, 82 reports each were submitted by bank and professional trustees. During 2003, fraud, money laundering, and embezzlement were the most prevalent types of offense. The number of STRs involving fraud remained stable at 38 percent, while the STRs involving money laundering and embezzlement increased from 27.7 to 36.6 percent and from 9.9 to 15 percent respectively.

Although the number of STRs filed by financial institutions in Liechtenstein is relatively small, they have generated several money laundering investigations. The EFFI works closely with the prosecutor's office and law enforcement authorities, as well as with a special unit of the National Police, known as the EWOK, that deals with economic and organized crime. The EWOK is a special unit of eight to ten police officers established specifically to address money laundering crimes. When authorized to do so by a Special Investigative Judge, the police can use special investigative measures.

Well over 100 STRs made it to the Public Prosecutor's Office, which has doubled its staff to better handle the caseload. Three indictments have resulted from those 100 STR referrals. Liechtenstein has not adopted the EU-driven policy of reversing the burden of proof, i.e., making it necessary for the defendant to prove that he had acquired assets legally instead of the state's having to prove he had acquired them illegally. Most of the customers involved in money laundering activities were from Switzerland, Germany, and Austria. Customers from the United States (along with those from Britain) ranked fourth in STR filings. The EFFI reports that about \$260 million worth of suspicious money originated from the United States.

In 2003, the GOL received 129 inquiries from 18 foreign FIUs. This figure is almost twice the number received the previous year. In the same period, the EFFI submitted 145 inquiries to 18 different countries. This represents an increase of nearly 65 percent over the preceding year. The most frequent judicial cooperation requests originated from or were directed to Germany, Switzerland, and Austria.

In late 2002, the International Monetary Fund (IMF) assessed Liechtenstein's financial sector. The IMF's assessment was overall a positive one, noting that staffing deficiencies that existed throughout Liechtenstein's agencies (particularly the FSA and the Insurance Supervisory Authority) were due to lack of personnel and not the competence and professionalism of the existing staff. The IMF also

found that while the then current legislation addressed terrorism financing to an extent, it was not completely covered.

Liechtenstein has in place legislation to seize, freeze, and share forfeited assets with cooperating countries. The Special Law on Mutual Assistance in International Criminal Matters gives priority to international agreements. Money laundering is an extraditable offense, and legal assistance is granted on the basis of dual criminality (i.e., the offense must be a criminal offense in both jurisdictions). Article 235A provides for the sharing of confiscated assets, and this has been used in practice.

A series of amendments to Liechtenstein law, adopted by Parliament on May 15, 2003, include a new catchall criminal offense for terrorist financing along with amendments to the Criminal Code, the Code of Criminal Procedure and the Due Diligence Act. Liechtenstein also has issued ordinances to implement UNSCRs 1267 and 1333. Amendments to the ordinances in October and November 2001 allow the GOL to freeze the accounts of individuals and entities that were designated pursuant to these UNSCRs. The GOL updates these ordinances regularly. 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. The total value reported frozen as of December 2003 by the Liechtenstein authorities based on UNSCR 1267 is \$145,300. According to the 2003 Liechtenstein report to the UN, six Taliban-related entities have been located in Liechtenstein. Their assets have been frozen and overlap with the \$145,300 reported above.

The GOL has also improved its international cooperation provisions in both administrative and judicial matters. A Mutual Legal Assistance Treaty (MLAT) between Liechtenstein and the United States entered into force on August 1, 2003. The U. S. Department of Justice has acknowledged Liechtenstein's cooperation in the Al-Taqwa case and in other fraud and narcotics cases. The EFFI has in place a memorandum of understanding (MOU) with the Belgian FIU. Further MOUs are being prepared with Switzerland, France, Italy, Croatia, Poland, San Marino, and Lithuania. In addition, preliminary talks are being held with Russia and Germany.

Liechtenstein is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The GOL is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and the UN International Convention for the Suppression of the Financing of Terrorism. Liechtenstein has now ratified all twelve relevant international conventions and protocols. Liechtenstein has also signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Liechtenstein has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision" and has adopted the EU Convention on Combating Terrorism.

The Government of Liechtenstein has made consistent progress in addressing previously noted shortcomings in its anti-money laundering regime. It should continue to build upon the foundation of its evolving anti-money laundering/counterterrorist financing regime. Liechtenstein should accede to the 1988 UN Drug Convention. Liechtenstein should eliminate all bearer passbook accounts, require reporting of cross-border currency movements, and insist that trustees and other fiduciaries comply fully with all aspects of the new anti-money laundering legislation and attendant regulations, including the obligation to report suspicious transactions. The Einheit fuer Finanzinformationen, the Financial Intelligence Unit, should be given access to additional financial information. While Liechtenstein recognizes the rights of third parties and protects uninvolved parties in matters of confiscation, the government should distinguish between bona fide third parties and others.

Lithuania

With ten commercial banks, two foreign bank branches and 58 credit unions, Lithuania is not a regional financial center. Lithuania has established laws that have created adequate legal safeguards against money laundering; however, its geographic location still makes it a target for smuggled goods and tax evasion. The sale of narcotics does not generate a significant portion of financial crime and money laundering activity in Lithuania; and in 2004, there were no reported cases of money laundering related to narcotics. Most financial crimes are tied to tax evasion, smuggling, illegal production and sale of alcohol, capital flight, and profit concealment. The shadow economy is estimated to account for approximately 18 percent of the total gross domestic product of Lithuania.

The flow of smuggled goods, principally cigarettes and alcohol, from Russia and Belarus, is driven by price differentials between regional non-European Union (EU) countries, Lithuania, and the West. A pack of cigarettes in Lithuania can cost one-fourth the price of a pack in the rest of the EU. Experts anticipate that smuggling will increase when Lithuania adopts the minimum EU excise rate in 2009. Smuggled goods from China are also a source of illicit income through underreporting of the goods' value to Customs and the Lithuanian Tax Administration in order to avoid the value added tax (VAT). With the removal of border checkpoints after Lithuania's accession to the EU on May 1, 2004, Customs officials are only able to inspect Chinese goods if they receive information that allows them to track the goods to Lithuanian warehouses.

Lithuania is not an offshore financial center; however, the State Tax Administration states that it has encountered cases of Lithuanian companies purchasing goods in Russia at lower prices, and then attributing higher prices to offshore companies outside Lithuania, in order to conceal their illicit profits.

Lithuania has Free Economic Zones (FEZ) in the cities of Klaipeda, Kaunas, and Siauliai. Klaipeda is the country's largest seaport, Kaunas is an air, road, and rail hub and Siauliai has the largest airport in the Baltic region. There are currently four businesses operating in the Klaipeda FEZ, the largest of Lithuania's zones, with 130 million euros (\$174 million) in total foreign investment. Klaipeda has signed contracts with four more enterprises to begin operations in 2005. Companies operating the FEZs receive the same legal guarantees as those operating elsewhere. Parliament approved a law on the fundamentals of FEZs in June 1995 that regulates conditions for the establishment of companies in these zones. Businesses in the FEZs receive corporate tax reductions for the first 10 years of existence, customs tax exemptions, VAT exemptions and discounted land leases. Lithuania's EU accession agreement permits the indefinite operation of existing free trade zones, but precludes the establishment of new ones. The Government of Lithuania (GOL) has no indication that any of the FEZs are being used in trade-based money laundering schemes or by the financiers of terrorism.

The GOL criminalized the act of money laundering in 1997 with the Law on the Prevention of Money Laundering (LPML), which entered into force in 1998. Lithuania does not have an "all serious crimes" anti-money laundering law. On January 29, 2004, the Lithuanian Parliament amended the definition of money laundering in Article 216 of the Criminal Code. The law now says that a money launderer, i.e., any person or enterprise, "who carries out financial operations with his own or another person's money or property, or with part of them, knowing that such money or property was acquired in a criminal way, concludes the agreements, uses them in economic or commercial activity, or makes a fraudulent declaration that they are derived from legal activity, for the purposes of concealing or legitimizing these proceeds shall be punished by imprisonment for a term of up to seven years."

Individuals must declare to Customs cash they transport into or out of the country in excess of LTL 10,000 (approximately \$3,800). Since Lithuania's EU accession, this requirement applies only to non-EU citizens. Customs authorities must report to the Financial Crimes Investigative Service (FCIS), Lithuania's financial intelligence unit, within seven working days, any violations for failure to declare currency in excess of 50,000 litas (approximately \$19,200).

Money Laundering and Financial Crimes

On November 25, 2003, the Lithuanian Parliament adopted the Amendment to the Law on the Prevention of Money Laundering (the LPML Amendment), which came into force on January 1, 2004, in order to comply with the obligations specified in the EU's Second Money Laundering Directive and terrorism convention, as well those in the FATF's Forty Recommendations.

Four new regulations were published in 2004 to implement the new requirements of the LPML. In July, the cabinet expanded the criteria to identify suspicious money operations. The new list includes 25 detailed criteria, such as an unusual increase in cash payments, cashing 100,000 litas (approximately \$40,000) or more within seven days, structuring funds under the reporting requirements, and cashing more than 100,000 litas (approximately \$40,000) in seven days using a foreign credit card.

The LPML Amendment expands the types of financial and non-financial entities subject to the requirement to report suspicious or unusual activity of any amount, and the identity of the clients involved, to the FCIS. In addition to financial institutions, the reporting requirements now extend to post offices, lawyers associations, investment companies, and insurance companies. It also expands the list of professions that have to implement preventive measures against money laundering to include auditors, accountants, notaries, tax advisors, enterprises providing bookkeeping or tax consultation services, lawyers and their assistants, casinos, and people who are engaged in commercial or economic activity related to real estate, precious stones, metals, works of art, antiquarian cultural valuables, or other high value goods. The Cabinet also adopted new rules to provide the FCIS information on the identity of subjects involved in suspicious transactions. The regulation establishes a list of data and documents that a bank or other financial institution must request from a person whose transaction requires customer identification. The Cabinet also adopted detailed rules governing the management of suspicious transactions registers. Banks are aware of their reporting requirements and although not very happy about the burden imposed on them, have been very cooperative and report and exchange information of their own accord, not only upon request of the FCIS.

For large transactions exceeding 50,000 litas (approximately \$19,200), the LPML requires all financial institutions to collect information on the identity of the customer, maintain the documents for a minimum of ten years, and report the activity to the FCIS within seven days of the transaction. The LPML Amendment also mandates a stricter customer identification policy for insurance companies and casinos. Insurance companies must identify customers whose annual insurance payment exceeds 8,500 litas (approximately \$3,270). Casinos must register patrons who wager, win, or exchange currency for chips for amounts larger than 3,500 litas (approximately \$1,345). Although the insurance companies and casinos are not obligated to report customer identification, they usually file this information with the FCIS. Starting in January 2004, all taxpayers were required to submit an annual income and property declaration to the Tax Inspectorate. Prior to this, only politicians, business managers, and those purchasing property with a value in excess of 46,000 litas (approximately \$17,700), were obliged to submit declarations. The change to the regulation closes the loophole that allowed funds that were undeclared or from unknown sources to be used to purchase real estate.

Credit institutions (banks) are all privately owned and also function as bureaux de change. They must be licensed by the Central Bank of Lithuania (BOL) and follow special record keeping requirements. The BOL has the authority to examine the books, records, and other documents of all financial institutions and casinos. The BOL then informs law enforcement authorities of any violations recorded during its examination. The LPML protects bankers who report required information to the FCIS. There were no investigations started in 2004 against bank officials for complicity in money laundering. Insurance and brokerage companies are under supervision by the Insurance and Brokerage Commission, which can execute administrative measures or revoke a company's license.

The FCIS, located in the Ministry of the Interior (formerly the Tax Police Department), is Lithuania's Financial Intelligence Unit (FIU). There were 156 suspicious transaction reports (STRs) filed with the

FCIS in 2002, 115 in 2003, and only 65 in 2004. In addition to STRs, the FCIS receives currency transaction reports (CTRs) for currency exchanges over 50,000 litas (approximately \$19,200). There were 43,164 CTRs filed with the FCIS in 2002, 1,020,668 in 2003, and 747,748 in 2004. In total, there have been approximately 423 STRs and 3,921,000 CTRs filed with the FCIS since 1998.

The FCIS reported that there were no convictions for money laundering in 2004; however the Prosecutor's Office initiated criminal proceedings for nine suspected cases of money laundering, and seven additional cases of suspected tax evasion, document forgery, and smuggling. The nine suspected money laundering cases were uncovered due to an investigation by the FCIS into 119 suspicious bank transactions. The lack of adequate information sharing among the FCIS, Customs, and Border Guards, limited training, and corruption of officers at the regional level can sometimes hinder investigations and cooperation among the Lithuanian law enforcement agencies; although in recent years, the GOL has made an effort to provide several training seminars to various law enforcement entities.

On May 1, 2003, the new Criminal Code of the Republic of Lithuania came into force, replacing the 1961 Criminal Procedures Code. Article 216 of the Code increases the role of prosecutors and closes loopholes with regard to corruption. Previously, the police could freeze/seize assets on their own authority, but now they must go to the prosecutors with the named property and receive authority to freeze/seize the assets of a suspected crime. The suspect may appeal to a higher court, and the decision of the Supreme Court is final.

Prosecutors may prohibit individuals suspected of involvement in money laundering or other financial crimes from disposing of property for a period of up to six months. Freezing assets for a longer period requires a court order. The court can seize only property which the criminal or accomplice used as an instrument of a crime or a means to commit a crime or which was acquired as the direct result of a criminal act. The court may seize assets in order either to ensure the possibility of forfeiture in a criminal case or to secure a judgment in a civil action. Upon conviction of money laundering or terrorism financing, individuals may be subject to fines, restrictions on operating any companies owned by them, or liquidation of property.

In November 2004, the Cabinet approved the new "rules on stopping suspicious money operations and providing information to the FCIS." These rules entitle the FCIS to request any legal or natural entities (except notaries) to freeze suspicious money transactions for 48 hours. The FCIS may extend the freeze if an investigation is started. The FCIS froze over 25 million litas (approximately \$9.6 million) in assets from January through October 2004. In 2003, the FCIS froze over 52 million litas (approximately \$20 million). There are no figures available for the total value of forfeited crime-related assets. Proceeds from seizures and forfeitures go into the national budget. Lithuania does not share crime-related assets with other governments.

Article 250 of the Lithuanian Criminal Code, which came into effect in April 2003, establishes the financing of terrorism as a crime and prescribes imprisonment of four to twenty years. The GOL has independent national authority to freeze assets linked to terrorism. The amended LPML includes the direct or indirect funding of terrorism within the definition of terrorist financing. The LPML obligates the reporting institutions to notify the FCIS immediately about money transactions (both cash and non-cash) that might be related to terrorist financing, irrespective of the amount of the transaction. The LPML Amendment also includes terrorist financing as a predicate offense for money laundering.

In April 2004, the Parliament passed a law on the Implementation of Economic and other International Sanctions, which makes international financial sanctions, including terrorist sanctions, valid in Lithuania. Provisions of the law apply to the actions of Lithuanian legal and natural persons in foreign countries, irrespective of whether foreign countries implement international sanctions as applied by Lithuania. The State Security Department, the lead GOL agency coordinating efforts against terrorism, and the FCIS circulate to financial institutions the names of all terrorist individuals and entities on the UNSCR 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global

Terrorists designated by the United States pursuant to E.O. 13224. On May 15, 2003, the Governmental Decree “On the Approval of the Criteria in Observance Whereof a Monetary Operation is Considered Suspicious” was supplemented. One of the new criteria states that if data identifying a bank customer, a representative of the customer conducting a transaction, or the subject on behalf of whom the monetary operation is being conducted, correspond to the data about persons related to terrorist activity, and included on the circulated lists, such person is to be considered suspicious, and his transactions treated accordingly. To date, the government has provided no indication that searches have yielded evidence of terrorist assets. Charitable and nonprofit entities do not play a role as conduits to finance terrorism. Alternative remittance systems reportedly do not exist in Lithuania.

Lithuania has signed memoranda on exchange of money laundering-related financial and intelligence information with the FIUs of Belgium, Croatia, the Czech Republic, Estonia, Finland, Latvia, Bulgaria, Slovenia, and Poland. Lithuania and Germany signed an agreement in 2001 to cooperate in the fight against organized crime and terrorism. The FCIS signed four agreements in 2004 covering cooperation against economic and financial crimes, money laundering, and the exchange of information with the European Anti-Fraud Office, the Azerbaijan Revenue Service, the Italian Guardia Di Finanza and the Estonian Tax and Customs Board. There is a mutual legal assistance treaty (MLAT) between the United States and Lithuania, which entered into force in 1999. Lithuanian law enforcement cooperates with the United States in investigations and the exchange of information related to money laundering, financial crimes, terrorist financing and customs issues. In 2004, FCIS responded to five FBI and FinCEN requests in 2004 for cooperation on money laundering and fraud cases. The police and FCIS continue to cooperate with U.S. law enforcement bodies on a significant Russian Organized Crime/Money Laundering investigation. Through the MLAT and other requests, the GOL provided bank records and other evidence to the United States to be used at trial; and Lithuania allowed bank officials to travel to the United States to testify at trial.

Lithuania is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. Lithuania is also a party to the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime. Lithuania is a member of the Council of Europe’s Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), and the FCIS is a member of the Egmont Group.

The Government of Lithuania should continue its efforts to enhance its anti-money laundering/counterterrorist financing regime. In particular, Lithuania should ensure that its asset forfeiture regime is adequate and should consider enactment of measures to allow asset sharing with third party jurisdictions that participate in the investigation of international money laundering cases. Lithuania also should ensure that non-governmental organizations, including charities, are adequately supervised and regulated to prevent their abuse by criminal or terrorist groups. Lithuania should provide adequate resources and training to its law enforcement entities to ensure the successful investigation and prosecution of money laundering and terrorist financing.

Luxembourg

Despite its standing as the smallest member of the European Union (EU), Luxembourg is one of the largest financial centers in the world. Its strict bank secrecy laws allow international financial institutions to benefit from and operate a wide range of services and activities. With over a trillion euros in assets managed by the global investment fund industry, Luxembourg joins the United States and France as one of the top three domiciles for investment fund activity. Luxembourg is considered an offshore financial center, with foreign-owned banks accounting for a majority of the nation’s total bank assets. Although there are a handful of domestic banks operating in the country, the majority of banks registered in Luxembourg are foreign subsidiaries of banks in Germany, France, and Belgium.

For this reason (and also due to the proximity of these three nations to Luxembourg), a significant share of Luxembourg's suspicious transaction reports (STR) are generated from transactions involving clients in these three countries.

While Luxembourg is not a major hub for illicit drug distribution, the size and sophistication of its financial center create opportunities for drug-related money laundering and terrorist financing. According to a December 2004 International Monetary Fund (IMF) report, Luxembourg has "a solid criminal legal framework and supervisory system" to counter money laundering and terrorist financing, and is "broadly compliant with almost all of the Financial Action Task Force (FATF) Recommendations." The report also notes that Luxembourg's high level of cross-border business, obligatory banking secrecy, private banking, and "certain investment vehicles" create a challenging environment for countering money laundering and terrorist financing. Further complicating the scenario is the fact that Luxembourg currently has no cross-border reporting requirements.

As of November 2004, 165 banks, with a balance sheet total reaching 689 billion euros, were registered within Luxembourg. In addition, as of December 2004, a total of 1,951 "undertakings for collective investment" (UCIs), or mutual fund companies, whose net assets had reached over a trillion euros by the end of October 2004, were operating out of Luxembourg. Luxembourg has about 15,000 holding companies, 95 insurance companies, and 270 reinsurance companies. As of November 2004, the Luxembourg Stock Exchange listed over 30,000 securities issued by nearly 4,300 entities from about 100 different countries. Legislation passed in June 2004 permits the registration of venture capital funds (*Societe d'investissement en capital a risqué*, or "SICAR").

Luxembourg's financial sector laws are modeled to a large extent on EU directives. The Law of July 7, 1989, updated in 1998, serves as Luxembourg's primary anti-money laundering (AML) law, criminalizing the laundering of proceeds for an extensive list of predicate offenses, including narcotics-trafficking. The Law of April 5, 1993 implements the EU's 1991 First Anti-Money Laundering Directive (Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering) and includes among its provisions customer identification, record keeping, and suspicious transaction reporting requirements. The Act of August 1, 1998 expands the list of covered entities and adds corruption, weapons offenses, and organized crime to the list of predicate offenses for money laundering. The Act of June 10, 1999 further expands anti-money laundering provisions. Fraud committed against the European Union has also been added to the list of offenses. Although only natural persons are currently subject to the law, a bill is under consideration for 2005 that would add legal persons to its jurisdiction.

In an effort to bring Luxembourg into full compliance with the requirements of the EU's Second Anti-Money Laundering Directive, on November 12, 2004, Parliament approved legislation updating the nation's anti-money laundering laws. These legislative amendments formally transferred the requirements of the EU's Second Money Laundering Directive into domestic law. The 2004 amendments also broaden the scope of institutions subject to money laundering regulations. Under the current law, banks, pension funds, insurance brokers, UCIs, management companies, external auditors, accountants, notaries, lawyers, casinos and gaming establishments, real estate agents, tax and economic advisors, domiciliary agents, insurance providers, and dealers in high-value goods, such as jewelry and cars, are now considered covered institutions. AML law does not cover SICAR entities. All covered entities are required to file STRs with the Financial Intelligence Unit (FIU) and, though not legally required, are expected to send a copy of the report to their respective oversight authorities. Financial institutions are required to retain pertinent records for a minimum of five years; additional commercial rules require that certain bank records be kept for up to ten years. The AML law also contains "safe harbor" provisions that protect obliged individuals and entities from legal liability when filing STRs or assisting government officials during the course of a money laundering investigation. The 2004 amendments also contain new requirements regarding financial institutions' internal AML programs. It imposes stricter "know your customer" requirements, mandating their application to all

new and existing customers, including beneficial owners, trading in goods worth at least 15,000 euro. If the transaction or business relationship is remotely based, the law details measures required for customer identification. Financial institutions must ensure adequate internal organization and employee training, and must also cooperate with authorities, proactively monitoring their customers for potential risk. “Tipping off” has also been prohibited.

Although Luxembourg’s 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. No court order is required to investigate otherwise secret account information in suspected money laundering cases, or when a STR is filed. Financial professionals are obliged to cooperate with the public prosecutor in investigating such cases.

The Commission de Surveillance du Secteur Financier (CSSF) is an independent government body under the jurisdiction of the Ministry of Finance, that serves as the prudential oversight authority for banks, credit institutions, the securities market, some pension funds, and other financial sector entities covered by the country’s anti-money laundering and terrorist financing laws. The Luxembourg Central Bank oversees the payment and securities settlement system, and the Commissariat aux Assurances (CAA), also under the Ministry of Finance, is the regulatory authority for the insurance sector. The identities of the beneficial owners of accounts are available to all entities involved in oversight functions, including registered independent auditors, in-house bank auditors, and the CSSF.

Under the direction of the Ministry of the Treasury, the CSSF has established a committee, the Comité de Pilotage Anti-Blanchiment (COPILAB), composed of supervisory and law enforcement authorities, the FIU and financial industry representatives. The committee meets monthly to develop a common public-private approach to strengthen Luxembourg’s AML regime.

No distinctions are made in Luxembourg’s laws and regulations between onshore and offshore activities. Foreign institutions seeking establishment in Luxembourg must demonstrate prior establishment in a foreign country and meet stringent minimum capital requirements. Companies must maintain a registered office in Luxembourg, and background checks are performed on all applicants. A ministerial decree published in July 2004 modified the Luxembourg Stock Exchange’s internal regulations to make it easier to list offshore funds, provided the fund complies with CSSF requirements (as detailed in Circular 04/151). Also, a government registry publicly lists company directors. Although nominee (anonymous) directors are not permitted, bearer shares are permitted. Banks must undergo annual audits under the supervision of the CSSF (CSSF reg. No. 27). Independent auditors have established a peer review procedure in compliance with an EU recommendation on quality control for external audit work to assure the adherence to international standards on auditing.

Established within Luxembourg’s Ministry of Justice, the Cellule de Renseignement Financier FIU-LUX serves as Luxembourg’s FIU, receiving and analyzing STRs from the financial sector, and seizing and freezing assets when necessary. As part of modifications made in 2004 to Luxembourg’s money laundering law, the FIU’s official status as a division of the Ministry of Justice Public Prosecutor’s office was formalized. While the FIU’s superiors can require the FIU to take action against a suspect, they cannot prevent the FIU from prosecuting. Some members of the financial community continue to call for the creation of an administrative FIU body separate from the office of the public prosecutor. The FIU is responsible for providing members of the financial community with access to updated information on money laundering and terrorist financing practices. It also works closely with various regulatory bodies such as the CSSF and the CAA. The FIU and CSSF work together in investigations involving significant money laundering cases.

In order to obtain a conviction for money laundering, prosecutors must now prove criminal intent rather than negligence. Negligence, however, is still scrutinized by the appropriate sector oversight authority, with sanctions for noncompliance varying from 1,250 to 1,250,000 euros.

As of mid-December 2004, covered institutions had filed a total of 914 STRs. This figure represents a steady increase from previous years (832 STRs were filed in 2003, 631 in 2002, and 431 in 2001). At the end of 2004, three individuals were jailed pending charges of laundering approximately 50 million euros in cash of drug-related money. These cases have involved consistent, close coordination between Luxembourg and foreign law enforcement agencies. An ongoing investigation from 2002 concluded in mid-2004 with a conviction and a sentence of seven years in prison; the case remains under appeal by the defendant. Fourteen additional money laundering cases are still open and under investigation by law enforcement officials. There is a consistently high level of cooperation between U.S. and Luxembourg law enforcement authorities on money laundering investigations.

The law only allows for criminal forfeitures and public takings. Drug-related proceeds are pooled in a special fund to invest in anti-drug abuse programs. Funds found to be the result of money laundering can be confiscated even if they are not the proceeds of a crime. The GOL can, on a case-by-case basis, freeze and seize assets, including assets belonging to legitimate businesses used for money laundering. The government has adequate police powers and resources to trace, seize, and freeze assets without undue delay. Luxembourg has a comprehensive system not only for the seizure and forfeiture of criminal assets, but also for the sharing of those assets with other governments.

Luxembourg authorities have been actively involved in bilateral and international fora and training in order to become more effective at fighting the financing of terrorism. In July 2003, Luxembourg's parliament passed a multifaceted counterterrorism financing law known as *Projet de Loi 4954*, designed to strengthen Luxembourg's ability to fight terrorism and terrorist financing. The law defines terrorist acts, terrorist organizations, and terrorism financing in the Luxembourg Criminal Code. In addition, the specific crimes, as defined, will carry penalties of 15 years to life. The law also extends the definition of money laundering to incorporate new terrorism-related crimes, and, with regard to Special Investigative Measures, provides an exception to notification requirements in selected wiretapping cases. The November 2004 amendments bring Luxembourg into compliance with the FATF's Special Recommendation Number Four, by extending the reporting obligations of the financial sector to terrorist financing, independently from any context of money laundering. Covered institutions now are required to report any transaction believed to be related to terrorist financing, regardless of the source of the funds.

The Ministry of Justice studies and reports on potential abuses of charitable and non-profit entities to protect their integrity. Luxembourg authorities have not found evidence of the widespread use in Luxembourg of alternative remittance systems such as hawala, black market exchanges, or trade-based money laundering. Officials comment that existing AML rules would apply to such systems, and no separate legislative initiatives are currently being considered to address them.

In an effort to identify and freeze the assets of suspected terrorists, the GOL actively disseminates to its financial institutions information concerning suspected individuals and entities on the UNSCR 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. Luxembourg does not yet have legal authority to designate terrorist groups. The government is currently working on draft legislation with regard to this issue. Luxembourg strives to cooperate with and provide assistance to foreign governments in their efforts to trace, freeze, seize and forfeit assets. Dialogue and other bilateral proceedings between the GOL and the United States have been particularly extensive.

Furthermore, authorities can and do take action against groups targeted through the EU designation process, the UN, or on behalf of bilateral requests from other countries. Under the 2004 amendments to Luxembourg's AML law, bilateral freeze requests are limited to a new maximum of three months; designations under the EU, UN, or international investigation processes continue to be subject to freezes for an indefinite time period. Upon request from the United States, Luxembourg froze the bank accounts of individuals suspected of involvement in terrorism. Luxembourg has also independently

frozen several accounts, resulting in court challenges by the account holders. Since 2001, over \$200 million in suspect accounts have been frozen by Luxembourg authorities pending further investigations (most of the assets were subsequently released).

Luxembourg laws facilitating international cooperation in money laundering include the Act of August 8, 2000, which enhances and simplifies procedures on international judicial cooperation in criminal matters; and the Law of June 14, 2001, which ratifies the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. During its EU council presidency from January through June 2005, Luxembourg will play a role in shepherding the draft of the Third Money Laundering and Terrorist Financing Directive through the EU's legislative process.

Luxembourg is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. In November 2003, Luxembourg ratified the UN International Convention for the Suppression of the Financing of Terrorism.

Luxembourg is a member of the European Union and the FATF. The Luxembourg FIU is a member of the Egmont Group and has negotiated memoranda of understanding with several countries, including Belgium, Finland, France, Korea, Monaco, and Russia. Luxembourg and the United States have had a Mutual Legal Assistance Treaty (MLAT) since February 2001. Luxembourg's Agency for the Transfer of Financial Technology (ATTF) has consistently provided training and acted as a consultant in money laundering matters to government and banking officials in countries whose regimes are in the development stage. Since 2001, ATTF has provided assistance to government and banking officials from Bosnia, Bulgaria, Croatia, Cape Verde, China, the Czech Republic, Egypt, Macedonia, Romania, Russia, and Ukraine. The ATTF budget has grown steadily from approximately 700,000 euros in 2000, to over 2 million euros in 2004.

The Government of Luxembourg has enacted laws and adopted practices that help to prevent the abuse of its bank secrecy laws, and has enacted a comprehensive legal and supervisory anti-money laundering regime. However, further action should be taken to address issues such as the lack of a distinct legal framework for the Financial Intelligence Unit and the small number of money laundering investigations and prosecutions. The Financial Intelligence Unit should work with regulatory agencies to formulate and issue substantive guidance to financial institutions on anti-money laundering trends and techniques. Luxembourg should continue to strengthen enforcement to prevent abuse of its financial sector, and should continue its active participation in international fora. Luxembourg should enact 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. Its offshore financial sector is not fully developed. Macau's gambling industry, however, remains particularly vulnerable to money laundering.

In 2001, the IMF assessed Macau's anti-money laundering measures as part of a study of offshore financial centers, published on March 12, 2004. The IMF concluded, "Current anti-money laundering measures as they related to the BCP (Basel Committee's 'Core Principles for Effective Banking Supervision') and ICP (Insurance Core Principles issued by the International Association of Insurance Supervisors) need strengthening." In a prior IMF "Assessment of the Regulation and Supervision of

the Financial Sector of Macao” paper published in August 2002, the IMF concluded that Macau was “materially noncompliant” with the money laundering principles of the Basel Committee’s “Core Principles for Effective Banking Supervision,” and recommended a number of improvements.

Main money laundering methods in the financial system are wire transfers; currency exchange/cash conversion; and the use of nominees, trusts, family members, or third parties to transfer cash. Macau has taken several steps over the past two years to improve its institutional capacity to tackle money laundering. These will be helpful if they lead to greater legal enforcement. In October 2002 the Judiciary Police set up the Fraud Investigation Section. One of its key functions is to receive all suspicious transaction reports (STRs) in Macau and to undertake subsequent investigations.

In 2003, the Macau Special Administrative Region Government (MSARG) also prepared money laundering legislation that would incorporate the revised FATF Forty Recommendations and establish a Financial Intelligence Unit (FIU). In 2004, the MSARG continued interagency consultations on the bill. The FIU will be set up after passage of the legislation. In 2004, an interagency body consisting of representatives from the Monetary Authority of Macau, Macau Customs Service, Unitary Police, International Law Office, Gaming Inspection and Coordination Office, and other economic and law-enforcement agencies, continued to discuss the mechanics of the establishment of the FIU and exchanged information in the FIU’s absence.

The government also drafted a terrorist financing bill that, if passed and enforced, would strengthen its efforts. Macau’s financial system is governed by the 1993 Financial System Act and amendments, which lay out regulations to prevent use of the banking system for money laundering. 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 MSARG, including pawnbrokers, antique dealers, art dealers, jewelers, and real estate agents. There is no significant difference between the regulation and supervision of onshore and of offshore financial activities.

Macau law provides for forfeiture of cash and assets that assist in or are intended for the commission of a crime. During 2003 and the first ten months of 2004, the Narcotics Division of the Police seized almost 67,000 patacas (\$8,375), 35 cell phones, five cars, and five motorcycles.

The gaming sector and related tourism are critical parts of Macau’s economy. Taxes from gaming comprised 75 percent of government revenue in 2003, while revenues from gaming increased 45 percent during the first ten months of 2004, compared with a year earlier. The MSARG ended a long-standing gaming monopoly early in 2002 when it awarded concessions to two additional operators, the U.S.-based Venetian and Wynn Corporations. The Venetian opened its first casino, the Sands, on May 18, 2004. In addition, MGM announced its intention to open a casino in conjunction with the previous monopoly operator, Sociedade de Jogos de Macau (SJM), owned by local businessman Stanley Ho. The Venetian, Wynn, and MGM are scheduled to open casinos in 2006.

Under the old monopoly framework, organized crime groups were, and continue to be, associated with the gaming industry through their control of VIP gaming rooms, and activities such as racketeering, loan sharking, and prostitution. The VIP rooms catered to clients seeking anonymity within Macau’s gambling establishments, and were particularly removed from official scrutiny. As a result, the gaming

industry, in particular, provided an avenue for the laundering of illicit funds and served as a conduit for the unmonitored transfer of funds out of China.

The Sands, unlike SJM and new entrant Galaxy, does not cede control of its VIP gaming facilities to outside organizations, and organized crime has therefore is not believed to have penetrated this operation.

The MSARG's draft money laundering legislation includes provisions designed to prevent money laundering in the gambling industry. The legislation aims to make money laundering by casinos more difficult, improve oversight, and tighten reporting requirements. On June 7 2004, Macau's Legislative Assembly passed legislation allowing casinos and junket operators to make loans, in chips, to customers. The law requires both casinos and junket operators to register with the government.

Terrorist financing is criminalized under the Macau criminal code (Decree Law 58/95/M of November 14, 1995, Articles 22, 26, 27, and 286). The MSARG has the authority to freeze terrorist assets, although a judicial order is required. Macau financial authorities directed the institutions they supervise to conduct searches for terrorist assets, using the list, listed on the UN 1267 Sanctions Committee consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. No assets have been found to date.

The Macau legislature passed an counterterrorism law in April 2002 that is intended to assist with Macau's compliance with UNSCR 1373. The legislation criminalizes violations of UN Security Council resolutions, including counterterrorist resolutions, and strengthens counterterrorist financing provisions. The UN International Convention for the Suppression of the Financing of Terrorism will apply to Macau when the PRC accedes to it.

In 2003, the MSARG drafted a new counterterrorism bill aimed at strengthening counterterrorist financing measures. As of December 2004, the bill was under consultation within the administration. The law-also drafted to comply with UNSCR 1373-would make it illegal to conceal or handle finances on behalf of terrorist organizations. Individuals would be liable even if they were not members of designated terrorist organizations themselves. The Macau Government drafted additional measures which are still under discussion. These include an administrative regulation giving the Chief Executive of Macau the authority to designate terrorists and freeze assets of terrorists not on the UNSCR 1267 Sanctions Committee's consolidated list, and permitting assets to be frozen without first obtaining a court order. The legislation would also allow prosecution of persons who commit terrorist acts outside of Macau, and would mandate stiffer penalties.

The increased attention paid to financial crimes in Macau after the events of September 11 has led to a general increase in the number of suspicious transaction reports (STRs). Macau's Judiciary Police received 107 STRs in 2003, and 86 from January 1 to October 31, 2004, from individuals, banks, companies, and government agencies. Of these 193 STRs, 21 originated from the gaming sector. Seven STRs resulted in special investigations that were ongoing as of the end of 2004, although none of these investigations has resulted in prosecutions.

In 2003, the MSARG drafted a new money laundering bill that broadened the definition of money laundering to include all serious predicate crimes. The legislation also mandated greater customer identification, a more comprehensive reporting system regarding suspicious transactions, a duty to refuse to undertake suspicious transactions, more specific guidelines for the non-banking sector-such as real estate-and penalties for entities that fail to report suspicious transactions. The bill will extend the obligations of suspicious transaction reporting to lawyers, notaries, accountants, auditors, and offshore companies. In November 2003, the Monetary Authority of Macau issued a circular to banks, requiring that STRs be accompanied by a table specifying the transaction types and money laundering methods, in line with the collection categories identified by the Asia/Pacific Group on Money Laundering (APG).

In May 2002, the Macau Monetary Authority revised its anti-money laundering regulations for banks, to bring them into greater conformity with international practices. Guidance also was issued for banks, money changers, and remittance agents, addressing record keeping and suspicious transaction reporting for cash transactions over \$2,500. For such transactions, banks, insurance companies, and moneychangers must exert customer due diligence. The Monetary Authority of Macau, in coordination with the IMF, updated its bank inspection manuals to strengthen anti-money laundering provisions. The Monetary Authority inspects banks every two years, including their adherence to anti-money laundering regulations.

The United States has no law enforcement cooperation agreements with Macau, though cooperation between the United States and Macau routinely takes place. The Judiciary Police have been cooperating with law enforcement authorities in other jurisdictions through the Macau branch of Interpol, to suppress cross-border money laundering. In addition to Interpol, the Fraud Investigation Section of the Judiciary Police has established direct communication and information sharing with authorities in Hong Kong and mainland China.

The Monetary Authority of Macau also cooperates internationally with other financial authorities. It has signed memoranda of understanding with the People's Bank of China, China's Central Bank, the China Insurance Regulatory Commission, the China Banking Regulatory Commission, the Hong Kong Monetary Authority, the Hong Kong Securities and Futures Commission, the Insurance Authority of Hong Kong, and Portuguese bodies including the Bank of Portugal, the Banco de Cabo Verde and O Instituto de Seguros de Portugal.

Macau participates in a number of regional and international organizations. It is a member of the Asia/Pacific Group on Money Laundering (APG), the Offshore Group of Banking Supervisors, the International Association of Insurance Supervisors, the Offshore Group of Insurance Supervisors, the Asian Association of Insurance Commissioners, and the International Association of Insurance Fraud Agencies.

In 2003, Macau hosted the annual meeting of the APG, which adopted the revised FATF Forty Recommendations and a strategic plan for anti-money laundering efforts in the region from 2003 to 2006. In September 2003, Macau became a party to the UN Convention against Transnational Organized Crime, as a result of China's ratification. Macau also became a party to the 1988 UN Drug Convention through China's ratification.

Macau has taken a number of steps in the past three years to raise industry awareness of money laundering. During a March 2004 IMF technical assistance mission, the IMF and Monetary Authority of Macau organized a seminar for financial sector representatives on the FATF Revised Forty Recommendations. The Macau Monetary Authority trains banks on anti-money laundering measures on a regular basis.

Macau should implement and enforce existing laws and regulations, and pass and implement its pending legislation. Macau should ensure that regulations, structures, and training are put in place to prevent money laundering in the gaming industry, including implementing, as quickly as possible, the regulations it has drafted on the prevention of money laundering in casinos. Macau should pass legislation to establish a financial intelligence unit as soon as possible.

The MSARG should take steps to implement the new FATF Special Recommendation Nine, adopted by the FATF in October, 2004, requiring countries to implement detection and declaration systems for cross-border bulk currency movement. Macau should increase public awareness of the money laundering problem, improve interagency coordination, and boost cooperation between the MSARG and the private sector in combating money laundering.

Macedonia

Macedonia is not a regional financial center. The country's economy is mainly cash-based, and citizens lack trust in the banking system following bank failures and a pyramid scheme in the early 1990s. Money laundering in Macedonia is mostly connected to financial crimes such as tax evasion, smuggling, financial and privatization fraud, bribery, and corruption. Most of the laundered proceeds come from domestic criminal activities. A small portion of money laundering activity may be connected to narcotics-trafficking. There is no evidence that narcotics-trafficking organizations or terrorist groups control money laundering. In addition, there is no evidence that weapons or human traffickers have been involved in money laundering activities using bank or non-bank financial institutions. Nor is there evidence of financial institutions or the Government of Macedonia (GOM) or any of its officials being engaged in currency transactions involving proceeds from narcotics-trafficking, and in particular involving U.S. currency or currency derived from illegal drug sales in the U.S.

Article 273 of Macedonia's criminal code, which came into force in 1996, criminalizes any form of money laundering. The legislation specifically identifies narcotics and arms trafficking as predicate offenses, and contains an additional provision that covers funds acquired from other punishable actions. A new Law on Money Laundering Prevention (LMLP) was enacted in July 2004, replacing the 2001 version, thus harmonizing Macedonia's money laundering regulations with EU standards and Financial Action Task Force (FATF) recommendations. The new law requires financial institutions to record and report all cash transactions in excess of 15,000 euros, as well as any suspicious transactions. Reporting entities are protected by law in their cooperation with law enforcement authorities. Institutions are also required to identify, report and keep track of clients performing those transactions, and to prepare programs to protect themselves against money laundering. Banks and other financial institutions are required to maintain records necessary to trace and/or reconstruct significant transactions for up to 5 years. The LMLP provides penalties for individuals and entities that do not comply with regulations, and the Banking Law includes provisions for "banker negligence" that make bank officials responsible if their institutions launder money. The country has no secrecy laws, and supervisory authorities have full access to financial institutions' records. The banking community cooperates with law enforcement authorities in tracing or reconstructing cases. The Customs Administration is required to register and report the cross-border transport of currency or monetary instruments in amounts that exceed 10,000 euros.

Non-bank financial institutions such as exchange offices and non-bank money transfer agents are poorly supervised and audited. Although intermediaries such as lawyers, accountants, brokers and notaries are obliged to submit reports to the Directorate for Money Laundering Prevention, to date none have done so. A Law on Money Transfer by entities other than banks was passed in December 2003, and defines the rules for licensing, operating and supervising money transfer agents.

Macedonia is in the process of implementing complex legislative reforms, including amendments to the Constitution that will allow for the use of specialized investigative methods. It is also changing the Law on Criminal Procedure, the Criminal Code, the Law on Misdemeanors and the Law on Enforcement of Sanctions. These reforms should strengthen the fight against organized crime, corruption, terrorism, trafficking in human beings, money laundering, and narcotics by increasing penalties, refining and tightening definitions, and defining authority.

Macedonia is not an offshore financial center. There are no offshore banks or other financial institutions in Macedonia. There is no separate regulation for offshore businesses, as current laws govern foreign and domestic businesses. There is no evidence that alternative remittance systems exist in Macedonia.

The Directorate for Money Laundering Prevention (DMPLP) is part of the Ministry of Finance. The Directorate collects, processes, analyzes, and stores data received from financial institutions and other

government agencies. It has no authority to undertake any further action, except submitting collected information to the police and the judiciary. From its establishment on March 1, 2002 until the end of 2004, the Directorate received 60,717 reports from various entities, mostly banks. Twelve of these were sent on to relevant authorities for detailed investigation, out of which five led to tax evasion cases and other criminal charges.

In June 2002, Parliament passed a Law establishing a Financial Police Unit. The unit, in the Ministry of Finance, investigates financial crimes, bank fraud, tax evasion, terrorism financing and money laundering cases reported by the DMLP. A Director was finally appointed in June 2004. Although not completely staffed, the unit has received training on money laundering and more advanced training is planned for the future. So far, there have been no arrests or prosecutions related to money laundering or terrorist financing.

Macedonia has yet to criminalize terrorist financing. The National Bank and Ministry of Finance circulate the lists of terrorist financing entities they receive. The authorities are allowed to identify named accounts, but require court orders before they can freeze and/or seize assets in those accounts. According to the LMLP, financial institutions could temporarily freeze assets of suspected money launderers and terrorist financiers until a court issues a freeze order. So far, the authorities have not identified, and therefore have not seized or frozen, assets related to terrorist financing. While Macedonia's two top banks have computer systems that allow them to easily identify both account holders and transactions with individuals named in the lists, the other 18 banks have no such systems and must search their customer lists manually.

Macedonia has concluded a number of Police Cooperation Agreements with almost all of the countries in the region (Albania, Bulgaria, Croatia, Romania, Slovenia, Austria, Turkey, Greece, Russian Federation, Ukraine, and Egypt) and has mutual legal assistance agreements with many countries. The exchange of police information is regularly provided through Interpol channels. Macedonia 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. Macedonia has concluded bilateral agreements for exchanging information on money laundering with Bulgaria, Croatia, Slovenia, Ukraine, Romania, Serbia, Montenegro and Albania.

Macedonia is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), and underwent a second evaluation for effectiveness in preventing money laundering in October 2002. At its June 2004 meeting in the UK, the Egmont group accepted Macedonia as a fully-fledged member, thus recognizing the latest efforts by the DMLP under its new Director. Macedonia is a party to the 1988 UN Drug Convention. In May 2004, the Macedonian Parliament ratified the UN International Convention for the Suppression of the Financing of Terrorism, but has yet to ratify the UN Convention against Transnational Organized Crime.

The Government of Macedonia should work to pass its pending legislation and should continue its implementation of the new legislation, including the amendments to the Constitution that will allow for the use of specialized investigative methods. Macedonia also should provide the necessary resources and training to ensure full implementation of its laws, including the adequate supervision of non-bank financial institutions. Macedonia should criminalize terrorist financing.

Madagascar

Madagascar is not a regional financial center. Criminal activity in Madagascar reportedly includes smuggling of animal products such as tortoise shells and reptile skins for sale in international markets. These schemes have in the past been related to money laundering activities within the country.

In 1997, Madagascar criminalized money laundering related to narcotics-trafficking. In June and July 2004, the Senate and National Assembly enacted broader legislation to address money laundering, seizures, confiscation, and international cooperation in dealing with the proceeds of all types of crime. The banking regulatory framework and the internal policies of the banks provide for retention of significant documents, generally for at least five years. Current banking regulations and individual bank policies require financial institutions to know their customers and to document and retain proof of their efforts to carry out that function.

The 2004 legislation defines prohibited activities and covered actors. There are broad definitions of “money laundering”, “proceeds of crime”, and “assets.” The provisions apply to physical persons and legal entities involved in operations concerning the movement of capital. They apply to banking and credit establishments, intermediate financial institutions, insurance companies, mutual savings institutions, stock brokerages, moneychangers, casinos, gaming establishments, and entities involved in real estate operations.

The first part of the 2004 law addresses prevention. It prohibits all cash payments over 10 million Ariary (\$5000). All international transfers over 6 million Ariary (\$3000) must be managed by a recognized credit or financial institution. Banks must ensure they know the identity of all clients and are obligated to investigate the source of any transactions exceeding 50 million Ariary (\$25,000). The law also requires financial institutions to establish internal programs against money laundering, including centralization of information, training, internal controls and designation of a responsible official at each branch or office.

The second part of the 2004 law addresses detection. The law authorizes the establishment of a financial intelligence service, which will serve as a clearinghouse for customer information and liaison with judicial authorities. This financial intelligence service was not yet operational by the end of 2004. Judicial authorities are authorized to use electronic, audio and video surveillance, monitor bank accounts, and access bank systems during the course of an investigation.

The law permits the freezing and seizure of assets that are the object of investigation, fines and imprisonment for money laundering and other infractions. The Government of Madagascar, through the Central Bank, currently distributes lists of individuals and organizations linked to terrorism finance throughout the banking system.

Sentences for individuals convicted of money laundering include imprisonment and fines ranging from 100,000 Ariary up to five times the laundered sum. The government can confiscate the individual’s assets and properties—as well as those of a spouse or children. Proceeds from the sale of these items can be used to fund efforts to combat organized crime and drug trafficking. No arrests or prosecutions for money laundering or terrorist financing were presented during calendar year 2004.

Madagascar is a party to the 1988 United Nations Drug Convention, the United Nations Convention against Transnational Organized Crime, and the United Nations International Convention for the Suppression of the Financing of Terrorism.

The Government of Madagascar should join the Eastern and Southern African Anti-Money Laundering Group and implement the financial intelligence service authorized in the 2004 money laundering legislation.

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 and converting remittance savings systems abroad. Under 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) drafted a “Money Laundering and Proceeds of Serious Crime” bill, which was considered in Parliament’s Commerce and Industry Committee in 2003. The committee requested revisions in the proposed legislation before it is considered in the full Parliament. The draft law would 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. The bill stipulates that the seized assets become the property of the GOM and should be used in the fight against money laundering. Reportedly, there has been no further action by the Parliament regarding the draft legislation in 2004.

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 designated under E.O. 13224 by the United States Government. 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 the UN International Convention for the Suppression of the Financing of Terrorism, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime.

The Government of Malawi should enact comprehensive anti-money laundering legislation and counterterrorist finance legislation in order to develop viable regimes to thwart both money laundering and terrorist financing regimes as it has agreed to do as a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG). Malawi should become a party to the UN Convention against Transnational Organized Crime.

Malaysia

Malaysia is not a regional center for money laundering. However, its formal and informal financial sectors are vulnerable to abuse by narcotic traffickers, financiers of terrorism and criminal elements. Malaysia’s relatively lax customs inspection at ports of entry and free trade zones, its uneven enforcement of intellectual property rights, and its offshore financial services center serve to increase its vulnerability.

Since 2000, Malaysia has made significant progress in constructing a comprehensive anti-money laundering regime. Malaysia’s National Coordination Committee to Counter Money Laundering (NCC), comprised of members from thirteen government agencies, oversaw the drafting of Malaysia’s Anti-Money Laundering Act 2001 (AMLA) and coordinates government-wide anti-money laundering efforts.

The AMLA, enacted in January 2002, criminalized money laundering and lifted bank secrecy provisions for criminal investigations involving more than 150 predicate offenses. The law also created a Financial Intelligence Unit (FIU) located in the Central Bank, Bank Negara Malaysia (BNM). The FIU is tasked with receiving and analyzing information, and sharing financial intelligence

with the appropriate enforcement agencies for further investigations. The Malaysian FIU works with more than twelve other agencies to identify and investigate suspicious transactions.

The Government of Malaysia (GOM) has a well-developed regulatory framework, including licensing and background checks, to oversee onshore financial institutions. BNM stringent 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. A comprehensive supervisory framework has been implemented to audit financial institutions’ compliance with AMLA. Currently, there are 300 examiners who are responsible for money laundering inspections for both onshore and offshore banks

Malaysia has strict “know your customer” rules under the AMLA. Every transaction, regardless of its size, is recorded. Reporting institutions must maintain records for at least six years and report any suspicious transactions to the Central Bank’s Financial Intelligence Unit (FIU). Regardless of the transaction size, if the reporting institution deems a transaction suspicious, it must report that transaction to the FIU. Officials indicate that they receive regular reports from institutions, but cannot divulge the volume or frequency of such reports. Reporting individuals and their institutions are protected by statute with respect to their cooperation with law enforcement. While Malaysia’s bank secrecy laws prevent general access to financial information, those secrecy provisions are waived in the case of money laundering investigation under the AMLA.

Malaysia has adopted “due diligence” or “banker negligence” laws that make individual bankers responsible if their institutions launder money. Both reporting institutions and individuals are required to adopt internal compliance programs to guard against any offense under the AMLA. Under the AMLA, any person or group who engages in, attempts to engage in or abets the commission of, money laundering would be subject to criminal sanction. Reporting institutions are required to file suspicious transaction reports under the AMLA. All reporting institutions are subject to the same review by the FIU and other law enforcement agencies. Reporting institutions include: commercial banks, money changers, discount houses, insurers, insurance brokers, Islamic insurance and reinsurance (takaful and retakaful) operators, offshore banks, offshore insurers, offshore trusts, the Pilgrim’s Fund (to pay for Hajj trips to Mecca), Malaysia’s postal service, development banks such as Malaysia’s National Savings Bank (Bank Simpanan Nasional), The People’s Cooperation Bank (Bank Kerjasama Rakyat Malaysia Berhad), and licensed casinos.

The detailed regulations for examining money laundering are still in development for all segments of the financial industry. By using a consultative approach, the Central Bank’s FIU continues to expand the scope of institutions which must report suspicious transactions. This approach encouraged Malaysia’s professional societies for lawyers and accountants to add suspicious transaction reporting requirements to their bylaws. Likewise, in consultation with the Security Commission, stockbrokers and brokerage houses are now required to submit suspicious transaction reports. The Government’s consultative approach has minimized potential political fallout from the statute’s expansion.

Malaysia’s fledgling Islamic finance sector, accounting for approximately 10 percent of total deposits, is subject to the same strict supervision to combat financial crime as the commercial banks. A combination of legacy exchange controls imposed after the 1997-98 Asian financial crisis and robust regulation and supervision by the Central Bank makes the Islamic financial sector as unattractive to financial criminals as is the conventional financial sector.

In 1998 Malaysia imposed foreign exchange controls that restrict the flow of the local currency, the ringgit, from Malaysia. Onshore banks must record cross-border transfers over RM5, 000 (approximately \$1,300). Since April 2003, an individual form is completed for each transfer above RM50, 000 (approximately \$13,170). Recording is done in a bulk register for transactions between

RM5, 001 and RM50, 000. Banks are obligated to record the amount and purpose of these transactions.

Malaysia's offshore banking center in the island of Labuan, located off the eastern coast of Malaysia, is vulnerable to money laundering and the financing of terrorism. The Labuan Offshore Financial Services Authority (LOFSA) is under the authority of the Central Bank, Bank Negara. The offshore sector has different regulations for the establishment and operation of offshore businesses, than for onshore businesses. However, the same anti-money laundering laws as those governing domestic financial service providers govern the offshore sector. Offshore banks, insurance companies, and trust companies are required to file suspicious transaction reports under the country's anti-money laundering law.

LOFSA licenses offshore banks, banking companies, trusts and insurance companies, and performs stringent background checks before granting an offshore license. The financial institutions operating in Labuan are generally among the largest international banks and insurers. Nominee (anonymous) directors are not permitted for offshore banks, trusts or insurance companies. Labuan has 4,065 registered offshore companies, money banking companies, trusts, and insurance companies. Offshore companies must be established through a trust company. Trust companies are required by law to establish true beneficial owners and submit suspicious transaction reports as necessary. Bearer instruments likewise are prohibited in Labuan, but there is no requirement to reveal the true identity of the beneficial owner of international corporations. LOFSA officials may require any organization operating in Labuan to disclose information on its beneficial owner or owners.

As of December 2004, Labuan has 53 offshore banks in operation, along with 101 insurance and insurance-related companies, 59 leasing operations, 15 fund management groups, 30 trust companies, three money banking companies, and 2,348 offshore companies (both trading and non-trading). Many of the companies established in Labuan are Japanese firms established primarily to service Japanese companies in Malaysia. Malaysia bans offshore casinos and Internet gaming sites.

The Free Zone Act of 1990 is the enabling legislation for free trade zones in Malaysia. The zones are divided into Free Industrial Zones (FIZ), where manufacturing and assembly takes place, and Free Commercial Zones (FCZ), generally for warehousing commercial stock. The Minister of Finance may designate any suitable area as an FIZ or FCZ. Currently there are 13 FIZs and 14 FCZs in Malaysia. The Minister of Finance may appoint any federal, state or local government agency or entity as an authority to administer, maintain and operate any free trade zone. Legal treatment for such zones is also different. The time needed to obtain such licenses from the administrative authority for the given free trade zone depends on the type of approval. Clearance time ranges from 2-8 weeks. There is no information available suggesting that Malaysia's free industrial and free commercial zones are being used for trade-based money laundering schemes or by the financiers of terrorism. However, the GOM considers these zones as areas outside the country and receive with more lenient tax and customs treatment relative to the rest of the country. As such, the free trade zones are vulnerable to money laundering.

In April 2002, the GOM passed the Mutual Assistance in Criminal Matters Bill and, in 2004, Malaysia made its first arrest for money laundering. The GOM is currently prosecuting this case as well as investigating several others. Malaysia cooperates with regional, multilateral, and international partners to combat financial crimes and permits foreign countries to check the operations of their banks' branches. The FIU has signed Memoranda of Understanding (MOUs) with the FIUs of Australia, Indonesia, and the Philippines. MOUs with the United States, the United Kingdom, Japan, South Korea, the Netherlands, Finland, Albania, Thailand, and Argentina are pending.

Parliament passed amendments to the Anti-Money Laundering Act, the Subordinate Courts Act, and the Courts of Judicature act in November 2003. The Criminal Procedure code is the last major piece of domestic legislation that needs an amendment before the can be incorporated into domestic law. The

amendments to the AMLA, once enacted, will make the financing of terrorism one of the 168 predicate offenses for which money laundering can be charged as a crime but additional review mandated by Parliament has delayed the amendment's entry into force. A Select Committee is currently reviewing changes to The Criminal Procedure Code—the last major piece of domestic legislation that needs amending before being enacted in domestic law. When implemented, the 2003 amendments will increase penalties for terrorist acts, allow for the forfeiture of terrorist-related assets, allow for the prosecution of individuals who provide material support for terrorists, expand the use of wiretaps and other surveillance of terrorist suspects, and permit video testimony in terrorist cases. GOM officials expect the committee to conclude its review by July 2005 and Royal assent to follow shortly thereafter. Enactment of the amendment will enable the GOM to accede to the 1999 UN Convention for the Suppression of the Financing of Terrorism. Additionally, the Cabinet has approved, as policy, the ratification of all remaining counterterrorist conventions. Malaysia is a party to the 1988 UN Drug Convention.

Despite of the absence of legislation criminalizing terrorist financing, the GOM has cooperated closely with U.S. law enforcement in investigating terrorist-related cases since the signing of a joint declaration to combat international terrorism with the United States in May 2002. The GOM currently has the authority to identify, freeze terrorist or terrorist-related assets and 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 evidence of its willingness to cooperate internationally in the global effort to thwart terrorism, the Ministry of Foreign Affairs, in conjunction with Malaysia's anti-money laundering unit within the Central Bank, opened the Southeast Asian Region Centre for Counter-Terrorism (SEARCCT) in August 2003.

The GOM has rules regulating charities and other non-profit entities. The Registrar of Societies is the principal government official who supervises and controls charitable organizations, with input from the Inland Revenue Board and occasionally the Companies Commission. The Registrar mandates that every registered society of a charitable nature submits its annual returns, which include financial statements. Should the Registrar find activities he deems suspicious, he will inform the FIU of such activities. Negotiations are currently underway to expand the scope of AMLA reporting institutions to include charitable organization governed by the Registrar of Societies. Malaysia's tax law allows contributions to charitable organizations (Zakat, as required by Islam) to be deducted from one's total tax liability, encouraging the reporting of such contributions. Such contributions can be taken as payroll deductions, another tool to prevent the abuse of charitable giving.

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's FIU gained membership to the Egmont Group of Financial Intelligence Units in July 2003.

The Government of Malaysia continues to make a broad, sustained effort to combat money laundering and terrorist financing flows within its borders. For all entities such as trust companies and International Business Companies (IBCs), Malaysia should insist on "fit and proper tests" for all management, and identification of all beneficial owners. Malaysia should also insist on the registration of trusts and of the beneficial owners of the 4,000 International Business Companies, 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. Customs regulations and inspections should be strengthened, particularly in the free trade zones. Malaysia is a signatory to the UN Convention against Transnational Organized Crime, which came into force in September 2003. Malaysia should ratify that Convention. The Malaysian Parliament should enact terrorist financing legislation in 2005 and the GOM should accede to the UN International Convention for the Suppression of the Financing of Terrorism and to all other terrorist-related UN Conventions.

The Maldives

The Maldives is not an important regional financial center. The financial sector of the Maldives is very small, 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. The MMA has authority to supervise the banking system through the Maldives Monetary Authority Act. These laws and regulations provide the MMA with 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. Separate laws address the narcotics trade, terrorism, and corruption: Law No. 17/77 on Narcotic Drugs and Psychotropic Substances prohibits consumption and trafficking of illegal narcotics. The law also prohibits laundering of proceeds from the illicit 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 empowers judicial authorities to freeze accounts pending a court decision.

The Government of the Maldives is in the process of drafting anti-money laundering legislation, with IMF assistance. The government has recently set up a Financial Intelligence Unit (FIU) within the MMA. Currently, there are no laws or regulations governing the FIU. Regulations to cover the FIU are expected to be included in the new money laundering legislation.

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 of any such terrorist activity is unlawful. The MMA has issued “know your customer” directives and other instructions to banks, including freezing 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 directives 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 and to the 1999 UN International Convention for the Suppression of the Financing of Terrorism. The Maldives has not signed the UN Convention against Transnational Organized Crime.

The Government of the Maldives should enact comprehensive anti-money laundering and counterterrorist financing legislation that conforms to international standards. The legislation should include all regulations necessary to successfully establish the new Financial Intelligence Unit (FIU). The Maldives should also sign and ratify the UN Convention against Transnational Organized Crime.

Mali

Mali's per capita gross domestic product (GDP) of \$250 (2002) places it among the world's 10 poorest nations. Mali is not considered an important regional financial center nor is it experiencing an increase in financial crimes. Mali has no banks with offshore facilities. Drug trafficking is also not a significant problem in Mali. There is no evidence of Mali's financial institutions engaging in currency transactions involving narcotics-trafficking. Contraband cigarette smuggling originating in West Africa and transiting Mali is significant and includes arms smuggling as well. The smuggling operators are controlled by the Salafist Group for Preaching and Combat (GSPC)—a terrorist organization. Mali has an internal market for smuggled cigarettes and textiles, but these activities are primarily a way to avoid Malian customs duties and are not related to the narcotics trade. Other than the smuggling of contraband in Mali's north, no significant organized crime is known to exist in Mali.

Money Laundering and Financial Crimes

Drug smuggling, smuggling, and money laundering are all criminal offenses in Mali. Mali has introduced a new comprehensive banking law with international and European standards that will protect bankers and others with respect to their cooperation with law enforcement entities. The new banking law will, when enacted, also regulate the transfer of currency. The Malian National Assembly has not, as yet, ratified the new comprehensive law. Further, it is not among the list of laws to be discussed during the current session.

The National Assembly approved, during its Fall 2004 session, a new law on the growing role of banks in the economy and the spread of the use of bank notes among the population. The law's intention is not only to reduce the amount of currency used in financial transactions, urging the use of checks in its place, but also to encourage the use of the banking system. Bank secrecy is very limited in Mali. Mali routinely provides law enforcement authorities with client and ownership information in investigative cases. At present, Malian customs checks passengers at airports for certificates of exchange to ascertain if money exchange within the country was through a legal source.

Mali is part of the West African Economic and Monetary Union (WAEMU). All WAEMU countries have a monetary committee that reviews, records and reports significant currency transactions. In addition, all WAEMU country banks are required to maintain records necessary to reconstruct significant transactions for ten years and are required to report suspicious transactions on a regular basis.

Money laundering controls are also applied to non-banking financial institutions, such as exchange houses, stock brokerages, casinos, insurance companies, etc., as well as intermediaries such as lawyers, accountants, and broker/dealers. There have been no ramifications, to date, related to any changes in Mali's policies and laws related to money laundering and terrorist financing nor have banking or political groups objected. There have been no arrests or prosecutions for money laundering or terrorist financing in Mali to date.

Mali is not considered an offshore financial center. No offshore banks, international business companies, or other forms of exempt or shell companies or trusts exist in Mali. There are no free trade zones in Mali.

Smuggled property involved in international drug trade, money laundering, or terrorist financing in Mali can be seized and sold with the proceeds going to the government. Assets are frozen until the investigation is complete. The Malian public and political response to government efforts to seize and/or forfeit assets has been very supportive. The Malian banking community has been very cooperative with enforcement efforts to trace funds and seize bank accounts. Under a new Banking law, the Ministry of Economy and Finance would receive the proceeds from asset seizures and forfeitures. Mali has not enacted laws for the sharing of seized assets with other governments.

The Government of Mali strictly enforces existing drug-related asset seizure and forfeiture laws. The Ministry of Finance and the Ministry of Security are responsible for tracing and seizing assets. The GOM is severely under-manned, under-trained, and under-financed to trace and seize assets adequately. Mali's law enforcement organizations operate independently of each other with little to no coordination. The police narcotics department, Gendarme, Customs and border police seized drugs during 2003 and 2004. The GOM did not keep records of previous years' seizures; however, GOM officials feel that the problem continues to be small. When asked, Mali has been cooperative and supportive of efforts by the USG and other countries to trace and seize assets; however, there is little coordination relating to drug interdiction between Mali and its neighbors.

Mali is a key regional partner in the global war on terrorism. Terrorism and terrorist financing are considered serious crimes in Mali. The GOM has the authority to identify, freeze, and seize terrorist finance related assets. The Ministry of Finance has circulated the names of suspected terrorists and terrorist organizations to Malian financial institutions. To date, no assets have been identified in Mali.

While the hawala system exists in Mali, it is primarily used for salary transfers of Malians working abroad. A Committee of Malians finances salaries to Malian families; in exchange, the foreign salaries earned are used to buy French commercial goods. Not all Malians use the banking system because some work abroad without legal work permits and are forced to repatriate funds through non-traceable means. The financial sector is making efforts to explain the safety of banks to thwart the misuse of charitable and/or non-profit entities that might be used as conduits for the financing of terrorism.

Mali has entered into bilateral agreements between BCEAO (Central Bank of West African States) countries for the exchange of information on money laundering. The countries include: Cote d'Ivoire, Senegal, Togo, Burkina Faso, Guinea Bissau, Niger, and Benin. The GOM has no specific agreement with U.S. authorities on a mechanism for exchanging records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing and other serious crime investigations; however, international agreements pledge Mali to share information in such cases. Mali has not entered into any relevant bilateral treaties, agreements, or other mechanisms for information exchange with the United States.

Mali is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. In November 2000, Mali was one of 14 West African countries to attend a meeting to establish the Intergovernmental Action Group against Money Laundering (GIABA).

The Government of Mali should enact and fully implement comprehensive anti-money laundering legislation that comports with international standards. Additionally, it should ensure appropriate law enforcement personnel are trained and able to perform their duties.

Malta

Malta joined the European Union (EU) on May 1, 2004. As part of its preparation for this event, Malta strengthened its regulatory regime and introduced measures to attract European investors and 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.

Since 1997, Malta has been closing the loopholes on all offshore financial activities. All licenses for offshore registered businesses expired on September 30, 2004, completing Malta's transition from an economy with over 400 international business corporations in 2001 to a country where offshore banking and business is no longer legal. Companies and trusts are now fairly well regulated, and international entities are subject to 35 percent tax. Bearer shares or anonymous accounts are no longer permitted in Malta.

The Government of Malta (GOM) criminalized money laundering in 1994. Maltese law imposes a maximum punishment of approximately \$2.5 million and/or 14 years in prison for those convicted of money laundering crimes. Also in 1994, the GOM issued the Regulations for the Prevention of Money Laundering, applicable to financial and credit institutions, life insurance companies, and investment and stock brokerage 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 August 2003, a new set of regulations combined the 1994 money laundering law and the Second EU Directive on the Prevention of Money Laundering, and became the national law, which expands anti-money laundering requirements to designated non-bank financial businesses and professions.

The Maltese Financial Services Authority (MFSA) is the regulatory agency responsible for licensing new banks and financial institutions; additionally the MFSA has been responsible for monitoring financial transactions going through Malta since the supervisory function of the Central Bank of Malta

was passed to the MFSA in 2002. Recently the MFSA widened its regulatory scope to encompass banking, insurance, investment services, company compliance, and the stock exchange. The MFSA has a rigorous process of analyzing companies prior to granting a license. This entails detailed analyses of all the applications it receives, including information about the directors and other persons involved in the management of the company.

In December 2001, Malta's parliament established the Financial Intelligence Analysis Unit (FIAU) through an amendment to the Prevention of Money Laundering Act, 1994, to serve as Malta's Financial Intelligence Unit (FIU). The unit became fully functional in October 2002. The FIAU is independent and has a board that consists of members nominated by the Central Bank of Malta, the MFSA, the Police, and the Attorney General. Board members are not subject to the direction or control of their parent agency or any other authority.

The FIAU co-ordinates the fight against money laundering, collects information from financial institutions, and liaises with parallel international institutions as well as the MFSA and the GOM Police. The GOM requires banks, bureaux de change, stockbrokers, insurance companies, money remittance/transfer services, and other designated non-bank financial businesses and professions to file suspicious transaction reports (STRs) with the FIAU, which investigates them. The FIAU also conducts organized training sessions for Maltese financial practitioners to make them aware of their responsibilities.

The FIAU is leading an initiative to consolidate all guidance notes for all of the covered financial services and other businesses. In 2003, the FIAU, together with the Banking Unit at the MFSA, updated the Guidance Notes for Credit and Financial Institutions issued by the Central Bank of Malta in 1996.

STRs are not required to be filed for subjects suspected of negligence; only intentional and willful blindness offenses are penalized in Malta. The FIAU received 76 STRs in 2003 and 46 STRs in 2004. Stronger enforcement should continue as the FIAU continues analyzing STRs for referral for police investigation. Malta has also moved to bolster the prosecutorial opportunities for financial crime. 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.

In January 2002, the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) conducted a second round mutual evaluation of the overall effectiveness of the Maltese anti-money laundering system and practices, including compliance with the FATF Special Recommendations on Terrorist Financing. The review found that Malta was in partial compliance with Special Recommendation No. 1 (ratification and implementation of UN instruments), because it had signed and ratified the pertinent UN Conventions, but had not yet fully implemented UNSCRs 1269, 1373, and 1390.

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 UNSCR 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 reportedly 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.

Malta is a founding member of the MONEYVAL and chaired the committee until December 2003. The FIAU became a member of the Egmont Group in July 2003. Malta is no longer a member of the Offshore Group of Banking Supervisors, but has joined the International Organization of Securities Commissions (IOSCO). Malta is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism. Malta has ratified the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and the Council of Europe European Convention on the Suppression of Terrorism, and has amended its criminal code to be in alignment with these conventions.

The Government of Malta should continue to enhance its anti-money laundering regime; in particular, Malta should adopt reporting requirements for cross-border currency transportation, including the reporting of international wire transfer activity, and should enact a safe harbor provision to protect those who report suspicious activity in accordance with GOM requirements.

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 60,000. The financial system in RMI has total banking system assets of \$90 million and total deposits of \$76 million, with domestic deposits exceeding 50 percent of the gross domestic product. The RMI financial sector consists of two commercial banks, one of which is insured by the Federal Deposit Insurance Corporation (FDIC), and a government-owned development bank whose primary function is to perform development lending in government-prioritized sectors; there are also 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. Among other initiatives, the reform program called for the establishment of the requisite infrastructure for detecting, preventing, and combating money laundering and terrorist financing.

The Marshall Islands has not seen an increase in financial crime in recent years. There have not been any prosecutions for money laundering. However, an evolving trend that poses a challenge to RMI's anti-money laundering/counterterrorist financing effort is the significant outflow of cash, generally attributed to expatriate businesses sending proceeds out of the country. There is currently no requirement to report cross-border currency transfers. The government is proposing an amendment to the Banking Act, that would address the problem.

Money laundering has been 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. The substantial and comprehensive effort to align the Marshall Islands' anti-money laundering regime with international standards, including the adoption of new laws, a new regulatory scheme, and the establishment of a Financial Intelligence Unit (FIU), resulted in its removal from the Financial Action Task Force's (FATF's) Non-Cooperating Countries and Territories list in 2002.

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 has the power to receive, analyze, and disseminate financial intelligence. In

2003, its processes were streamlined and automated to the fullest extent possible, given the limited resources available to the DFIU.

In May 2002, the GRMI 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. Money laundering controls extend to all financial institutions, but do not cover professionals, i.e., lawyers and accountants. However, individuals can be held liable for money laundering violations by their institutions.

Under the Banking Amendment, the Proceeds of Crime Act, and the Count-Terrorism Act, the RMI can freeze, seize, and upon conviction transfer to the general fund, the proceeds of any crime that results in a one-year or greater sentence. Provisions allow for a broad range of forfeiture: any real or personal property owned by the person, any property used in the crime, and any proceeds of the crime. The Mutual Assistance Act allows the transfer to a requesting government of proceeds of such a crime committed in a foreign country. The Counter-Terrorism Act provides for the closing of any businesses involved in exporting or importing terrorist funds or supplies. These laws allow for both civil and criminal forfeiture. Although the laws are designed to meet the GRMI's international obligations, their effectiveness has not been tested, as there has been no terrorist activity in the RMI and therefore no seizures.

Depending on the nature of the offense, the Attorney General or the Banking Commission would be responsible for enforcement and for seizures of assets. Police powers are adequate, but resources are limited. However, the GRMI retains a close relationship to U.S. institutions and could call on them for assistance in cases of concern to the United States. Assets can be frozen "without undue delay."

Since the passage of its anti-money laundering law, and a suite of counterterrorism laws, as well as the subsequent promulgation of implementing regulations, the GRMI has undertaken a number of initiatives to further strengthen its anti-money laundering/counterterrorist financing (AML/CFT) regime. The government and local institutions have received positive reports from FATF.

However, a very significant problem has resulted from efforts to comply with AML/CFT requirements. This issue is causing a system-wide disturbance in banking and more specifically in transaction settlement and clearance. The Bank of the Marshall Islands (BOMI), in an effort to assure full compliance, commissioned an internal audit of its procedures and controls in 2003. The results of that audit identified several weaknesses which BOMI has taken steps to correct. However, the existence of the audit, and fears of sanctions under the Bank Secrecy Act and the USA PATRIOT Act, have led Citizens Security Bank of Guam to discontinue its "payable through" relationship with BOMI, effective February 15th, 2004. Suspension of "payable through" will mean BOMI checks cannot be used outside the country. This situation has the potential to disrupt that status quo in the business community. It will also mean that the second largest population center, Ebeye, will have no banking services available for international transactions, as there is no Bank of Guam branch on Ebeye.

The RMI offshore financial sector is vulnerable to money laundering. Nonresident corporations (NRCs), the equivalent of international business companies, can be formed. Currently, there are 5,500 registered NRCs, half of which are companies formed for registering ships. 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. The corporate registry program, however, does not allow the registering of offshore banks, offshore insurance firms, and other companies which are financial in nature.

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 nonresident trusts, partnerships, unincorporated associations, and domestic and foreign limited liability companies. Offshore banks and insurance companies are not permitted in the Marshall Islands.

Having established the requisite supervisory processes to ensure compliance with legislative mandates for detection and suppression of money laundering and terrorist financing, the GRMI's main emphasis in 2003 was on fine-tuning these processes. After undertaking nine on-site examinations of financial institutions, following procedures developed in cooperation with the FDIC, the Banking Commission has now gained a better understanding of the risk profile of these institutions with respect to their exposure to money laundering and terrorist financing. This has proven especially useful in amalgamating some supervisory processes with the routine FIU processes, thereby maximizing benefit for the limited resources available to the GRMI. The Banking Commission had planned that some of the supervisory processes would be incorporated into the required annual audits of banks, but this initiative was not completed in 2003; it was to be continued in 2004. In 2003, the Banking Commission recruited an Assistant Commissioner who will spearhead this task along with other examination tasks relating to anti-money laundering compliance and prudential banking practices.

The GRMI has enacted a Proceeds of Crime Act, Counter-Terrorism Act, and Foreign Evidence Act. Although the GRMI is not a signatory to the UN Vienna Convention on Drug Trafficking, RMI has acceded to all 12 major multilateral conventions and protocols related to states' responsibilities for combating terrorism under the International Convention for the Suppression of the Financing of Terrorism.

The Marshall Islands is a member of the Asia/Pacific Group on Money Laundering. The DFIU became a member of the Egmont Group 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 Government of the Republic of the Marshall Islands (GRMI) continues to strengthen its key defenses against money laundering and terrorist financing, and has commenced work aimed at aligning its anti-money laundering system with the revised 40 recommendations of the Financial Action Task Force on Money Laundering. These tasks are highlighted in the draft Fourth Anti-Money Laundering Implementation Plan, covering the period from 2004 onward. The Republic of the Marshall Islands should accede to the 1988 UN Drug Convention. Additionally, the Marshall Islands should require the identification of the beneficial owners of Non-resident Corporations.

Mauritania

Mauritania is not a regional financial center. Its economic system suffers from a combination of weak Central Bank oversight, lax financial auditing standards, porous borders, and corruption in government and the private sector. Mauritania is a transit country for a variety of smuggled goods, including cigarettes, diverted food aid, small arms, clandestine immigrants. Government officials acknowledge that money laundering occurs in Mauritania, but most involves profits from graft and small-scale illicit

activity. Terrorism financing and narcotics proceeds are believed to constitute a small portion of the sums laundered in Mauritania.

Money laundering occurs on a small scale within local banks. Money laundering is a criminal offense in Mauritania. The main law governing money laundering, enacted in 1992, focuses specifically on laundering from narcotics-trafficking. The Government of Mauritania (GOM) is drafting a new body of laws that, when enacted, will strengthen Government control over money laundering related to terrorist groups and activities. Banks are currently required to record and report to the Central Bank the identity of customers engaging in large-scale financial transactions. The GOM did not arrest or prosecute anyone for money laundering or terrorist financing activities in 2004.

Mauritania is a party to the 1988 UN Drug Convention, acceded to the International Convention for the Suppression of the Financing of Terrorism, and has also ratified the Organization of African Unity Convention on the Prevention and Combating of Terrorism of July 1999.

Mauritania is not an offshore financial center; nor are there free trade zones in Mauritania, although the GOM does grant tax relief to certain small-scale export sectors of the economy.

The Government has demonstrated a willingness to cooperate with the United States on combating terrorist financing and related issues, but local efforts are hampered by a serious lack of resources, knowledge, and expertise in this area. Law enforcement and judicial procedures and systems for identifying and freezing assets related to illegal activity are, at best, still in their initial phases. Although no significant legal loopholes exist to allow traffickers or terrorist financiers to shield assets, such loopholes are not really necessary given the very weak enforcement of current money laundering laws.

The GOM recently created an economic-crimes investigation unit that is specifically designed to investigate financial crimes such as corruption and money laundering, but this unit is in its very early developmental stages and does not appear to be receiving the resources needed to be effective over the long term.

The Government of Mauritania should enact anti-money laundering that includes all serious crimes and should enact counterterrorist financing legislation that comport with international standards.

Mauritius

Mauritius is a developing financial hub and a major route for foreign investments into the Asian sub-continent. Officials of the Government of Mauritius (GOM) indicate that the majority of money laundering in Mauritius takes the form of schemes aimed at channeling illicit proceeds through both domestic and offshore banks.

Money laundering is a criminal offense in Mauritius. In February 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. Mauritius plans to expand the reporting obligation to real estate agents, dealers in precious gems, and horse racing bookmakers. In 2004, most of the suspicious activity reports being filed came from the offshore sector.

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. Since its inception, the FIU has developed into a fully functioning organization. The FIU was admitted to the Egmont Group in 2003. Its major challenge continues to be the development of an information technology structure to store SARs, perform complex analyses on them, and provide accessibility to the SARs to other law enforcement entities. As of November 2004, the FIU had received a total of 300 SARs, of which 100 had been referred to the ICAC. The FIU would like to put in place a system that will allow for the on-line submission of SARs. It would also like to develop partnerships with local and regional institutions involved in anti-money laundering and the prevention of terrorist financing activities.

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 the regulation, which includes the licensing, of the non-bank financial sector. All applications to form offshore companies (now called global business companies or GBCs) 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 GBCs.

The Prevention of Terrorism Act of 2002 was promulgated in Mauritius on February 19, 2002. This legislation criminalizes terrorist financing. The legislation gives the GOM 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 and to both the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Mauritius is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. In August 2003, representatives from Mauritius attended the ESAAMLG sixth meeting of the Task Force in Uganda. Mauritius also completed the first round of ESAAMLG mutual evaluations in 2003. In August 2004, Mauritius hosted the Fourth Meeting of the Council of Ministers of the ESAAMLG, and Minister Sushil Khushiram of the GOM Ministry of Industry, Financial Services and Corporate Affairs, was appointed Chairman of the ESAAMLG. Mauritius is a member of the Offshore Group of Banking Supervisors.

The Government of Mauritius should continue to take a leadership role in regional outreach through the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG). It should also continue to take an active role within the Egmont Group.

Mexico

The illicit drug trade continues to be the principal source of funds laundered through the Mexican financial system. Mexico is a major drug producing and drug-transit country. Mexico also serves as one of the major conduits for proceeds from illegal drug sales leaving the United States. 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.

Currently, there are 32 commercial banks and 80 foreign financial representative offices operating in Mexico, with seven commercial banks representing 88 percent of total assets in the banking sector. Commercial banks, foreign exchange companies, and general commercial establishments are allowed to offer money exchange services. Mexico has 81 insurance companies, one mutual insurance company, 13 bonding institutions, 211 credit unions, and 28 money exchange houses. The size of the

Money Laundering and Financial Crimes

underground economy is unknown, although it is estimated to account for anywhere between 20 and 40 percent of the gross domestic product in Mexico. While casinos are not permitted in Mexico, gambling is legally allowed through national lotteries, horse races, and sport pools.

Remittances from the United States to Mexico are at an all-time high, and are expected to have exceeded \$14 billion in 2004. Although non-bank companies continue to dominate the market for remittances, many U.S. banks have teamed up with their Mexican counterparts to develop systems to simplify and expedite the transfer of money. These measures include wider acceptance by U.S. banks of the *matricula consular*, an identification card issued by Mexican consular offices to Mexican citizens residing in the United States that has been criticized, based on security issues. In some cases, neither the sender nor the recipient of a remittance is required to open a bank account in the United States or Mexico, but must simply provide the *matricula consular* as identification and pay a flat fee. Although these systems have been designed to make the transfer of money faster and less expensive for the customers, the rapid movement of such vast sums of money by persons of questionable identity leaves the new money transfer systems open to potential money laundering and exploitation by organized crime groups.

According to U.S. law enforcement officials, Mexico remains one of the most challenging money laundering jurisdictions for the United States, especially with regard to the investigation of money laundering activities involving the cross-border smuggling of bulk currency from drug transactions. While Mexico has taken a number of steps to improve its anti-money laundering system, significant amounts of narcotics-related proceeds are still smuggled across the border. In addition, such proceeds can still be introduced 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 to implement 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, stock markets, and credit institutions) to know and identify customers and maintain records of transactions. These entities must report suspicious transactions, transactions over \$10,000, and transactions involving employees of financial institutions who engage in unusual activity.

Financial institutions with a reporting obligation now require occasional customers performing transactions equivalent to or exceeding \$3,000 in value to be identified, so the transactions can be aggregated daily to prevent circumvention of the requirements to file cash transaction reports (CTR) and suspicious transaction reports (STR). Financial institutions also have implemented programs for screening new employees and verifying the character and qualifications of their board members and high-ranking officers.

In 2001, Mexico established STR requirements for the smaller foreign exchange houses that process most of the remittances from Mexican workers in the United States, and in May 2004 reporting requirements for all exchange houses and money remittance businesses entered into effect. Legislation enacted in 2004 also expanded reporting requirements to many peripheral financial entities, such as real estate brokerages, attorneys, notaries, and accountants. Current provisions do not include reporting requirements for offshore banks or casinos.

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. Mexico's reporting requirements included a wider range of monetary instruments (e.g. bank drafts) than those of the United States. In 2004 alone over \$14 million in unreported funds were seized at Mexican airports in joint operations with the United States. In the first operation, inspectors seized some \$13 million in drug-related currency in Mexico. In the second operation, inspectors seized \$1.5 million and provided leads to colleagues in other countries that resulted in the seizure of another \$1.5 million in drug-related currency.

In 1997, the GOM established a financial intelligence unit, the Dirección General Adjunta de Investigación de Operaciones (DGAIO), under the Secretariat of Finance and Public Credit (Hacienda). The Hacienda expanded the authority of the DGAIO in 2004 by consolidating all of the Hacienda offices responsible for investigating financial crimes into the DGAIO, which has since been renamed the Unidad de Inteligencia Financiera (Financial Intelligence Unit, or UIF). In addition to its previous responsibilities as the DGAIO, the UIF also reviews all crimes linked to Mexico's financial system and examines the financial activities of public officials. The UIF's personnel now number 70—most of whom are forensic accountants, lawyers, and analysts. The director reports to the Minister of Finance. The UIF received an average of 500 STRs and 2,500 CTRs per month in 2004.

Following the analysis of CTRs and STRs, the UIF sends reports that are deemed to require further investigation, and have been approved by Hacienda's legal counsel, to the Office of the Attorney General (PGR). As of November, the UIF had sent 63 cases to the PGR in 2004, and 476 since its inception in 1997. As part of a more comprehensive approach to fighting organized crime, the PGR incorporated its special financial crimes unit—which has the authority to initiate, coordinate, and determine the course of preliminary financial crimes inquiries—into the Office of the Deputy Attorney General for Organized Crime (SIEDO). The UIF works closely with SIEDO in carrying out money laundering investigations. In addition to working with SIEDO, UIF personnel have initiated working-level relationships with other federal law enforcement entities, including the Federal Investigative Agency (AFI), in order to support the investigations of criminal activities with ties to money laundering.

In September 2003, Mexico underwent its second Mutual Evaluation by the FATF, and the findings of the evaluation team were accepted at the FATF plenary meetings in June 2004. The evaluation team found that the GOM had made progress since the first mutual evaluation by removing specific exemptions to customer identification obligations, implementing on-line reporting forms and a new automated transmission process for reporting transactions to the UIF, and slightly reducing the delay in reporting transactions overall. The GOM also developed an overall anti-money laundering strategy and plan.

However, the FATF evaluation team also identified a number of deficiencies in the system. Mexico does not have a separate offense of terrorist financing. Bank and trust secrecy continue to impede many aspects of Mexico's anti-money laundering/counterterrorist financing system, particularly for law enforcement and prosecutorial and judicial authorities during investigations and prosecutions. With regard to lifting bank secrecy, although customers are notified, the National Banking and Securities Commission (CNBV) must approve any requests for bank secrecy to be lifted during an investigation. The approval of such a request by the CNBV cannot be challenged, and financial institutions must respond with the required information within three days. If the CNBV does not approve the request, prosecutors must request a judicial order to lift bank secrecy, and the account holder may challenge the judge's decision. Limited co-ordination among key government institutions and procedural barriers impede effective money laundering prosecution.

Money Laundering and Financial Crimes

In November 2003, the Senate passed proposed amendments to the Federal Penal Code that would link terrorist financing to money laundering. This legislation, once passed by the lower house of Congress, will bring Mexico into compliance with international standards. The proposed amendments also create two new crimes: conspiracy to launder assets, and international terrorism (when committed in Mexico to inflict damage on a foreign state). The legislation has not yet been passed, and it is unlikely that this will occur prior to the second half of 2005.

The lack of significant legislation criminalizing the financing of terrorism places Mexico in a position of noncompliance with the FATF Special Recommendations on Terrorist Financing and the UNSCR 1373 requirements. However, because terrorism is declared to be a serious crime, money laundering associated with terrorism is punishable under the existing Penal Code. The GOM has responded to U.S. Government (USG) efforts to identify and block terrorist-related funds, and, although no assets were frozen, it continues to monitor suspicious financial transactions.

Although the United States and Mexico both have forfeiture laws and provisions for seizing assets abroad derived from criminal activity, USG requests to Mexico for the seizure, forfeiture, and repatriation of criminal assets have not met with success, as Mexican authorities have difficulties with assets seized for forfeiture in Mexico if these assets are not clearly linked to narcotics. Most assets seized during law enforcement operations go to the Service for the Management and Transfer of Assets (SAE), a semi-autonomous branch of the Hacienda established in late 2002. Although Mexican officials have made significant progress in modernizing their approach to asset seizure, actual asset forfeiture remains a challenge. In two significant U.S. cases involving fraud, authorities seized real property and money generated from the crime. Although authorities gained forfeiture of the property in the United States, counterparts in Mexico did not carry out such orders in Mexico, nor have they returned related assets to the United States for forfeiture.

Mexico has developed a broad network of bilateral agreements with the United States, and regularly meets in bilateral law enforcement working groups with the United States. The GOM and the 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.

The United States temporarily suspended information exchange with Mexico in April 2004. Financial intelligence provided to the UIF by the U.S. financial intelligence unit (the Financial Crimes Enforcement Network, or FinCEN) was disseminated by the GOM without prior USG authorization. The unauthorized disclosure of sensitive financial information was done in breach of the well established and clearly defined protocols of FinCEN, as well as the principles of the Egmont Group—of which both the United States and Mexico are members—for information exchange. Information exchange resumed in June 2004 after Mexico substantially implemented a number of measures to ensure that information is disseminated to appropriate government agencies in a manner that protects its confidentiality and warns of the consequences of unauthorized disclosure.

In addition to its membership in the FATF, Mexico participates in the Caribbean Financial Action Task Force as a cooperating and supporting nation and in the South American Financial Action Task Force as an observer member. Mexico is a member of the Egmont Group and the OAS/CICAD Experts Group to Control Money Laundering. The GOM is a party to the 1988 UN Drug Convention. In 2003, the GOM ratified several other international treaties, including the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the Inter-American Convention Against Terrorism. The GOM ratified the UN Convention against Corruption in July 2004.

The Government of Mexico should fully implement and improve the mechanisms for asset forfeiture and money laundering cooperation with the United States, and should increase efforts to control the bulk smuggling of currency across its borders. Mexico should also closely monitor remittance systems for possible exploitation by criminal or terrorist groups. Mexico should enact its proposed legislation to criminalize the financing and support of terrorists and terrorism. Furthermore, despite the preventive mechanisms that have been put in place, improved cooperation among law enforcement authorities and a strong public campaign against corruption, Mexico continues to face challenges in prosecuting and convicting money launderers, and should continue to focus its efforts on improving its ability to do so.

Micronesia

The Federated States of Micronesia (FSM) is a sovereign state in free association with the United States. The FSM is not a regional financial center. It is not known to be a significant money laundering location and there has been no known money laundering related to narcotics proceeds or terrorist financing. Misuse of public funds has generated illicit proceeds and led to a number of indictments and convictions of politicians and their associates, including on money laundering charges. There may be limited financial crimes outside the formal banking sector by cash dealers involved in sending remittances to the home countries of some foreign workers. Financial crimes are rare in the commercial sector. The FSM's distance from other countries and sparse transportation links to the outside world seem to have limited the amount of contraband brought into the FSM. The market for smuggled goods is not developed.

There are three financial institutions in the nation: the Bank of Guam, the Bank of the FSM, and the FSM Development Bank. The FSM Development Bank is a non-depository institution owned and financed by the FSM National Government. The Bank of Guam is chartered in the U.S. and falls under U.S. regulations and the Federal Deposit Insurance Corporation (FDIC). The locally chartered Bank of the FSM is the only non-U.S. bank insured by the FDIC. As a result, these two commercial institutions are subject to supervision by the FSM Banking Board as well as to inspection and regulation by the FDIC. The Banking Board has made the development and monitoring of anti-money laundering and anti-financing of terrorism activities one of its top priorities. There are no off-shore financial centers, banks, trusts, shell banks, casinos, or free trade zones in the FSM.

Money laundering is a criminal offense under the Money Laundering and Proceeds of Crime Act, in effect since 2001 and favorably reviewed by the IMF Legal Department. The Act criminalizes money laundering and provides for the freezing and seizure of assets, including substitute assets. It incorporates due diligence provisions. Predicate crimes include all serious offenses punishable by imprisonment of more than one year. The law also provides for collection of financial information and intelligence and international cooperation in money laundering matters. Officials and private individuals from Chuuk State were arrested on money laundering charges, related to misuse of government assets in 2004. The FSM Attorney General's office is developing revisions to the legislation to tighten requirements for record keeping, establish cross-country currency reporting requirements, address non-bank establishments, and allow civil as well as criminal actions for forfeiture to bring the statutes into better compliance with international standards. These changes are scheduled to be submitted to Congress in May 2005.

The FSM Department of Justice has established procedures for regular notification to the Banking Board of the names of suspected terrorist individuals and organizations. No assets of individuals or entities have been seized or frozen. The government recognizes the existing of alternative remittance systems for expatriate workers from the Philippines, but does not have resources to monitor this activity. The FSM is a party to the UN International Convention for the Suppression of the Financing of Terrorism. New counterterrorism legislation is under development; the draft is expected to be sent

to Congress in May 2005; in lieu of these statutes, the FSM would apply the current money laundering law against terrorist financing.

Legislation to enhance 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. The FSM has cooperated with U.S. law enforcement agencies. The FSM is a party to the 1988 UN Drug Convention.

The Government of the Federated States of Micronesia should continue to enhance its anti-money laundering regime by criminalizing terrorist financing and adopting and implementing pending laws and regulations.

Moldova

Moldova is not considered an important regional financial center. It is a transit country, but the extent of related money laundering is unknown. As Moldova continues to suffer from severe economic conditions, proceeds from narcotics transactions remain small and incomes are generally low. Criminal proceeds laundered in Moldova are derived substantially from foreign criminal activity and, to a lesser extent, domestic criminal activity and corruption. A rise in Internet-related fraud schemes is evident. Although a significant black market exists in Moldova for a number of goods, narcotics proceeds are not a significant funding source. Instances of money laundering have occurred in the banking system. Domestic and foreign organized crime syndicates are believed to control most money laundering proceeds, and Government of Moldova (GOM) authorities are not known to encourage or facilitate laundering of proceeds from criminal or terrorist activity. While currency transactions involving laundered proceeds may include U.S. currency (counterfeit or genuine), regional organized crime activities likely account for the majority of profits.

Money laundering became a criminal offense in November 2001, and the law was amended in June 2002. It remained unchanged when the new criminal code was adopted in June 2003. The legislation applies to proceeds of “all crimes,” not just narcotics activity, with banks and non-bank financial institutions (NBFIs) required to report transactions over a certain amount to the Center for Combating Economic Crimes and Corruption (CCECC). On July 1, 2004, the Law on Money Laundering was amended to raise the reporting threshold from 100,000 lei to 300,000 lei for individuals, and from 200,000 lei to 500,000 for legal entities. However, the amendments still require reporting transactions under the threshold if, when combined with other transactions during a one-month period, they reach a total which crosses that threshold. This amendment may actually increase the amount of reporting required. Current anti-money laundering legislation also covers gold, gems, and precious metals, and any person involved in laundering money.

Banks must maintain transfer records for a period of five years after an account opens or after any financial transaction takes place and seven years after foreign currency contract transactions, whichever is later. Suspicious transactions have been reported, as required, since the law was enacted. Both banks and NBFIs are protected from criminal, civil, and administrative liability asserted as a result of their compliance with the reporting requirements, and no secrecy laws exist that would prevent law enforcement or banking authorities from accessing financial records. A May 2003 amendment states that forwarding such information to law enforcement entities or the courts is not a breach of confidentiality, as long as it is done in accordance with the regulations. Current legislation contains provisions authorizing sanctions of commercial banks for negligence. GOM efforts against the international transportation of illegal-source currency and monetary instruments largely focus on cross-border currency reporting forms, completed at ports of entry (POE) by travelers entering Moldova.

The CCECC serves as Moldova's Financial Intelligence Unit (FIU). In 2004, the CCECC created a money laundering section of ten investigators to pursue suspicious financial transactions. According to Moldovan authorities, there are currently 11 full-fledged criminal investigations underway for money laundering, and 36 preliminary investigations that have been completed and recommended for opening full-fledged investigations. (Under Moldovan criminal procedure, cases first undergo a preliminary investigation by operative investigators before being sent to criminal investigators and prosecutors who decide whether a full investigation will be launched.) The CCECC identified a list of non-resident companies suspected of involvement in money laundering and asked all banks to report any transactions done by these entities in order to prevent illegal transactions. While banks were initially resistant toward money laundering legislation, they have since adopted compliance programs as required by the law. However, Moldova remains predominantly a cash society as people have little trust in banks. This makes money laundering investigations difficult.

Moldova is not considered an offshore financial center, and only two foreign banks exist in Moldova: "Banca Comerciala Romana," a Romanian bank; and "Unibank," in which the Russian bank "Petrocomert" holds 100 percent of the shares. These banks are regulated in the same manner as Moldovan commercial banks. Offshore banks are permitted, so long as they are licensed by the NBM and background checks are conducted on shareholders and bank officials. Nominee (anonymous) directors are not allowed, and banks do not permit bearer shares. The Ministry of Finance (MOF) currently licenses five casinos, although they are reportedly not well regulated or controlled.

Article 106 of the Moldovan criminal code, enacted June 12, 2003, relates specifically to asset seizure and confiscation. The article, titled "Special Seizures," describes a special seizure as the forced transfer of ownership of goods used during, or resulting from a crime to the state. The article may be applied to goods belonging to persons who knowingly accepted things acquired illegally, even when prosecution is declined. However, it remains unclear whether asset forfeiture may be invoked against those unwittingly involved in or tied to an illegal activity. Money laundering crimes are the purview of the CCECC, while narcotics-related seizures are within the jurisdiction of the Ministry of Interior (MOI). The GOM currently lacks adequate resources, training, and experience to trace and seize assets effectively.

Moldova codified the criminalization of terrorist financing in the Law on Combating Terrorism, enacted November 12, 2001. Article 2 defines terrorist financing, and Article 8/1 authorizes suspension of terrorist and related financial operations. Current GOM capabilities to identify, freeze, and seize terrorist assets are rudimentary, with investigators lacking advanced training and resources. While the National Bank of Moldova (NBM) receives updated lists of suspected terrorists, no al-Qaida or Taliban related assets have been identified, frozen, or seized in Moldova. No hawala system exists in Moldova. Investigation into misuse of charitable or non-profit entities is non-existent, as the GOM has neither the resources nor ability to perform these tasks. In December 2004, the Parliament amended the law on money laundering to include provisions on terrorist financing. Moldova has made no arrests for terrorist financing.

No agreements, bilateral or otherwise, exist between the USG and the GOM regarding the exchange of records in connection with narcotics, terrorism, terrorist financing, or other serious criminal investigation. No negotiations are underway to establish such a mechanism. Current legislation does not prohibit cooperation on a case-by-case basis. GOM authorities continue to solicit USG assistance on individual cases and cooperate with U.S. law enforcement personnel when presented with requests for information/assistance. There are no known cases of GOM refusal to cooperate with foreign governments or of sanctions or penalties being imposed upon the GOM for a failure to cooperate. Moldova is a party to the 1988 UN Drug Convention, the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime, and the UN International Convention for the Suppression of the Financing of Terrorism, and cooperates in accordance with these agreements where resources and abilities permit. In addition to these, Moldova has signed an

agreement with CIS member states for the exchange of information on criminal matters, including money laundering. In 2004, the CCECC was accepted as an observer at the Eurasian Group on Combating Money Laundering and as a candidate in the Egmont Group.

The Government of Moldova should continue to enhance and implement its anti-money laundering/counterterrorist financing regime. Moldova should ensure full implementation of its laws and improve the mechanisms for sharing information and forfeiting assets. Additionally, the Moldova should provide appropriate training for its law enforcement personnel and officials involved in the asset forfeiture program.

Monaco

The Principality of Monaco is considered vulnerable to money laundering due to its strict bank secrecy laws, network of casinos, and unregulated offshore sector. The principality does not face the ordinary forms of organized crime, and the crime that does exist does not seem to generate significant illegal proceeds (save for fraud and offenses under the Law on Checks); rather, money laundering offenses relate mainly to offenses committed abroad. Russian organized crime and the Italian Mafia reportedly have laundered money in Monaco. Monaco remains on an OECD list of so-called “non-cooperative” countries in terms of provision of tax information.

Monaco is the smallest country in Europe, after the Vatican. There are approximately 70 banks and financial institutions in Monaco, with more than 300,000 accounts (with a population of about 7,000 Monegasque nationals and another 25,000 foreign residents). Approximately 85 percent of the banking customers are nonresident. In 2002, the financial sector represented over 17 percent of Monaco’s economic activity. The non-banking financial institutions include insurance companies, portfolio management companies, and trusts created through notaries, of which there are three, all nominated by the Prince. Accountants and the 25 legal professionals in the country are also included in the non-banking category. The real estate sector is another important area because of the high prices for land throughout the principality. There are also four casinos run by the Société des Bains de Mer (with a state-owned majority interest).

Monaco’s banking sector is linked to the French banking sector through the Franco-Monegasque Exchange Control Convention signed in 1945 and supplemented periodically, most recently in 2001. Through this convention, Monaco uses the banking legislation and regulations issued by the French Banking and Financial Regulations Committee, including Article 57 of France’s 1984 law regarding banking secrecy. Most of Monaco’s 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 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.

Although the French Banking Commission is the supervisor for Monegasque institutions, Monaco shoulders its own responsibility for legislating and enforcing measures to counter money laundering and terrorism financing. Thus, though the rules are the same for both countries, the degree of enforcement may vary. The Finance Councilor (within the Government Council) is responsible for anti-money laundering implementation and policy. Money laundering in Monaco is a criminal offense. It is criminalized by Act 1.162 of 7 July 1993, “On the Participation of Financial Institutions in the Fight against Money Laundering,” and Section 218-3 of the Criminal Code, and amended by Act

1.253 of 12 July 2002, “Relating to the Participation of Financial Undertakings in Countering Money Laundering and the Financing of Terrorism.”

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 illicit funds to purchase property (which is itself subject to confiscation).

The 2002 amendments to the 1993 money laundering legislation include bringing corporate service providers, portfolio managers, and Monaco Law 214 trustees, as well as institutions within the offshore sector, into line with the obligations of banks. New procedures have also been put into place, which include internal compliance, identification of the client, and records maintenance. Government authorities held briefings to explain the new procedures to companies requiring compliance officers. Meetings are also held with compliance officers so that implementation issues and concerns may be aired and addressed.

Offshore companies are subject to the same due diligence and suspicious reporting obligations as banking institutions, and Monegasque authorities conduct on-site audits. The 2002 legislation also strengthens the “know your client” obligations for casinos and obliges companies responsible for the management and administration of foreign entities not only to report suspicions to Monaco’s Financial Intelligence Unit (FIU), but also to set up internal anti-laundering and counterterrorist financing procedures, the enforcement of which is monitored by the FIU.

Banking laws do not allow anonymous accounts, but Monaco does permit the existence of alias accounts, where the owner uses a pseudonym in lieu of the real name. Cashiers do not know the client, but the bank knows the identity of the customer and retains client identification information.

Prior approval is required to engage in any economic activity in Monaco, regardless of its nature. The Monegasque authorities issue approvals of the type of business to be engaged in, and the location for a given length of time. Of particular importance is the fact that this government approval is personal and may not be assigned. Changes in any of the above terms require the issuance of a new approval.

Monaco established its FIU, the Service d’Information et de Controle sur les Circuits Financiers (SICCFIN), to collect information on suspected money launderers. SICCFIN receives suspicious transaction reports, analyzes them, and forwards them to the Prosecutor when they relate to drug-trafficking, organized crime, terrorism, terrorist organizations, or the funding thereof. SICCFIN also is responsible for supervising the implementation of anti-money laundering legislation. SICCFIN also has provided training to intermediaries, most recently to lawyers and notaries. Under Law 1.162, Article 4, SICCFIN may suspend a transaction for up to twelve hours and advise the judicial authorities to investigate.

In November 2001, Monaco and France 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. The 2002 amendments to the money laundering legislation increase SICCFIN’s investigatory powers. In 2002, SICCFIN received 275 disclosures, 33 of which were passed to the Public Prosecutor for further investigation. In 2003, SICCFIN received 250 disclosures, 19 of which were referred to the public prosecutors. By mid-December 2004, SICCFIN had received an additional 326 disclosures, of which 18 were passed to the Public Prosecutor for further investigation. In 2004 SICCFIN received and answered 126 requests for financial information

Investigation and prosecution are handled by the two-officer Unite de lutte au blanchiment (Unit Against Money Laundering) within the police. The Groupe de repression du banditisme (Group Against Organized Crime) may also handle cases. Depending on the number and types of cases, there

are seven police officers equipped to deal with money laundering. Monaco has had three convictions for money laundering, and one acquittal. Monaco encounters obstacles because predicate offenses for money laundering are committed abroad; despite the existence of money laundering, often the crime that receives the conviction is the predicate crime and not the money laundering offense.

Monaco's legislation allows for confiscation of property of illegal origin as well as a percentage of illegally acquired and legitimate property that has been co-mingled. A court order is required for confiscation. In the case of money laundering, confiscation of property is restricted to the offenses listed in the Criminal Code. On the basis of letters rogatory, over 11.7 million euros have been seized. Monaco has extradited criminals, mainly to Russia.

In July and August 2002, Monaco passed Act 1.253 and promulgated two Sovereign Orders, intended to implement UNSCR 1373, which outlaw terrorism and its financing. Monaco is a party to the UN International Convention for the Suppression of the Financing of Terrorism; in April and August 2002, Monaco promulgated Sovereign Orders to import into domestic law the international obligations it accepted when it ratified that Convention.

The Securities Regulatory Commissions of Monaco and France signed a memorandum of understanding on March 8, 2002, on the sharing of information between the two bodies. The agreement was a step in Monaco's efforts to conform to standards proscribed by the International Organization of Securities Commissions, whose mission is to establish international standards to promote the integrity of securities markets. The Government of Monaco sees the MOU as an important tool in combating financial crimes, particularly money laundering.

In 2004 SICCFIN signed information exchange agreements with counterparts in Malta, Poland, Andorra, Mauritius, Slovakia, Canada, and Peru. In previous years it had signed such agreements with Slovenia, Italy, Ireland, Lebanon, Switzerland, Liechtenstein, Panama, Luxembourg, France, Spain, Belgium, Portugal, and the United Kingdom. SICCFIN is a member of the Egmont Group. It is a priority for Monaco to satisfy mutual legal assistance requests, which are enforced swiftly, and there is no obstacle to international judicial cooperation.

Monaco was admitted to the Council of Europe on October 4, 2004. Well before that date, in 2002, SICCFIN approached the Council of Europe's MONEYVAL Committee and requested full participation in that Committee, including having an evaluation conducted on its anti-money laundering regime. In October 2002, the evaluation was performed; the evaluators acknowledged the extensive and thorough regime that has been developed.

Monaco is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. In May 2002, Monaco acceded to the Council of Europe Convention on the Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

The Government of Monaco should amend the Criminal Code to include an "all-crimes" approach, rather than the current list of predicate offenses. Monaco should also amend its legislation to implement full corporate criminal liability and establish a central registry for IBCs. Monaco should continue to enhance its anti-money laundering and confiscation regimes.

Mongolia

Mongolia is not a financial center. Crimes related to banking activities are relatively few, and an upward trend has not been observed. Markets in Mongolia are licensed and monitored by the government authorities. Mongolia's vulnerability to transnational crimes such as money laundering has grown with the country's increased levels of international trade, tourism, and banking. Mongolia's long, unprotected borders with Russia and China make it particularly vulnerable to smuggling and narcotics-trafficking. The growing North Korean presence in Mongolia also makes the country

vulnerable to counterfeit U.S. currency. Illegal money transfers and public corruption are other sources of illicit funds. Although the Government of Mongolia (GOM) is drafting anti-money laundering legislation, it 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.

The prepared draft law "On Combating Against Money Laundering and Funding Terrorism" (draft AML law), which is projected to pass within the next two legislative sessions, and the draft law on amending the criminal code will have provisions that define money laundering as a criminal offense. In addition, actions involving use of illegally obtained assets and money are considered to be crimes.

The Central Bank, tax authorities and law enforcement agencies have the power to investigate, within their respective jurisdictions, transactions and books of banks and other financial institutions. According to Article 39 of the Criminal Code, officers of financial institutions are obligated to provide to law enforcement agencies information on crimes that have become known to them. The draft AML Law will introduce suspicious transaction reporting (STR) requirements. The draft AML law provides that legal entities conducting the activities of banks, non bank financial institutions, commercial insurance companies, activities described by Article 15.3.1 of the Law on Special Licensing of Commercial Activities, savings and loan cooperatives, and their subsidiaries or branches have an obligation to inform relevant agencies about applicable transactions. The draft AML Law also has a provision on monitoring the management of reporting entities.

Article 7 of the Law on Banking, which provides for the confidentiality of bank records, also states that a bank or its officers shall not be liable for cooperating with a law enforcement agency. The draft AML law has a similar provision. It also states that management and officers of a bank who are involved in crimes can be charged for criminal, civil and/or administrative violations.

The Law on Foreign Currency Regulation (Article 17 and others) has provisions that regulate the flow of foreign currency through the Mongolian border. Police pay attention to international trafficking of foreign currency or other payment documents that have illegal origins, but there have been no investigations to date. Since January 1, 2004, there have been no reported incidents of money laundering or terrorism funding, and likewise no arrests or prosecutions.

A draft law "On Amending the Criminal Code" has been developed together with the draft AML law to implement the requirements of UNSCR 1373. The Foreign Currency Department of the Central Bank regularly distributes the lists of members of al-Qaida, the Taliban and other associated persons, supplied by the USG, to banks and financial institutions along with recommended measures.

The President of Mongolia directed the introduction of legal regulations combating terrorism by issuing Decree #60 in 2001, entitled "Supporting Establishment of an International Coalition Against Terrorism". Accordingly, the GOM adopted Resolution #226 in 2001, entitled "Supporting Activities of the International Coalition Against Terrorism". The resolution requires relevant agencies to exchange information and cooperate with their counterparts in coalition countries regarding terrorists, drug-trafficking and money laundering actions. Both the directive and resolution are currently enforced with no objections by any political parties.

There is a system to track, identify, investigate, seize, confiscate or impose fines regarding assets created through grave crimes such as international trafficking, narcotics-related crimes or funding of terrorism. These proceedings shall be carried out according to rules provided by the Criminal Code and the Criminal Procedure Code. Assets confiscated or fines collected are transferred to the GOM budget.

Mongolia is a party to the 1988 UN Drug Convention. Mongolia became a party to the UN International Convention for the Suppression of the Financing of Terrorism on February 25, 2004. In

recent years Mongolia has increased its participation in fora that focus on transnational criminal activities and, in 2004, became a member of the Asia/Pacific Group on Money Laundering.

The Government of Mongolia should pass and implement comprehensive anti-money laundering and counterterrorist financing legislation. It should subsequently take steps to fully implement those laws and build a comprehensive anti-money laundering regime capable of thwarting terrorist financing that comports with international standards.

Montserrat

Montserrat has one of the smallest financial sectors of the Caribbean overseas territories 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. There are no exchange controls for transactions below EC\$250,000.

As of 2003, Montserrat's offshore sector consists of 11 offshore banks, all owned and controlled by Latin American interests, approximately 22 international business companies (IBCs) and 30 Companies Act companies, the majority of which engage only in conducting local business. Insurance and trust services are negligible. IBCs may be registered using bearer shares, providing for anonymity of corporate ownership. The Financial Services Centre (FSC) regulates offshore banks, while the Eastern Caribbean Central Bank (ECCB) supervises Montserrat's two domestic banks. In 2002, the government entered into a memorandum of understanding (MOU) with the ECCB to provide assistance in the supervision of Montserrat's offshore banking sector, as the FSC does not have sufficient staff to undertake an ongoing supervision program for offshore banks. MOUs also have been entered into with four overseas regulators to provide a mechanism for collaboration in the supervision of most of the offshore banks. No examinations have been done of the offshore banks to evaluate their compliance with anti-money laundering programs.

The Proceeds of Crime Act (POCA), 1999, criminalizes the laundering of proceeds from any indictable offense except domestic drug-trafficking. Likewise, tipping off is prohibited except in money laundering cases tied to drug-trafficking. Both individuals and legal entities are subject to the law, and self-laundering is covered for all offenses. The legislation also imposes broad requirements on financial institutions regarding customer identification and record keeping and mandates the reporting of suspicious transactions to a designated authority. Under the POCA, the Governor has issued a non-mandatory Practice Code establishing further comprehensive guidance for financial institutions. There are no reporting requirements for cross-border currency movements.

The Offshore Banking Act (OB Act) and the Financial Services Commission Act, 2001 (FSC Act) are the governing pieces of legislation for the offshore sector. The OB Act addresses licensing of offshore banks, prudential and supervision requirements, and liquidation issues. The FSC Act establishes the FSC and sets out its authorities and administration.

The Money Laundering Regulations 2000 apply to banks, securities dealers, money transmission services, company management services, and financial leasing companies. The Regulations do not explicitly address offshore banks, and it remains unclear whether they are subject to the Regulations' requirements. The Regulations call for covered entities to maintain internal reporting procedures. Anonymous accounts are prohibited. Any suspicious activity must be reported to the police. Customer identification provisions contain exemptions that allow banks to open accounts and transact business without verifying customer identity. For example, no identification is required for one-off transactions under EC \$40,000, nor is it required when a customer is introduced to the bank—the introducer may provide written assurance the customer has been subject to identification. Banks are required to keep records for five years; however, inspections of domestic banks have shown widespread deficiencies in

implementation. The Practice Code contains more explicit instructions for banks, but because it is not mandatory, deficiencies are apparent in the implementation of many requirements.

The Reporting Authority (RA) was established in 2002, under the POCA, to serve as Montserrat's Financial Intelligence Unit (FIU). The RA consists of the Commissioner of Financial Services, the Attorney General and the Commissioner of Police. The Order establishing the RA sets forth only a single power, to disclose information it receives to law enforcement agencies; however, subsequent amendments have provided for the receipt of suspicious transaction reports (STRs). It does not authorize the receipt or analysis of information, although this occurs in practice. As of October 2002, 20 STRs had been received by the RA, all from one offshore bank. As of 2003, there have been no prosecutions for money laundering.

Montserrat has criminalized terrorist financing. The UN International Convention for the Suppression of the Financing of Terrorism has not been extended to Montserrat; however, Montserrat has implemented provisions in local legislation to put into practice applicable provisions of the Convention. The UNSCR 1267 Sanction Committee's consolidated list is circulated to financial institutions.

The POCA provides for freezing and confiscation of the proceeds of crime and international cooperation. Except in terrorist financing cases where a restraint order may be obtained once a criminal investigation has commenced, criminal proceedings must be instituted before assets can be frozen. As of 2003, no property related to money laundering or terrorist financing had been frozen, seized or confiscated. Montserrat has not considered a mechanism to share seized assets.

In October 2002, the Caribbean Financial Action Task Force (CFATF) conducted a second round mutual evaluation of Montserrat, in conjunction with the IMF and World Bank.

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 CFATF and is subject to the 1988 UN Drug Convention.

The Government of Montserrat should criminalize self-laundering related to domestic drug-trafficking. Montserrat should make the full operation of the Reporting Authority a priority, including assuring it has the necessary authority to receive and analyze suspicious transaction reports. It should enact measures to identify and record the beneficial owners of IBCs and immobilize bearer shares. Montserrat also should enact cross-border currency reporting requirements and close the loopholes in its customer identification procedures. Montserrat must ensure adequate oversight and supervision of its offshore sector to deter criminal and terrorist organizations from abusing its financial services sector.

Morocco

Morocco is not a regional financial center and the extent of the money laundering problem in Morocco is not known. Morocco remains an important producer and exporter of cannabis, with estimated revenues of \$12 billion annually, according to a joint study released in late 2003 by the United Nations Office on Drugs and Crime (UNODC) and Morocco's Agency for the Promotion and the Economic and Social Development of the Northern Prefectures and Provinces of the Kingdom. Some of these proceeds may be laundered in Morocco and abroad. There is no indication that international or domestic terrorist networks have engaged in widespread use of the narcotics trade to finance terrorist organizations and operations in Morocco. Press reports indicate, however, that the Spanish investigation into the March 11, 2004 terrorist bombings in Madrid found that the alleged Moroccan

national perpetrators of the attacks financed the purchase of the explosives used in the blasts through modest sales of cannabis resin in Spain.

Morocco has a significant informal economic sector, including remittances from abroad and cash-based transactions. There are unverified reports of trade-based money laundering, including bulk cash smuggling, under-and over-invoicing, and the purchase of smuggled goods. Banking officials have indicated that the country's system of unregulated money exchanges provides opportunities for potential launderers. Morocco has a free trade zone in Tangier, with customs exemptions for goods manufactured in the zone for export abroad. There have been no reports of trade-based money laundering schemes or terrorist financing activities using the Tangier free zone or the zone's offshore banks, which are regulated by an interagency commission chaired by the Ministry of Finance.

There have been no reported arrests or prosecutions for money laundering or terrorist financing in Morocco since January 1, 2004. Morocco has a relatively effective system for disseminating U.S. Government (USG) and United Nations Security Council Resolution (UNSCR) freeze lists to the financial sector and law enforcement. Morocco has provided detailed and timely reports requested by the UNSC 1267 Committee. A handful of small value accounts have been administratively frozen based on U.S. Executive Order 13224 freeze lists.

The Moroccan financial sector 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 (CBM), which monitors and regulates the banking system. A separate Foreign Exchange Office regulates international transactions. Morocco has used administrative instruments and procedures to freeze suspect accounts.

However, CBM issued Memorandum No. 36 in December 2003, in advance of passage of still pending anti-money laundering legislation, instructing banks and other financial institutions to conduct their own internal analysis/investigations. It also mandates "know your customer" procedures, reporting of suspicious transactions and the retention of suspicious activity reports. Morocco also has in effect: legislation prohibiting anonymous bank accounts; foreign currency controls that require declarations to be filed when transporting currency across the border, although not strictly enforced; and internal bank controls designed to counter money laundering and other illegal/suspicious activities.

In June 2003, Morocco implemented a comprehensive counterterrorism bill that provided the legal basis for the lifting of bank secrecy to obtain information on suspected terrorists, freeze suspect accounts and prosecute terrorist finance-related crimes. The law also provides for the seizing and confiscation of terrorist assets and for international cooperation with regard to foreign requests for freezing assets of a suspected terrorist entity. This law brought Morocco into compliance with UNSCR 1373 requirements for the criminalization of the financing of terrorism.

As of December 2004, Morocco was moving towards the enactment of two laws that will further strengthen Morocco's anti-money laundering system: a banking/financial sector reform bill and an anti-money laundering bill. The anti-money laundering bill reportedly includes, among other provisions, a suspicious transaction reporting scheme and the creation of a Financial Intelligence Unit (FIU). The bills are based on the Financial Action Task Force (FATF) Forty Recommendations and Egmont Group guidelines and will help bring Morocco's financial sector in line with international standards.

Together, the three bills will enhance the supervisory and enforcement authority of the Central Bank and outline investigative and prosecutorial procedures. In the interim, the Central Bank has already mandated "know your customer" requirements and the reporting of suspicious transactions by financial institutions. All money transfer activities that take place outside the realm of the official Moroccan banking system—as set by the CBM guidelines—are deemed illegal. The pending bills will

also expand the CBM's regulatory authority over non-banking financial transactions. Other significant provisions include: the lifting of bank secrecy during investigations, as well as legal liability protection of bankers and investigators for cooperation during investigations.

Morocco is a party to the UN International Convention for the Suppression of Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Morocco is also a party to the UN International Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention); in fact, Morocco has ratified or acceded to all UN and international conventions and treaties related to counterterrorism.

The Government of Morocco should move expeditiously to pass the banking sector reform bill and the anti-money laundering bill. As part of its anti-money laundering program, Morocco should establish a centralized Financial Intelligence Unit (FIU) that will receive and analyze suspicious transaction reports and disseminate them to appropriate law enforcement agencies for investigation.

Mozambique

Mozambique is not a regional financial center. Money laundering is fairly common, however, and local authorities believe that narcotics proceeds have helped finance the recent proliferation of new restaurants, shopping centers, hotels, and mosques in the country, especially in the capital. These businesses reputedly conceal profits made by those importing hashish and heroin from South Asia via Tanzania and, to a lesser extent, cocaine from South America via Brazil. Most narcotics are destined for South African and European markets; Mozambique is not a significant consumption destination and is rarely a transshipment point to the United States. Local organized crime controls narcotics-trafficking operations in the country, with certain recent immigrants from Pakistan and India also playing a prominent role. Money laundering in the banking sector is also considered to be a serious problem; and in recent years, prominent public figures in the Central Bank, the law enforcement community and the media have been murdered for investigating fraud and money laundering in these institutions. For example, in 2001, the Chief of Banking Supervision at the Central Bank was murdered in the stairwell of a bank that had been under investigation. Despite these problems, or perhaps because of them, there are no known links between Mozambique-based drug traffickers, money launderers and the financing of terrorists.

The financial sector in general is not believed to be experiencing any reported increase in crimes such as money laundering, but it is hard to be certain because very few instances of laundering are formally reported or investigated. Black markets for smuggled goods and financial services are widespread, dwarfing the formal retail and banking sectors in most parts of the country and making it difficult to determine when and where laundering of narcotics money takes place. Local officials are often directly involved with drug trafficking and the laundering of profits, including the ex-chief of the Criminal Investigative Police and several of his top officers, who are now awaiting trial on narcotics-trafficking charges. Evidence of money laundering was cited by the government as a reason for arresting these officials in 2003, but they are being prosecuted for narcotics-trafficking, not money laundering.

Money laundering has long been a criminal offense in Mozambique, but criminal charges and prosecutions for money laundering have been rare because the law had not been narrowly defined until enactment of the 2002 Anti-Money Laundering Act. Implementing regulations for most components of this law were only issued in September 2004, with more regulations reportedly forthcoming in 2005. The law contains specific provisions related to narcotics-trafficking, but also includes a wider range of offenses as predicates for money laundering. There were no money laundering arrests in 2004, nor any prosecutions.

According to the 2002 law, banks and exchange houses must immediately record and report to the Attorney General's office any cash transaction valued at 441 times the national minimum wage, which amounts to about \$18,000. In addition, exchange houses are required to turn in records of all transactions on a daily basis. All credit card transaction attempts over \$5,000 must also be reported and can only be processed with approval from the Central Bank. Banks and exchange houses are required to keep transaction records for 15 years (Article 15 of 2002 law). Financial institutions are required to report any suspicious transactions immediately to the Attorney General's office (Article 16). The Attorney General, in turn, is required to determine within 48 hours whether to permit the transaction (Article 19). Individuals who report suspicious transactions in good faith receive protection under the 2002 law (Article 21). Bank secrecy laws exist in Mozambique but do not apply in the case of suspected money laundering (Article 17).

The 1996 Money Exchange Act requires any individual carrying more than \$5,000 over the border to file a report with Customs. Taking more than \$5,000 in local currency out of the country is prohibited. The 2002 Anti-Money Laundering Act includes due diligence provisions that make both respective bankers and banks responsible if financial institutions launder money (Article 27). Money laundering controls apply to all formal non-banking financial institutions, including exchange houses, brokerages houses, casinos and insurance companies. Cash couriers must meet cross-border currency requirements, but usually fall outside the scope of anti-money laundering law because they generally work in the informal sector.

Mozambique has not explicitly criminalized the financing of terrorism. Its 1991 Crimes against the Security of State Act criminalizes terrorism, but financing is not addressed. The 2002 anti-money laundering law does list terrorism finance as a serious crime subject to the scope of the law, but elaborates no further (Article 4). The same law codifies Mozambique's long-authority to identify, freeze, seize and/or forfeit the assets of those charged with financial crimes, including terrorist financing (Articles 5 and 6). Financial institutions do not have direct access to the names of persons or entities included on the UN 1267 Sanctions Committee consolidated list or the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224; these lists are distributed only to the Central Bank, the Attorney General, and the Ministry of Foreign Affairs. Authorities in these institutions have not positively identified any of the persons or entities on these lists operating in Mozambique, and therefore no assets have been identified, frozen, or seized.

Mozambique is not considered an offshore financial center. Many local businessmen use offshore banking in nearby countries, such as Mauritius. There are no free trade zones in Mozambique. Authorities acknowledge that alternative remittance systems are common in Mozambique, many of which operate in exchange houses that, on paper, are heavily regulated but in fact can easily avoid reporting requirements. There are no serious legislative, judicial, or regulatory measures being considered to address this problem. Charitable institutions must receive approval by the Ministry of Justice (MOJ) before receiving a charter, and are subject to investigation by the MOJ thereafter. However, there is no evidence of the MOJ seriously investigating any charities at this time.

Mozambique is a party to the 1988 UN Drug Convention and the International Convention for the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. It is also a member of a FATF-style regional body, the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG). Mozambique has entered a series of formal agreements with neighboring countries to share financial information required by law enforcement bodies. Cooperation with the United States on these matters has taken place on an informal basis.

The 2002 Anti-Money Laundering Act contains provisions authorizing the seizure and forfeiture of assets, including those of legitimate businesses used to launder money. In such a case, the Central Bank would be responsible for the initial tracing of assets and the Attorney General would be

responsible for freezing and confiscating assets. The Attorney General also has authority to auction off confiscated assets and to distribute proceeds to a range of parties. Despite this legal framework, the institutions authorized to implement the law do not have an established system for identifying and freezing narcotics-related assets, and no assets have been seized to date under the 2002 Anti-Money Laundering Act.

The law allows for both civil and criminal forfeiture. An example of civil forfeiture would be the seizure of cash in excess of the \$5,000 limit from an individual who tried, secretly, to carry this amount across the border. The seized funds would be sent by Customs to the Central Bank. Appeals then could be made directly to the Bank. Private financial institutions are more closely regulated by criminal forfeiture acts, but are also subject to civil suits. Financial institutions also have the right to file a civil suit against the government for loss of business in cases of unreasonable suspension, a provision that will likely discourage enforcement of the law.

The Government of Mozambique should clarify that the financing of terrorism is specifically criminalized, either by its 1991 or 2002 legislation, or else it should do so in a new instrument. It should proceed as soon as possible with the issuance of the additional implementing regulations to the 2002 Anti-Money Laundering Act. It should establish a financial intelligence unit in accordance with international standards. It should ratify the UN Convention against Transnational Organized Crime. It must also address some additional and serious obstacles to enforcement of its laws, such as resource constraints affecting the Attorney General's office and the Criminal Investigative Police, significant corruption of the latter, and intimidating tactics on the part of organized crime against investigating prosecutors at the Attorney General's Anti-Corruption Unit. These practical measures will be necessary to enforce any laws.

Namibia

Namibia is not a regional financial center. In addition to its Central Bank, Namibia has four 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 financial institutions.

In November of 2004, Namibia criminalized money laundering with passage of the Prevention of Organized Crime Bill. The new law requires both bank and non-bank financial institutions to report suspicious transactions to the Central Bank and provide relevant documents and other information to government authorities for use in criminal investigations. Non-bank financial institutions, such as private pension funds, the stock exchange, and investment companies, were previously exempted from such reporting requirements.

Parliament will consider a separate anti-money laundering bill—the Financial Intelligence Act (FIA)—in early 2005. The FIA is expected to add additional reporting requirements and strengthen the Government's ability to investigate and prosecute money laundering crimes. It will also establish a financial intelligence unit. The FIA is also expected to address cross-border currency reporting requirements and information sharing with foreign law enforcement authorities. Namibia currently does not have laws that criminalize the financing of terrorism. The Government intends to table its Combating of Terrorist Activities Bill in Parliament in 2005. Under the proposed counterterrorism law, the Government would be empowered to proscribe an organization if it commits or participates in terrorism; prepares for acts of terrorism; promotes or encourages terrorism; or is otherwise involved with terrorism. The proposed law would also prohibit individuals from providing money or other property with the intention or knowledge (or suspicion) that such money or other property would be used for the purposes of terrorism (regardless whether or not a terrorism act was committed). Individuals who do so would be subject to prosecution and imprisonment not to exceed 20 years.

There have been no known arrests or prosecutions for money laundering or terrorist financing since January 1, 2004.

Namibia is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG). Namibia served as the Chair of ESAAMLG from August 2001 until August 2002. Namibia is a party to the UN Convention against Transnational Organized Crime and the 1988 UN Drug Convention. In November 2001, the GRN signed the UN International Convention for the Suppression of the Financing of Terrorism, and is making progress toward becoming a party.

The Government of Namibia should pass counterterrorism and related legislation that criminalizes terrorism financing and further strengthens the country's nascent anti-money laundering regime, as it has committed to doing through its membership in ESAAMLG. Namibia should continue its efforts toward becoming a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Nauru

Nauru is a small Central Pacific island nation with a population of approximately 13,000. 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. The currently insolvent government-owned Bank of Nauru acts as the Central Bank for monetary policy. Nauru's legal, supervisory, and regulatory framework has provided significant opportunities in the past decade for the laundering of the proceeds of crime.

In June 2000, the Financial Action Task Force (FATF) placed Nauru on its initial list of fifteen Non-Cooperative Countries and Territories. In response to mounting international pressure, the Government of Nauru, in August 2001, passed the Money Laundering and Proceeds of Crime Act of 2001 (AMLA 2001). The AMLA 2001 requires financial institutions to verify and record the identity of account holders and to maintain accounts in the name of the account holder, thereby prohibiting anonymous accounts and accounts held in fictitious names. The AMLA 2001 also requires financial institutions to report suspicious transactions, and to develop internal anti-money laundering policies and procedures. The new legislation allowed for the establishment of a Financial Intelligence Unit (FIU) called the Financial Institutions Supervisory Authority (FISA). FISA has not yet been formed and no suspicious transaction reports have been filed to it. The AMLA 2001 provided for mutual assistance with respect to money laundering investigations. However, there are limitations regarding compliance with foreign requests for assistance. Nauru may refuse to comply with a foreign 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. However, the Government of Nauru (GON) has since cooperated with officials from the United States and other countries in certain criminal investigations involving Nauru's institutions.

On September 7, 2001, the FATF issued a press release recognizing the passage of the Nauru's AMLA 2001. The FATF, however, found the legislation to have several deficiencies. It urged Nauru to enact appropriate amendments by November 30, 2001, in order to avoid the application of countermeasures. On December 5, 2001, the FATF called upon its members to impose countermeasures against Nauru because of Nauru's failure to remedy deficiencies in its anti-money laundering regime.

On December 6, 2001, Nauru amended the AMLA 2001 to address certain deficiencies in the original act. The amendment clarified that the law applies to all financial institutions incorporated under the laws of Nauru (as opposed to just financial institutions conducting business within Nauru). It also broadened the definition of money laundering. Despite the passage of its anti-money laundering

legislation with amendments, Nauru continued to lack a legal framework and an effective regime for the regulation and supervision of the nearly 400 registered 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 the 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.

In December 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. In the announcement, the U.S. Treasury published a list of 161 banks licensed by the Republic of Nauru, the majority of which were thought to be shell banks. In April 2003, U.S. Treasury and FinCEN issued a proposed rule pursuant to section 311 to invoke Special Measure Five, prohibiting U.S. financial institutions from opening or maintaining any payable-through or correspondent accounts involving a Nauru financial institution.

The Anti-Money Laundering Act 2003 AMLA consolidates the Anti-Money Laundering Act of 2001 and the Anti-Money Laundering (Amendment) Act of 2001. The amended legislation gives the Nauru FIU, the Financial Institutions Supervisory Authority, if and when it is established, authority to cooperate with foreign states, including the power to obtain search warrants, track property, and issue monitoring orders. The amended legislation also gives the Director of Public Prosecutions the power to freeze and seize assets relating to money laundering. Legislative amendments to the Corporation Act 1972 were also enacted in 2003 to abolish offshore banking and eliminate all bank secrecy provisions. Nauru took further steps to publish the list of corporations that recently held Nauruan offshore banking licenses.

Following the election of a reformist government in 2004, Nauru enacted a series of legislative acts to reform its anti-money laundering laws and respond to deficiencies identified by the FATF. In 2004, the GON passed the Anti-Money Laundering Act of 2004, the Banking (Amendment) Act of 2004, the Corporation (Amended) Act of 2004, the Financial Transactions Reporting Act of 2004, the Counter-Terrorism and Transnational Organized Crime Act of 2004, the Mutual Assistance in Criminal Matters Act of 2004, and the Proceeds of Crime Act 2004.

The Anti-Money Laundering Act 2004 enacted on September 6, 2004 expands the coverage and scope of anti-money laundering requirements to banks, money remitters, securities and investment businesses, insurance, real estate agents, dealers in precious metals and stones, trust or company service providers, and legal entities. The new legislation provides the powers of search and seizure to law enforcement, and enables freezing and forfeiture of tainted property and terrorist property. The Act also allows mutual assistance in relation to anti-money laundering investigations with foreign states.

At the October 2004 Plenary, the FATF recommended that its member states withdraw all countermeasures against Nauru in view of Nauru’s having taken several significant steps to ensure that offshore banks previously licensed in Nauru no longer existed and no longer conducted banking activity. As of January 1, 2005, The United States had not conformed to the FATF recommendation to withdraw its countermeasure. The FATF also invited Nauru to submit an implementation plan with benchmarks and timetables regarding the steps it would take to cure the remaining deficiencies of its anti-money laundering regime.

A technical team from the Pacific Island Forum Secretariat (PIF) will travel to Nauru in early 2005 to assist Nauru in developing and implementing its anti-money laundering regime. The PIF technical team will assist in establishing Nauru's FIU- the Financial Institutions Supervisory Authority- and will provide training for prosecutors and investigators of financial crimes.

Nauru has observer status within the Asia/Pacific Group on Money Laundering and recently joined the United Nations. Nauru has signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

The Government of Nauru should continue to work with the Financial Action Task Force (FATF) to ensure that its anti-money laundering regime comports with the FATF's revised Forty Recommendations and its nine Special Recommendations on Terrorist Financing, and that whatever remnant of its offshore financial sector remains is regulated consonant with those standards. Nauru should become a party to the UN International Convention for the Suppression of the Financing of Terrorism, and to all UN Conventions pertaining to terrorism. Nauru should also ratify the UN Convention against Transnational Crime and accede to the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.

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 2004. Since the dissolution of Parliament in May 2002, any new laws must be passed by royal ordinance, which must be renewed after six months. Draft anti-money laundering legislation has been prepared but has not yet passed into law or ordinance. There were no prosecutions or even arrests for money laundering during 2004.

Banks are required to record the identity of customers engaging in significant transactions. In particular, all transactions which involve payments in foreign currency require prior approval by the NRB (Nepal's Central Bank). Any Nepali citizen who wishes to open a foreign currency account must obtain a license to do so from the NRB, and Nepali citizens wishing to take currency overseas must obtain approval from the NRB by clearly outlining the purpose for transferring funds overseas. The NRB normally approves small amounts (in USD thousands) for travel, education and medical treatment. For business transactions, however, a letter of credit from a bank recognized by the NRB must be opened by documenting the transaction details. Banks have provided records regarding bank accounts of individuals and institutions to assist in GON investigations into corruption by senior officials. Nepal has enacted bank secrecy laws that prevent the disclosure of client and ownership information to individuals and law enforcement authorities; however, the present law does not prevent the disclosure of client and ownership information to the NRB, courts, auditors or the Commission for Investigation of Abuse of Authority (CIAA). Nepal has explored the development of an offshore financial sector, but one does not exist at present.

The NRB has the authority to freeze and seize assets related to criminal investigations. However, the GON's ability to identify and trace assets is hindered by a lack of a computerized information sharing system. For example, many bank branch offices do not have computers. The Nepal Police also have the authority to seize any goods or property related to criminal investigations.

A hawala system of informal remittances (called the hundi system in Nepal) is widespread. Expatriate Nepali workers—the primary source of hundi transactions—are often employed in the Gulf, Malaysia, and other countries that have introduced new, more stringent regulations on informal remittance

systems. Nepali workers in India still utilize hawala-hundi transactions. There have been no significant initiatives to regulate the system in Nepal. However, GON officials claim that changes in the laws of other countries have forced some Nepalese hundi users to conduct their transactions through formal banking institutions. In Nepal, the hundi system is linked to issues of capital flight, tax avoidance, and corruption.

Nepal has not passed any laws criminalizing terrorist financing. However, the Terrorist and Destructive Activities Act and the Bank and Financial Institutions Ordinance 2004, working in tandem, reportedly criminalize terrorist financing. Under the Bank and Financial Institutions Ordinance 2004, the NRB has the authority to seize any assets deemed to have been used in terrorist activities. No assets belonging to individuals or entities on the UNSCR 1267 Sanctions Committee's consolidated list have been identified in Nepal. Additionally, the State Offense Act of 1989 authorizes security forces to arrest and prosecute any Nepalese or foreign citizen involved in any criminal activities against the state or associated with foreign terrorist activity. The GON made one arrest for terrorist financing in 2004.

The Government of Nepal is a party to the 1988 UN Drug Convention. It has also signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Nepal should proceed with ratification of this Convention. Nepal should also sign and ratify the UN International Convention for the Suppression of the Financing of Terrorism. Legislative action in Nepal has clearly been handicapped by the lack of a sitting Parliament. As soon as practicable, Nepal should enact the provisions of its 2002 Master Plan for Drug Control, including anti-money laundering and terrorist finance legislation, and develop a comprehensive anti-money laundering regime that would require the mandatory filing of suspicious transaction reports (and clarify that this may be done without violating current bank secrecy provisions), foster international cooperation in the area of anti-money laundering initiatives, and establish a financial intelligence unit. It also should initiate efforts to regulate its domestic hundi dealers.

The Netherlands

The Netherlands is a major financial center and as such is an attractive target for the laundering of funds generated from a variety of illicit activities. Activities involving money laundering are often related to the sale of heroin, cocaine, cannabis, or synthetic and designer drugs (such as ecstasy). Activities involving financial fraud are believed to generate a considerable portion of domestic money laundering. Much of the money laundered in the Netherlands is likely owned by major drug cartels and other international criminal organizations and much of it flows through the formal financial sector. There are no indications of syndicate-type structures in organized crime or money laundering, and there is virtually no black market for smuggled goods in the Netherlands. Although under the Schengen Accord there are no formal controls on the borders with Germany and Belgium, the Dutch authorities run special operations in the border areas designed to keep smuggling to a minimum. The Netherlands is not an offshore financial center nor are there any free trade zones in the Netherlands.

In 1994, the Government of the Netherlands (GON) criminalized money laundering related to all crimes, although prosecutors first had to prove the predicate offense before prosecuting for money laundering. In December 2001, legislation was enacted making facilitating, encouraging, or engaging in money laundering a separate criminal offense, regardless of the source of the funds, easing somewhat the government's burden of proof regarding the criminal origins of proceeds. Under the law, the GON needs only to prove that the proceeds "apparently" originated from a crime; self-laundering is also covered. The penalty for deliberate acts of money laundering is a maximum of four years' imprisonment and a maximum fine of 45,000 euros, while liable acts of money laundering (of people who do not know first-hand of the criminal nature of the origin of the money, but should have reason to suspect it) are subject to a maximum imprisonment of one year and a fine no greater than

45,000 euros. Repeated convictions for money laundering offenses may be punished with a maximum imprisonment of six years and a maximum fine of 45,000 euros, and those convicted may also have their professional licenses revoked. In addition to criminal prosecution for money laundering offenses, money laundering suspects can also be charged with participation in a criminal organization (Article 140 of the Penal Code), violations of the financial regulatory acts, violations of the Sanctions Act, or noncompliance with the obligation to declare unusual transactions according to the Economic Offenses Act.

The Netherlands has comprehensive money laundering legislation. The Services Identification Act (WID) and the Disclosure Act set forth identification and reporting requirements. All financial institutions in the Netherlands, including banks, bureaux de change, casinos, life insurance companies, securities firms, stock brokers, and credit card companies, are required to report cash transactions over 15,000 euros, as well as any less substantial transaction that appears unusual, a broader standard than “suspicious” transactions, to the Office for Disclosure of Unusual Transactions (MOT), the Netherlands’ Financial Intelligence Unit (FIU). In December 2001, the reporting requirements were expanded to include trust companies, financing companies, and commercial dealers of high-value goods. In June 2003, notaries, lawyers, real estate agents/intermediaries, accountants, business economic consultants, independent legal advisers, trust companies and other providers of trust related services, and tax advisors were added. Reporting entities that fail to file reports with the MOT may be fined 11,250 euros or be imprisoned up to two years. Under the Identification of Services Act (WID), all those that are subject to reporting obligations must identify their clients, including the identity of ultimate beneficial owners, either at the time of the transaction or 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 seven years. 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. Furthermore, current legislation requires Customs authorities to report unusual transactions to the MOT; however, the Dutch do not currently have a currency declaration requirement for incoming travelers.

The Money Transfer and Exchange Offices Act, which was passed in June 2001, requires money transfer offices, as well as exchange offices, to obtain a permit to operate, and subjects them to supervision by the Central Bank. Every money transfer client has to be identified.

The Central Bank of the Netherlands, which merged with the Pension and Insurance Chamber in April 2004, and the Financial Markets Authority, as the supervisors of the Dutch financial sector, regularly exchange information nationally and internationally. Sharing of information by Dutch supervisors does not require formal agreements or memoranda of understanding (MOUs).

The MOT, which was established in 1994, reviews and analyzes the unusual transactions and cash transactions filed by banks and financial institutions. The MOT receives over 85 percent of unusual transaction reports electronically through its secure website. It forwards suspicious transaction reports with preliminary investigative information to the Police Investigation Service and to the office for operational support of the National Public Prosecutor for MOT cases (BLOM). In 2002, the MOT received 137,339 reports and forwarded 24,741 to the BLOM as suspicious transactions. In 2003, the MOT received 177,157 unusual reports (totaling over 1.5 billion euros), of which 37,748 were flagged by the MOT as suspicious transactions for further investigation by the BLOM. The 30 percent increase in reports is attributed to the new reporting requirements for money transfer businesses and high value

goods dealers as well as an increase in the total amount of money transfers. The average amount reported was 41,000 euros in 2003, an increase from the 34,800 euros reported (on average) in 2002.

In order to facilitate the forwarding of suspicious transactions, the MOT and BLOM created an electronic network called Intranet Suspicious Transactions (IST). Also, a secure website for the actual reporting of unusual transactions by financial institutions was developed, thus completing the electronic infrastructure. Furthermore, fully automatic matches of data with the police databases are included with the unusual transaction reports forwarded to the BLOM. Since the money laundering detection system also covers areas outside the financial sector, the system is used for detecting and tracing terrorist financing activity.

On January 1, 2003, the MOT and BLOM formed a special unit (the MBA-unit) to work together to analyze data generated from the IST. Once the data is analyzed by the MBA-unit, it forwards reports to the police. In 2003, the MBA-unit sent 275 reports to the police for further investigations. Future plans are for the MBA-unit to focus on more project-based strategic type work by analyzing transaction reports that fit profiles provided by the police.

In 2003, BLOM opened 559 investigations, which involved 13,171 transactions. Of these 559 investigations, 75 were related to actions by the Public Prosecutor Hit-And-Run Money Laundering (HARM) team, established in 2001, resulting in the confiscation of approximately 8.1 million euros and the arrest of 78 suspects. Both the MOT and BLOM are internationally recognized institutions that play a major role in the Egmont Group. BLOM provides the anti-money laundering division of Europol with suspicious transaction reports, and Europol applies the same analysis tools as BLOM.

In 2004, an evaluation of the anti-money laundering reporting system, commissioned by the Minister of Justice, was published. In response to the report, the GON announced a number of measures to enhance the effectiveness of the anti-money laundering system. These measures include: an instruction on money laundering for the Public Prosecution Service, new indicators for reporting requirements, amendments to anti-money laundering legislation (Disclosure Act and the Identification of Services Act), and an agreement of cooperation between the National Police and the Dutch Internal Revenue Service Investigation Office. These measures are currently being implemented or will take effect during the course of 2005.

The Netherlands has enacted legislation governing asset forfeitures. The 1992 Asset Seizure and Confiscation Act enables the authorities to confiscate assets that are illicitly obtained or otherwise connected to criminal acts. The legislation was amended in 2003 to improve and strengthen the options for identifying, freezing, and seizing criminal assets. The police and several special investigation services are responsible for enforcement in this area. These entities have adequate powers and resources to trace and seize assets. Asset seizure has been fully integrated into all law enforcement investigations into serious crime. Statistics provided by the Office of the Public Prosecutor show that the amount of assets seized in 2003 amounted to 10.1 million euros (\$11 million), compared to 7.9 million euros (\$10.5 million) in 2002. The United States and the Netherlands have an agreement on asset sharing dating back to 1994. The Netherlands also has a treaty on asset sharing with the UK, as well as an agreement with Luxembourg.

In June 2004, the Minister of Justice sent an evaluation study to the Parliament on specific problems encountered with asset forfeiture in large, complex cases. In response to this report, the GON announced several measures to improve the effectiveness of asset seizure enforcement, including steps to increase expertise in the financial and economic field, assign extra public prosecutors to improve the coordination and handling of large, complex cases, and establish a specific asset forfeiture fund.

Terrorist financing is a crime in the Netherlands. The “Sanction Provision for the Duty to Report on Terrorism” was passed in 1977 and amended in June 2002, to implement European Union (EU) Regulation 2580/2001 and UNSCR 1373. This ministerial decree provides authority to the

Netherlands to identify, freeze, and seize terrorist finance assets. The decree also requires financial institutions to report to the MOT all transactions (actually carried out or intended) that involve persons, groups, and entities that have been linked, either domestically or internationally, with terrorism. Any terrorist crime will automatically qualify as a predicate offense under the Netherlands “all offenses” regime for predicate offenses of money laundering. Involvement in financial transactions with individuals and/or organizations designated nationally, by the EU, or by the UN has been made a criminal offense. The Dutch Finance Ministry, in close coordination with the Foreign Affairs Ministry, distributes lists of designated entities to financial institutions and relevant government bodies (including local tax authorities). Freezing of assets is an administrative procedure. The Netherlands has frozen more terrorist related assets than any other EU member state.

The Act on Terrorist Offenses took effect on August 10, 2004. The new Act introduces Article 140A of the Criminal Code, which criminalizes participation in an organization when the intent is to commit acts of terrorism, and defines participation as membership or providing provision of monetary or other material support. Article 140A carries a maximum penalty of fifteen years’ imprisonment for participation in and life imprisonment for leadership of a terrorist organization. The Netherlands Security Service investigates terrorist financing, and is cooperating with law enforcement entities that are experienced in this area.

Dutch civil law requires registration of all active foundations in the registers of the Chambers of Commerce. Each foundation’s formal statutes (creation of the foundation must be certified by a notary of law) must be submitted to the Chambers. Charitable institutions also register with, and report to, the tax authorities in order to qualify for favorable tax treatment. Approximately 15,000 organizations (and their managements) are registered in this way. The organizations have to file their statutes, showing their purpose and mode of operations, and submit annual reports. Samples are taken for auditing. Data about informal hawala banking as a potential money laundering/terrorist financing source is still scarce. The Ministry of Justice has ordered a study in this field, to be published shortly.

The Netherlands is in full compliance with all Financial Action Task Force (FATF) Recommendations, with respect to both legislation and enforcement. The Netherlands also complies with the EU Second Money Laundering Directive, and in some areas, is ahead of the EU legislation (such as full money laundering controls on money remitters, including licensing and identification of customers). In December 2003, the International Monetary Fund (IMF) conducted an assessment of the Netherlands’ anti-money laundering and counterterrorist financing system. The Report on the Observance of Standards and Codes (ROSC), released in September 2004, indicates that the Netherlands has a sound anti-money laundering and counterterrorist financing framework.

In December 2004, the Dutch EU Presidency reached a political agreement within the EU on the Third Money Laundering Directive. The Dutch have already implemented some obligations resulting from this directive, such as effective supervision of currency exchange offices and trust companies. In November 2004, the Dutch EU Presidency also reached political agreement within the EU on a regulation controlling cross-border cash movements.

The MOT supervised the PHARE Project for the European Union (March 2002-December 2003). The PHARE Project was the European Commission’s Anti-Money Laundering Project for Economic Reconstruction Assistance to Estonia, Latvia, Lithuania, Poland, the Czech Republic, Slovakia, Hungary, Slovenia, Romania, Bulgaria, Cyprus, and Malta. The purpose of the project was to provide support to Central and Eastern European countries in the development and/or improvement of anti-money laundering regulations. For this purpose, the MOT established a project team and a consortium of international experts. Although the PHARE project concluded in December 2003, the MOT will still move forward with the enhancement of the FIU.NET Project, (an electronic exchange of current information between European FIUs by means of a secure web). Currently, there are eight countries

connected to the FIU.NET in Central and Eastern Europe. A representative of the Dutch MOT is assisting the Surinamese government in establishing a FIU.

The United States enjoys good cooperation with the Netherlands in fighting international crime, including money laundering. In September 2004, the United States and the Netherlands signed two agreements in the area of mutual legal assistance and extradition, stemming from the agreements that were concluded in 2003 between the EU and the United States. One of the amendments to the existing bilateral agreement is the exchange of information on bank accounts. The MOT has established close links with the U.S. Treasury's FinCEN and is also involved in efforts to expand international cooperation between disclosure offices.

The Netherlands is a member of the FATF and participates in the Caribbean Financial Action Task Force as a Cooperating and Supporting Nation. The MOT is a member of the Egmont Group. MOT has concluded formal information sharing MOUs with Belgium, Aruba and the Netherlands Antilles. 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." The Netherlands is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

The Netherlands should continue the strong enforcement of its anti-money laundering program and its leadership in the international arena.

Netherlands Antilles

The Netherlands Antilles, 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 Willemstad, the capital of Curacao, which is also the financial center of the five islands. Narcotics-trafficking and a lack of border control between Sint Maarten and St. Martin create opportunities for money launderers in the Netherlands Antilles. The Netherlands is reported to be the most significant source of suspicious transactions. Of note is the surge over the past few years of remittance transfers from the Netherlands.

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 approximately 18,750 international companies, mutual funds, and international finance companies. The laws 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. In early 2003, legislation was introduced to transfer supervision of the trust sector to the Central Bank. International corporations may be registered using bearer shares. The practice of the financial sector in the Netherlands Antilles is for either the bank or the company service providers to maintain copies of bearer share certificates for international corporations, which include information on the beneficial owner(s). 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.

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.

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. Thus, it is

sufficient to establish that the money launderer knew, or should have known, of the money's illegal origin.

In recent 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; introducing indicators for the reporting of unusual transactions for the gaming industry; issuing guidelines to the banking sector on detecting and deterring money laundering; and modifying existing money laundering legislation that penalizes currency and securities transactions, by including the use of valuable goods. The 2002 "National Ordinance on the Supervision of Fiduciary Business," institutes a Supervisory Board that oversees the international financial sector. At the same time, GONA subjected the members of this sector to know-your-customer rules. A GONA interagency anti-money laundering working group cooperates with its Kingdom counterparts.

Onshore banks are increasingly using their discretionary authority to protect themselves against money laundering. The largest commercial bank lowered its limits on moneygrams to \$2,000. Banks are reluctant to do business with the Internet gaming providers, provoking complaints from that sector. In 2003 Curacao was reported to have six sports booking sites and 100 Internet casinos. The MOT NA has issued a manual for casinos on how to file reports and has started to install software in casinos that will allow reports to be submitted electronically.

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, and also applies to courier services. Declaration of currency exceeding the limit must include origin and destination. There is a fine of up to NAF 500,000 (approximately \$280,900) or one year in prison. In July 2003, Sint Maarten Customs seized \$11,500 from a traveler, and in August 2003, \$20,000 in undeclared currency was seized from a Curacao passenger.

Unusual transactions are by law reported to the Financial Intelligence Unit (FIU), the Netherlands Antilles Reporting Center, Meldpunt Ongebruikelijke Transacties (MOT NA). On June 1, 2003, the Central Bank issued new consolidated reporting guidelines, replacing those of 1996. These guidelines are more closely focused on banks, insurance companies, pensions funds, money transfer services, and financial administrators now specifically include counterterrorism detectors. The Central Bank also established a Financial Integrity Unit to monitor corporate governance and market behavior. Entities under supervision must submit an annual statement of compliance.

The current staff of seven at the MOT NA continues to work diligently to enhance the effectiveness and efficiency of its reporting system. 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. All are now done on-line, and most of the matches with external databases will be done electronically. The MOT NA transmits information electronically to the police. 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, money transfers and game of chance transactions.

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.

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 the Taliban or 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.

Netherlands Antilles law allows the exchange of information between the MOT NA and foreign FIUs by means of memoranda of understanding and by treaty. The MOT NA's policy is to answer requests within 48 hours after receipt, although this timeframe is not always met. An agreement was signed in April 2002 between the Netherlands and the United States, which is also applicable to the Netherlands Antilles, for the exchange of information with respect to taxes. This agreement was scheduled to come into force in January 2004. The Mutual Legal Assistance Treaty between the Netherlands and the United States also applies to the Netherlands Antilles. In September 2003, the U.S. Attorney in St. Thomas indicted five defendants, including one from Sint Maarten, for charges including laundering funds totaling \$68 million. Cooperation with Sint Maarten under the MLAT was an important element in the investigation.

The MOT NA is an active member of the Egmont Group. The Netherlands Antilles is a member of the Caribbean Financial Action Task Force (CFATF), and as part of the Kingdom of the Netherlands, the Netherlands Antilles participates in the FATF. In 1999, the Netherlands extended application of the 1988 UN Drug Convention to the Netherlands Antilles. The Kingdom of the Netherlands became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2002. In accordance with Netherlands Antilles law, which stipulates that all the legislation must be in place prior to ratification, the GONA is preparing legislation that will enable the Netherlands Antilles to ratify the Convention.

The Government of the Netherlands Antilles has shown a commitment to combating money laundering by establishing a solid anti-money laundering regime. An increase to the MOT NA staff is particularly notable. The Netherlands Antilles should continue its focus on increasing regulation and supervision of the offshore sector and free trade zones and pursuing money laundering investigations and prosecutions. The Netherlands Antilles should criminalize the financing of terrorists and terrorism, and should enact the necessary legislation to implement the UN International Convention for the Suppression of the Financing of Terrorism.

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 criminalizes laundering the proceeds of a serious offense, if the launderer knew or believed that the proceeds were derived from a serious offense. In 2003, the law was extended to apply to those who are reckless as to whether the laundered property is the proceeds of 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, criminalizes terrorist financing. This Act also made the necessary changes to the existing law to enable New Zealand to ratify the UN International Convention for the Suppression of the Financing of Terrorism. 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 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. New Zealand is a member of the Financial Action Task Force, the Asia/Pacific Group on Money Laundering, 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.

The Government of 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

Nicaragua is not a regional financial center, but continues to be a major drug transit zone. This situation makes Nicaragua's financial system an attractive target for narcotics-related money laundering. Nicaraguan officials have expressed concern that, as neighbors have tightened their money laundering laws, established Financial Intelligence Units (FIUs) and taken other actions, more illicit money has moved into the vulnerable Nicaraguan financial system. However, this concern has not resulted in much action on the part of the government. While Nicaragua has pledged to fight terrorist financing, money laundering and other financial crimes, few resources have been allocated to this effort. Nicaragua continues to exercise weak oversight and regulatory control over its financial system. Money laundering unrelated to drug-trafficking is legally undefined, and all attempts to correct this deficiency have been stalled in the National Assembly for years.

Nicaragua does not permit offshore banks to operate as such, but it does permit them to operate through nationally chartered entities (such as a Panamanian bank currently working to establish a savings and loan company under a Nicaraguan charter). Bank and company bearer shares are permitted. Nicaragua has a well-developed indigenous gaming industry, which it is only now moving to control. There are no known offshore or Internet gaming sites in Nicaragua. Nicaragua does not have any "due diligence" or "banker negligence" laws to hold bank officials responsible for their institutions' money laundering.

In 1999, Nicaragua passed Law 285 that requires banks to report cash deposits over \$10,000 to the Superintendence of Banks, which then forwards the reports for analysis to the Commission of Financial Analysis (CAF). The CAF is not a financial intelligence unit. On paper, the CAF is composed of representatives from various elements of law enforcement and banking regulators, and is responsible for detecting money laundering trends, coordinating with other agencies and reporting its findings to Nicaragua's National Anti-Drug Council. In fact, the Commission is a non-functioning entity grossly under-funded and understaffed. Even if the CAF were operational, it is unlikely that it would be effective. In Nicaragua, banks tend to close the suspicious accounts, even as they are

notifying the Bank Superintendence, thereby allowing the money launderers to escape with their capital intact.

Legislation that would improve Nicaragua's anti-money laundering regime has been stalled in the National Assembly for years. Reportedly, this legislation, an amended drug law, would establish money laundering as an autonomous crime, require more stringent reporting of large and/or suspicious bank deposits, and reform and improve the CAF. It is unlikely that this reform legislation or any other major initiative in this area will make it out of the Assembly in the near or medium term.

Draft counterterrorism legislation, which would criminalize terrorist financing, is under consideration by the National Assembly, but remains far from passage. It is possible that many elements of terrorist financing can be prosecuted under existing laws. Nicaragua has the authority—through five Bank Superintendence administrative decrees—to identify, freeze, and seize terrorist-related assets, but has not, as yet, identified any such cases. Reportedly, there are no hawala or other similar alternative remittance systems operating in Nicaragua, and the Nicaraguans have not detected any use of gold, precious metals, or charitable organizations to disguise such transactions.

Nicaragua is currently negotiating a financial information sharing agreement with Costa Rica, largely based on model legislation produced by the Central American Parliament. It does not have such an agreement with the United States, but it cooperated, on an ad hoc basis, in a number of cases in 2004. This cooperation has enabled Nicaragua to benefit from several U.S. asset seizure cases and to recover \$2.7 million stolen by the former Nicaraguan tax director, and used to purchase properties in Florida. Under Law 285, 20 percent of the proceeds from drug-related asset seizures go to each of the following institutions: the Ministry of Health, the National Drug Directorate, the National Police narcotics section, the penitentiary system, and non-governmental organization drug prevention programs.

Nicaragua is a party to the 1988 UN Drug Convention. The country has also ratified the UN Convention on the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Nicaragua is a member of the Organization of American States and the Caribbean Financial Action Task Force.

The Government of Nicaragua should expand the predicate crimes for money laundering beyond narcotics-trafficking and should criminalize terrorist financing. It should also make it a priority to allocate the resources needed to develop a fully functioning financial intelligence unit and to fully implement its anti-money laundering regime. Nicaragua should take steps to immobilize its bearer shares and adequately regulate its gambling industry. These steps would significantly strengthen the country's financial system against money laundering and terrorist financing, and would ensure compliance with relevant international standards regarding anti-money laundering controls.

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 addition, all

foreign currency exchanges over 1 million CFA (approximately \$1,900) require written authorization from the Niger Ministry of Finance.

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. On November 27, 2003, the Niger Council of Ministers adopted a bill that formally prohibits money laundering and puts into place structures and regulations to deter such activity. The

bill became law in June 2004 after passage by the National Assembly. When in force, this law will bring Niger into conformity with the rest of the WAEMU nations. The bill called for the creation of a central office at the BCEAO for the coordination of money laundering issues and formally obliges all financial institutions in Niger to report suspicious activity. The office was established in 2004. Currently, banks in Niger report suspicious activity to the BCEAO and to local law enforcement, although there are no legal requirements to do so. In 2002, one bank account in Niger was frozen due to its relationship to illegal financial activity.

The WAEMU Council of Ministers also issued a directive in September 2002 on the topic of terrorist financing, requesting member countries to pass legislation requiring banks to freeze the accounts of any persons or organizations on the UN 1267 Sanctions Committee's consolidated list. In addition, the Government of Niger (GON) and the BCEAO actively comply with U.S efforts to combat terrorist financing. When notified of persons or entities designated by the UN 1267 Sanctions Committee's consolidated list or the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O 13224, the BCEAO promptly disseminates information to all financial institutions in Niger. Since January 1, 2004, there have been no reported cases of money laundering or terrorist financing in Niger.

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. In April 2004, The National Assembly adopted a domestic law on money laundering to implement GIABA. In September 2004, Niger ratified the UN Convention against Transnational Organized Crime and acceded to the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Niger should continue to implement all the provisions of the 2004 anti-money laundering laws.

Nigeria

The Federal Republic of Nigeria is the most populous country in Africa and is West Africa's largest democracy. Nigeria's large economy is also a hub of trafficking of persons and narcotics. Nigeria is a major drug-transit county. Nigeria is a center of criminal financial activity for the entire continent. Individuals and criminal organizations have taken advantage of the country's location, weak laws, systemic corruption, lack of enforcement, and poor economic conditions to strengthen their ability to perpetrate all manner of financial crimes at home and abroad. Nigerian criminal organizations have proven adept at devising new ways of subverting international and domestic law enforcement efforts and evading detection. Their success in avoiding detection and prosecution has led to an increase in many types of financial crimes, including bank fraud, real estate fraud, identity theft, and advance fee

fraud. Despite years of government effort to counter rampant crime and corruption, Nigerians continue to be plagued by crime. The Government of Nigeria (GON) has made efforts to counteract these crimes but, despite some successes in 2004, socio-economic conditions have impeded its efforts.

In addition to narcotics-related money laundering, advance fee fraud is a lucrative financial crime that generates hundreds of millions of illicit dollars annually for criminals. Initially, Nigerian criminals made advance fee fraud infamous; more recently, nationals of many African countries and from a variety of countries around the world have begun to perpetrate advance fee fraud. This type of fraud is referred to internationally as “Four-One-Nine” fraud (419 is a reference to the fraud section in Nigeria’s criminal code). While there are many variations, the main goal of 419 fraud is to deceive 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. Through the Internet, businesses and individuals around the world have been and continue to be targeted by perpetrators of 419 scams.

In June 2001, the Financial Action Task Force (FATF) placed Nigeria on its list of noncooperative countries and territories (NCCT) in combating money laundering. Among the deficiencies cited by the 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 a 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, the 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 2002, the FATF recommended countermeasures against Nigeria if the Government of Nigeria (GON) did not enact sufficient legislative reforms by December 15, 2002. That same month, Nigeria submitted an anti-money laundering implementation plan to the FATF, but it was deemed insufficient to justify delisting Nigeria.

On December 14, 2002, the National Assembly of Nigeria passed three pieces of anti-money laundering legislation, and President Olusegun Obasanjo signed the legislation into law the same day: an amendment to the 1995 Money Laundering Act that extends the scope of the law to cover the proceeds of all crimes; an amendment to the 1991 Banking and Other Financial Institutions (BOFI) Act that expands coverage of the law to stock brokerage firms and foreign currency exchange facilities, gives the Central Bank of Nigeria (CBN) greater power to deny bank licenses and allows the CBN to freeze suspicious accounts; and the Economic and Financial Crimes Commission (Establishment) Act that establishes the Economic and Financial Crimes Commission (EFCC), that coordinates anti-money laundering investigations and information sharing. The Economic and Financial Crimes Commission Act (2002) also criminalizes the financing of terrorism and participation in terrorism. Violation of the Act carries a penalty of up to life imprisonment. Based on this legislation, FATF decided not to recommend countermeasures against Nigeria; however, Nigeria remains on the NCCT list.

In April 2003, the EFCC was formally constituted, with the primary mandate to investigate and prosecute financial crimes. It has recovered or seized assets from various people guilty of fraud inside and outside of Nigeria, including a syndicate that included highly placed government officials who were defrauding the Federal Inland Revenue Service (FIRS). Several influential individuals have been arrested and are currently awaiting trial. In an effort to expedite the trial process, the Commission has been assigned two high court judges in Lagos and two in Abuja to hear all cases involving financial

crimes. This signals intent by the government to more aggressively investigate “419” and other economic crimes in Nigeria.

In 2004, the National Assembly passed the Money Laundering (Prohibition) Act (2004), which applies to the proceeds of all financial crimes. It also covers stock brokerage firms and foreign currency exchange facilities, in addition to banks and financial institutions. The legislation gives the CBN greater power to deny banks licenses and freeze suspicious accounts. This legislation strengthens the financial institutions by also requiring more stringent identification of accounts, removing a threshold for suspicious transactions, and lengthening the period for retention of records.

However, in November 2004, the Chairman of the EFCC stated publicly that over 90 percent of Nigeria’s banks were not in compliance with the new law. He said that banks were not adhering to the know-your-customer and know-your-customer’s-business provisions of the law, and that 95 percent of banks had not yet filed any suspicious transactions reports (STRs), something he deemed “suspicious by itself.” However, he vowed to promulgate a new initiative to educate bank personnel and the general public about the provisions of the law before he began imposing sanctions for non-compliance.

The EFCC recorded some successes in 2004 in the area of combating money laundering, including the arrest of several notorious advance fee fraud kingpins, who are currently being prosecuted. These include a group involved in the Brazilian bank scam that totaled \$242 million. The EFCC seized assets worth about \$300 million in 2004. The EFCC was involved in the prosecution of more than 100 high-profile financial crime cases in the Nigerian High Court, including bank fraud, tax evasion, and money laundering. For the first time in the history of the country, a sitting provincial governor is being tried for corruption and money laundering, and several other money laundering cases are being tried. There was one money laundering conviction in 2004. The EFCC established a Financial Intelligence Unit (FIU) in 2004 that is now receiving and analyzing STRs. However, as noted above, very few such reports have yet been filed.

Nigeria is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. On December 9, 2003, Nigeria signed the UN Convention against Corruption. The United States and Nigeria have a Mutual Legal Assistance Treaty, which entered into force in January 2003. Nigeria has signed memoranda of understanding with Russia, Iran, India, Pakistan, and Uganda to facilitate cooperation in the fight against narcotics-trafficking and money laundering. Nigeria has also signed bilateral agreements for exchange of information on money laundering with South Africa, the United Kingdom, and all Commonwealth and Economic Community of West African States countries. Nigeria has been instrumental in the establishment of a permanent secretariat for the Intergovernmental Task Force Against Money Laundering in West Africa (GIABA).

The Government of Nigeria should continue to engage with the FATF to ensure that Nigeria’s remaining anti-money laundering deficiencies are corrected. It should also bolster the Economic and Financial Crimes Commission by ensuring that it is adequately funded. Nigeria should construct a comprehensive anti-money laundering regime that willingly shares information with foreign regulatory and law enforcement agencies, is capable of thwarting money laundering and terrorist financing, and comports with all relevant international standards. Nigeria should criminalize the financing of terrorism consistent with the UN International Convention for the Suppression of the Financing of Terrorism.

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 international business companies. Marketers of offshore services promote Niue as a favored jurisdiction for establishing IBCs, for a variety of reasons. The presence of a significant number of international business companies operating offshore makes Niue particularly vulnerable to money laundering. With a population of roughly 2,100, Niue reported that it had registered 9,229 IBCs as of December 2003. Allowed under Niue's International Business Companies Act 1994, the IBCs are not required to disclose their beneficial ownership or to keep a register of directors. Moreover, Niue allows bearer shares and the marketing of shelf companies, which are offered by Internet marketers complete with associated offshore bank accounts and mail-drop forwarding services. The IBCs are legally formed and registered by a Panamanian law firm on Niue's behalf. The government reported in December 2003 that it had not registered any offshore financial service businesses, such as insurance companies, mutual fund companies, trust companies, and agents.

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 no relevant procedures in place to deal with their possible collection and analysis. Currently, the Proceeds of Crime Act allows the court to order the confiscation or forfeiture of property derived from a serious offense, once the offender has been convicted. The Act does not specifically address assets derived from narcotics-trafficking, terrorism financing, or organized crime. The government is working to amend the Act to allow it to freeze transactions in which money laundering or terrorism financing is suspected.

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 their 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. To date, no movement has been made towards the establishment of any operational FIU, domestic or regional.

Should a Niuean FIU become operational, financial institutions will be required to prepare a written statement of their internal procedures to make their officers and employees aware of the laws in Niue about money laundering; the procedures, policies, and audit systems adopted by the institution to deal with money laundering; and procedures to train the institution's officers and employees to recognize and deal with money laundering. The institutions then will have to submit the statement of those procedures to the FIU. The FIU will also have powers to conduct investigations to ensure compliance by financial institutions with the Financial Transactions Reporting Act 2000. Currently, casinos and notaries are not covered within the definition of "financial institution" under the Act, but the government is considering promoting an amendment that would substitute the definition of "financial institution" from the IMF model Financial Transactions Reporting Act.

The Financial Transactions Reporting Act 2000 provides that one of the functions of the financial intelligence unit is to issue guidelines to financial institutions in relation to transaction record keeping and reporting obligations and to provide training programs for financial institutions about transaction record keeping and reporting obligations.

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 the island by a registered agent and is accessible to appropriate officials.

Due to these reforms, the Financial Action Task Force (FATF) decided in October 2002 that Niue had in place an anti-money laundering system that generally meets international standards. Niue was therefore removed from the list of Non-Cooperative Countries or Territories (NCCT), on which it had been placed in June 2000. With Niue's removal from the NCCT list, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) lifted its advisory that had instructed all U.S. financial institutions to "give enhanced scrutiny" to all transactions involving Niue.

Niue is not a member of the United Nations. In November 2001, the government amended the United Nations Act 1946 to enable the Cabinet to promulgate regulations giving effect to UN Security Council resolutions. And, in September 2003, the Cabinet passed the United Nations Sanctions (Terrorism Suppression and Afghanistan Measures) Regulations 2003. Those regulations implement UN Security Council Resolution 1373, as well as Resolutions 1267 and 1333.

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.

The Government of Niue's 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 Financial Intelligence Unit (FIU). Niue must ensure that the recently enacted reforms are fully and effectively implemented. Additionally, Niue should criminalize terrorist financing.

Norway

Norway is not considered an important regional financial center. However, criminal activity, particularly connected with narcotics and economic crime, is increasing in Norway. According to Oekokrim, the economic crime unit of the Ministry of Justice, which serves as Norway's Financial Intelligence Unit (FIU), the rise in crime has been marked by increases in specialization, cooperation

between criminal networks, links between criminal and legal business activities, and the use of advanced technologies. Violent and professional armed robberies, often by foreigners, have also become more frequent. Authorities suspect that the proceeds of the robberies are laundered through registered companies formally or informally controlled by the criminals. Most money laundering occurs outside the banking and financial services system of Norway, due to the reporting requirements of the financial institutions; however, structuring of deposits still appears to be a problem within the financial system. Norway does not have a significant market for smuggled goods. Norway has neither free trade zones nor an offshore banking system.

In accordance with the Norwegian Penal Code, all forms of money laundering are criminal offenses. Norway's anti-money laundering legislation has been strengthened in recent years to conform to the Financial Action Task Force (FATF) Forty Recommendations. In 2004, a new Money Laundering Law took effect, replacing the provisions of the 1988 Financial Institutions Act. The new act strengthens registration requirements, broadens the obligation to report suspicious transactions, and makes negligent contravention of the act a criminal offense.

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.

All financial institutions are required to report large and suspicious transactions to Oekokrim, verify the identity of their customers, and keep records of transactions for at least five years. Money laundering controls are also applied to all non-bank financial institutions, such as insurance companies. Financial institutions are required to report large cash transactions, including cross-border transactions, to the Norwegian Central Bank, specifying sender and recipient information. Norway has not enacted secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law-enforcement authorities. Individual bankers may be held responsible if their institutions launder money; however, the law protects reporting individuals. The number of money laundering infractions reported by traditional financial institutions decreased during the first half of 2004. Oekokrim's money laundering unit attributes the decline to the financial institutions' initial uncertainty regarding procedures under the new Money Laundering Act and to their decision to focus on the most serious and complex cases.

Through June 30, 2004, Norwegian authorities initiated 292 money laundering investigations. A total of 245 cases resulted in indictments or fines, and there were 100 court convictions for money laundering. Most money laundering cases in Norway are related to domestic criminal activity, and no terrorist groups are known to have laundered funds in the country.

According to Norwegian laws, assets derived from criminal acts (narcotics-trafficking, money laundering, and support for terrorism), are to be seized and confiscated by the State. Oekokrim continues to establish systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets and remains the principal entity responsible for tracing and seizing assets, although any police unit may do so in Norway. Section 34 of the Penal Code establishes that confiscation is mandatory unless a court finds that the confiscation is unreasonable. In serious cases, the law allows for extended confiscation. The offender must be found guilty of a criminal act from which considerable proceeds are accrued. Considerable proceeds are defined as at least NOK 75,000 (\$12,000). Legitimate businesses may be seized if they are used to launder drug money or support terrorist activity, or are linked to other criminal proceeds. Substitute assets may be seized. Norway destroys seized drugs, alcohol, and cigarettes, but auctions off other items, including automobiles, private property, and buildings. The State receives the proceeds from the asset seizures and forfeitures.

The law allows civil as well as criminal forfeiture. In 2003 authorities issued 929 confiscation orders totaling over \$24 million. To date, Norway has not enacted laws for sharing narcotics assets with other countries.

On June 28, 2002, Norway enacted Section 147 (A-B) of the Penal Code, criminalizing the financing of terrorism. The new bill establishes legislative measures against acts of terrorism and the financing of terrorism, which fulfill the requirements of the UN International Convention for the Suppression of the Financing of Terrorism. The law applies to anyone who supplies funds to, or collects funds for, individuals or groups that plan acts of terrorism, and makes the support of terrorists with equipment or services a criminal offense. Norway has the authority to identify, freeze, and seize terrorist financial assets. There were no arrests or prosecutions for terrorist financing, and Oekokrim did not receive any suspicious transaction reports related to terrorism in 2004. Authorities have investigated one suspected instance of terrorist financing, but the case was dropped in 2004.

On October 11, 2002, Norway adopted the European Union's (EU's) Common Position on the application of specific measures to combat terrorism. The Common Position details the names of major terrorists groups. Norway has also distributed to financial institutions the UNSCR 1267 Sanctions Committee's consolidated list. In accordance with UNSCR 1267, the bank account of one individual has been frozen since February 2003. The amount frozen was approximately \$1,000.

Alternative remittance systems are prohibited in Norway. In November 2004, a Norwegian appellate court upheld the convictions of three Somalis accused of violating banking regulations by sending unauthorized remittances overseas. The prosecutor in the case reported that the men illegally remitted approximately \$6 million annually between 1998 and 2001. The ringleader of the scheme was sentenced to a one-year jail sentence and his two accomplices were fined approximately \$1,500 each.

Norway works with Europol and is a member of the FATF, Interpol, and Schengen. Oekokrim is a member of the Egmont Group. Norway is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Corruption. Norway is also a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the UN International Convention for the Suppression of the Financing of Terrorism; and the UN Convention against Transnational Organized Crime. Norway has now ratified all 12 of the International Conventions and Protocols relating to terrorism. Norway consults frequently with United States authorities in connection with investigations and proceedings related to narcotics, terrorism, terrorist financing, and other crimes. Norway's Money Laundering Act and Terrorist Financing Law ensure the availability of adequate records in connection with investigations of interest to the United States and other governments.

The Government of Norway should continue to enhance its anti-money laundering/counterterrorist financing regime. Norway should consider the adoption of laws that would allow the sharing of seized assets with third party jurisdictions that assisted in the conduct of the underlying investigation.

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. In 2004, Oman had a total of 17 banks with 353 branches. The banking system consisted of five local commercial banks with 304 Omani and 11 foreign branches, three local specialized banks with 26 local branches, and nine foreign incorporated banks with 23 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 instances of trade-based money laundering and customs fraud as well as unregulated lending schemes that fall outside government purview.

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. In a 2003 report to the UN Counter-Terrorism Committee, Omani officials stated that “the legal freezing measures designated by the Money laundering Act are applied to both residents and non-residents holding funds, financial assets, or other economic resources in the Sultanate of Oman if they are linked to terrorist-related activities.” In addition to an interagency committee for Anti-Money Laundering, the Sultanate has established a senior-level National Committee for Combating Terrorist Finance.

Royal Decree 72/2004 of July 7, 2004 promulgated the implementing regulations for the Law of Money Laundering. These regulations include, inter alia, the following provisions: a requirement that financial institutions “take steps to obtain information on customers who open accounts in an indirect way” and “keep electronic data on e-transactions”; guidelines in the area of profiling, requiring institutions to “check and double-check” certain classes of transactions (e.g., “customers getting loans from foreign institutions” and the “keeping of accounts that do not match the business nature”); requirements for government authorities to investigate all “suspicious dealings” using internal and external reporting mechanisms; authorization for the attorney general to freeze disputed assets upon the request of investigators; protection of “secret” information; an extensive training program, with introductory courses supplemented by instruction in international best practices and effective investigation techniques; definition of the organizational structure of the National Committee for Combating Money Laundering; and, cooperation with international organizations and information exchange with other countries, including collaboration on extradition issues.

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. Compliance personnel are now present in all banks. Oman plans to establish a Financial Intelligence Unit (FIU) that will review suspicious transactions and help coordinate resulting investigations. As of the end of 2004, there had been no arrests under the new law. No formal mechanism currently exists for information sharing among the Central Banks or FIUs of the Gulf Cooperation Council (GCC) members, although a banking supervision committee within the GCC does issue broad guidelines for financial institution oversight.

Oman regulates charitable organizations under the Non-Governmental Organizations Act promulgated pursuant to Royal Decree 14/2000. Under this act, the Minister of Social Development is responsible for approving and monitoring all charitable contributions and fundraising activities. There is a government-registered charity (the Oman Charitable Organization, or OCO), and all citizens and entities are encouraged to use this official channel for donations. The Ministry of Social Development recently registered a charity fund run by a prominent local businessman. At various times, charitable donations have been collected through individual accounts in local banks and sent abroad by individuals to support different causes, such as the Palestinian Intifada and the building of schools or mosques in Africa and South Asia. The local Shia minority is believed to transfer money to support their religious imams, mainly in Iraq and Iran. Apart from monthly remittances by expatriate laborers, local Indian businessmen have also been reported to channel funds in support of Hindu religious groups. In all of these cases, the CBO possesses the authority and ability to check on these accounts, as all banks and moneychangers have the obligation to report on transactions.

Informal lending societies reportedly have emerged in recent years as a popular alternative to formal banking in Oman. These societies provide interest free loans as a means for young Omanis to purchase homes and cars or service bank debts. The societies became the target of three separate warnings from the Ministry of Social Development calling on Omanis to avoid these unregulated and unregistered financial entities. Nevertheless, many Omanis flocked to these societies in solidarity with members of

their tribes and in protest against double-digit interest rates being charged by commercial banks. Later, as membership numbered in the thousands, serious problems emerged as several founding members absconded with funds from their societies. Suspicious members withdrew from the schemes, causing the collapse of many societies. Transactions in these societies are made in cash, and the societies are not registered with any government agency or institution. While such practices constitute only a fraction of overall financial transactions in Oman, they merit greater scrutiny on the part of ROP and CBO authorities. Reports of excess liquidity in the Omani financial system and the demonstrated popularity of informal societies lend credence to the view that a significant amount of wealth, amounting to hundreds of thousands if not millions of dollars, is circulating outside the formal financial system and its strict regulations, auditing requirements, and accountability to the CBO.

Oman has responded to terrorist asset freeze lists from the UN 1267 Sanctions Committee by distributing the lists to all banks and other financial institutions in the country for checking against their accounts. Thus far, the Government has reported negative results. Oman is a party to the 1988 UN Drug Convention. Although not yet a party to the UN International Convention for the Suppression of the Financing of Terrorism, Omani officials insist that Oman will soon accede. Oman has yet to sign the UN Convention against Transnational Organized Crime. Oman is a member of the Gulf Cooperation Council (GCC), which itself is a member of the Financial Action Task Force (FATF). Oman is also a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004. The MENAFATF is a FATF-style regional body. The creation of the MENAFATF is critical for pushing the region to improve the transparency and regulatory frameworks of its financial sectors.

Overall, the Government of Oman maintains a strong and effective regulatory regime with respect to its formal financial institutions. Oman should continue to implement its anti-money laundering program, specifically by establishing and dedicating adequate resources to its Financial Intelligence Unit (FIU) and training criminal investigators to initiate money laundering investigations from the field. Oman also should address the risks of alternative remittance systems and unregulated lending societies to launder money and sidestep formal government oversight of financial transactions. Applying the careful lessons learned in its tight regulation of the formal sector, Oman must now recognize that informal money transfer and cash-based lending societies represent vulnerabilities that must be addressed. Oman should sign and ratify both the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

Pakistan

Financial crimes related to narcotics-trafficking, terrorism, smuggling, tax evasion, and corruption remain a significant problem in Pakistan. Pakistani criminal networks play a central role in the transshipment of narcotics and smuggled goods from Afghanistan to international markets. Pakistan is a major drug-transit country. 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 network of private unregulated charities has also emerged as a major source of illicit funds for international terrorist networks.

Pakistan's current anti-money laundering regime is weak, outdated and based on a loose patchwork of laws and regulations. The major laws include: The Anti-Terrorism Act of 1997 (amended in October 2004 to increase maximum punishments), which defines the crimes of terrorist finance and money laundering and establishes jurisdictions and punishments; The National Accountability Ordinance of 1999, which requires financial institutions to report suspicious transactions to the National Accountability Bureau (NAB) and establishes accountability courts; and The Control of Narcotic Substances Act of 1997, which also requires the reporting of suspicious transactions, contains

provisions for the freezing and seizing of assets associated with narcotics-trafficking, and establishes special courts for offenses (including financing) involving illegal narcotics. The State Bank of Pakistan (SBP) and the Securities and Exchange Commission of Pakistan (SECP) regulate financial flows.

Since 2002, Pakistan's Ministry of Finance has been coordinating an interministerial effort to draft anti-money laundering and counterterrorist financing legislation, with the goal of bringing Pakistan into compliance with international norms. As of December 2004, this legislation had not received final cabinet approval, and therefore, had not been submitted to the National Assembly for enactment. The latest version of that legislation was reviewed by a delegation from a FATF-style regional body, the Asia/Pacific Group on Money Laundering (APG), in December 2004. The draft law, among other things, provides for a Financial Intelligence Unit (FIU), which does not currently exist in Pakistan.

Notwithstanding the absence of such legislation, the SBP, which serves as Pakistan's Central Bank, has created an anti-money laundering unit. It has also introduced FATF-compliant regulations in the areas of know-your-customer policy, record retention, due diligence of correspondent banks, and the reporting of suspicious transactions. The SECP, which has regulatory oversight for non-bank financial institutions, has applied know your customer regulations to stock exchanges, trusts, and other non-bank financial institutions. All transactions exceeding RS 50,000 (approximately \$847) must be carried out via check or bank draft, as opposed to cash. The NAB, the Anti-Narcotics Force, the Federal Investigative Agency, and the Customs authority oversee Pakistan's anti-money laundering efforts. The National Accountability Bureau has been effective in investigating and prosecuting corruption, but has been accused of political bias in selecting its targets.

Pakistan's cooperation in Operation Enduring Freedom has brought renewed focus on the role of informal financial networks in financing terrorist activity. In June 2004, the SBP required all hawalas to register as authorized foreign exchange dealers and to meet minimum capital requirements. Failure to comply was punished by forced closures. However, despite increased enforcement efforts, unregistered hawalas continue to operate illegally. A large percentage of hawala transfers to Pakistan consists of the repatriation of wages from the roughly five million Pakistani expatriates residing abroad. Nevertheless, the U.S. Government has observed a migration of an increasing number of transactions from the informal to the formal financial institutions sector, due to the GOP's regulation of the domestic hawala business, post-September 11 changes in the patterns of behavior of overseas Pakistanis, and a substantial increase in credit available in the formal financial sector.

There have been reports of money laundering in Pakistan using gold and gems, as well as cash transfers by couriers. Pakistani criminal networks play a central role in the transshipment of narcotics and smuggled goods from Afghanistan to international markets. 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. A nexus of private, unregulated charities has also emerged as a major source of illicit funds for international terrorist networks. As of December 28, 2004, Pakistan's Central Bank had frozen roughly \$10.5 million belonging to 12 entities and individuals, in compliance with UNSCR 1267.

Pakistan is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. As of December 2004, Pakistan had not signed the UN International Convention for the Suppression of the Financing of Terrorism. Pakistan became a member of the APG in 2000.

The Government of Pakistan should move quickly to enact anti-money laundering and counterterrorist financing legislation that conforms to international standards. It also should issue financial regulations that mandate the reporting of all suspicious transactions, and establish a Financial Intelligence Unit. In addition, in light of the role that private charities have played in terrorist financing, Pakistan should develop a system to regulate the finances of charitable organizations and to shut down those that finance violence and terrorism. Pakistan should ratify both the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of Terrorist Financing. Greater efforts are also needed to track and suppress trade-facilitated money laundering.

Palau

Palau is an archipelago of more than 300 islands in the Western Pacific with a population of nearly 20,000 and per capita GDP of about \$6,000. Upon its independence in 1994, the Republic of Palau entered the Compact of Free Association with the United States. The U.S. dollar is legal tender. Palau is not a major financial center. Nor does it offer offshore financial services. There are no offshore banks, trust companies, securities brokers/dealers or casinos in Palau. Palauan authorities believe that drug trafficking and prostitution are the primary sources of illegal proceeds that are laundered. Palau recently prosecuted its first ever case under the Money Laundering and Proceeds of Crimes Act (MLPCA) of 2001 (MLPCA) against a foreign national engaged in a large prostitution operation. The defendant was convicted on all three counts as well as a variety of other counts.

Amid reports in late 1999 and early 2000 that offshore banks in Palau had carried out large-scale money laundering activities, a few international banks banned financial transactions with Palau. In response, Palau established a Banking Law Review Task Force that recommended financial control legislation to the Olbill Era Kelulau (OEK), the national bicameral legislature, in 2001. Following that, Palau took several steps toward addressing financial security through banking regulation and supervision and putting in place a legal framework for an anti-money laundering regime. Several pieces of legislation were enacted in June 2001.

The Money Laundering and Proceeds of Crimes Act (MLPCA) of 2001 criminalized money laundering and created a financial intelligence unit. This legislation imposes threshold and suspicious transactions 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 funds of currency or securities involving a sum greater than \$10,000. All such transactions (domestic and/or international) are required to go through a credit or financial institution licensed under the laws of the Republic of Palau.

The Financial Institutions Act of 2001 established the Financial Institutions Commission, an independent regulatory agency, which is responsible for licensing, supervising and regulating financial institutions, defined as banks and security brokers and dealers in Palau. Currently, there are seven fully licensed banks in Palau and one with a conditional license. Six of the banks are majority foreign owned, and one is wholly Palauan owned. Three other banks had their licenses invalidated in 2002 and a license of another bank was revoked in 2003. One bank had its license revoked in early 2005 and one bank that is operating on a conditional license has met the conditions for reopening and is now functioning under the supervision of the FIC. Other entities subject to the provisions of the MLPCA, such as the seven money services businesses, two finance companies and five insurance companies, are essentially unsupervised. Once the amendments to the MLPCA are passed, all alternative money remittance systems will be licensed and regulated by the FIC. Credit and financial institutions are required to verify customers' identity and address. In addition, these institutions are required to check for information by "any legal and reasonable means" to obtain the true identity of the principal/party

upon whose behalf the customer is acting. If identification cannot, in fact, be obtained, all transactions must cease immediately.

The lack of both human and fiscal resources has hampered the development of a viable anti-money laundering regime in Palau. The Republic has only recently established a functioning Financial Intelligence Unit (FIU), though its operations are severely restricted by a lack of dedicated human and fiscal resources. The implementing regulations to ensure compliance with the MLPCA have yet to be written but the authorities have stated that they will be drafted once the revisions to the MLPCA have been passed. The will of the Executive branch to comply with international standards, however, was clearly demonstrated by President Remengesau in 2003, when he vetoed a bill that would have extended the deadline for bank compliance and would have reduced the minimum capital for a bank from \$500,000 to \$250,000. Additionally, the President established the Anti-Money Laundering Working Group that is comprised of the Office of the President, the FIC, the Office of the Attorney General, Customs, the FIU, Immigration and the Bureau of Public Safety. The Senate has recently refused to approve the re-nomination of the Chairman of the FIC, Daiziro Nakamura..

Palau has enacted several legislative mechanisms to foster international cooperation. The Mutual Assistance in Criminal Matters Act (MACA), passed in June 2001, enables authorities to cooperate with other jurisdictions in criminal enforcement actions related to money laundering and to share in seized assets. The Foreign Evidence Act of 2001 provides for the admissibility in civil and criminal proceedings of certain types of evidence obtained from a foreign State pursuant to a request by the Attorney General under the MACA. Under the Compact of Free Association with the United States, a full range of law enforcement cooperation is authorized and in 2004 Palau was able to assist the Department of Justice in a money laundering investigation by securing evidence critical to the case and freezing the suspected funds.

Pursuant to the adoption of the Asia/Pacific Group's (APG) mutual evaluation of Palau at its September 2003 Plenary, the Government of Palau (GOP) has proposed amendments to the MLPCA that, if enacted, would strengthen Palau's anti-money laundering regime. Among the more significant proposals are the following: the promulgation of reporting regulations for all covered financial institutions as well as alternative remittance providers; the requirement to obtain the identification of the beneficial owner of any type of account; mandatory reporting of suspicious transaction reports to the FIU regardless of the amount of the transaction; the requirement that any currency transaction over \$5000 be done by wire transfer; the requirement that alternative remittance systems providers report any cash remittance over \$500; and, a burden shifting regime for the seizure and forfeiture of assets upon a conviction for money laundering.

The President has also recently proposed the Cash Courier Act of 2004 that was drafted by the Palau Anti-Money Laundering Working Group.

The Omnibus Terrorism Act is currently pending in the OEK. If enacted with changes proposed by the President of the Republic, the Act would comport with current international standards, including provisions for the freezing of assets of entities and persons designated by the United Nations as terrorists or terrorist organizations, provisions for the regulation of non-profit entities to prevent abuses by criminal organizations and terrorists and provisions for criminalizing the financing of terrorism. The OEK has issued resolutions ratifying Palau's accession to all the United Nation's Conventions and Protocols relating to terrorism.

The Government of Palau has taken several steps toward enacting a legal framework by which to combat money laundering. It has signed Pacific Island Forum anti-money laundering initiatives and as a member of the Asia/Pacific Group on Money Laundering, Palau is committed to implement the Financial Action Task Force Revised Forty Recommendations and its Nine Special Recommendations on Terrorist Financing. As a party to the UN Convention for the Suppression of the Financing of Terrorism, Palau should criminalize the financing of terrorism. In continuing its efforts to comport with

international standards, Palau should enact legislation and promulgate implementing regulations to the MLPCA, as recommended by the APG, including but not limited to establishing funding for the FIU, eliminating the threshold for reporting suspicious transactions and beginning a broad-based implementation of the legal reforms already put in place.

Panama

The economy of Panama is service-based and heavily weighted toward maritime transportation, commerce, tourism, banking, and financial services. Panama is a major drug-transit country. 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's) 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. Despite significant progress to strengthen Panama's anti-money laundering regime since October 2000, money laundering remains a serious threat to the stability of the country's legitimate financial institutions. Panama is a destination for 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 31), captive insurance companies (corporate entities created and controlled by a parent company, professional association, or group of businesses), and trust companies. Transfer of negotiable (bearer) bonds is another potential vulnerability that could be exploited by money launderers. The high volume of trade occurring through the CFZ (there are approximately 2,600 businesses established in the Zone) presents opportunities for trade-based money laundering to occur.

Law No. 41 (Article 389) of October 2, 2000 amended the Penal Code by expanding the predicate offenses for money laundering beyond narcotics-trafficking, to include criminal fraud, arms trafficking, trafficking in humans, kidnapping, extortion, embezzlement, corruption of public officials, terrorism, and international theft or trafficking of motor vehicles. Law No. 41 establishes a punishment of five to 12 years imprisonment and a fine.

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 monies, accounting fraud, insider trading, and the submission of fraudulent data to supervisory authorities. Law No. 1 of January 5, 2004, adds crimes against intellectual property as a predicate offense for money laundering.

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 to the Unidad de Analisis Financiero (UAF), Panama's Financial Intelligence Unit (FIU), currency transactions in excess of \$10,000 and suspicious financial transactions. Law 42 also mandates that casinos, CFZ businesses, the national lottery, real estate agencies and developers, and insurance/reinsurance companies report to the UAF currency or quasi-currency transactions that exceed \$10,000. Furthermore, Law 42 requires Panamanian trust companies to identify to the Superintendencia of Banks the real and ultimate beneficial owners of trusts.

Executive Order 213 of October 3, 2000, amending Executive Order 16 of 1984 relating to trust operations, provides for the dissemination of information related to trusts to appropriate administrative and judicial authorities. Furthermore, in October 2000, Panama's Superintendencia of Banks issued

Agreement No. 9-2000 that defines requirements that banks must follow for identification of customers, exercise of due diligence and retention of transaction records.

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, and also began drafting a law to regulate the operations of pawnshops and exchange houses. It also increased the number of inspections of finance companies it conducted. The Autonomous Panamanian Cooperative Institute 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 CFZ, outlining their responsibilities regarding prevention of money laundering and requirements under Law 42. 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. In 2004, the Stock Commission announced that it would begin investigating suspicious activity.

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, through enhanced communication and information flow, training programs, and technology, at strengthening the capabilities of those government institutions responsible for preventing and combating financial crimes and terrorist financed activities.

In 2002, the Institute of Autonomous Panamanian Cooperatives, UAF, and the U.S. Embassy Narcotics Assistance Section cosponsored a roundtable on money laundering that offered practical training to financial institutions to assist them in meeting the reporting requirements under Law No. 42. In 2003, Panama launched an education program related to prevention of money laundering and terrorist financing. Panama's Banking Association, the Inter-American Development Bank, the Panamanian Government, and the United States Government financed this campaign. Initiatives under this campaign include a crime analysis seminar, a regional seminar on money laundering for banking regulators, and the detection and reporting of suspicious activities for the banking sector. During 2004, the programs included training for the Gaming Control Commission and a seminar for the Hemispheric Congress on the prevention of money laundering. In 2004, more than 5,000 officials from public and private sector institutions received training through this campaign. Participants included representatives from banks, credit unions, real estate agencies, stockbrokers, insurance companies, Colon Free Trade Zone companies, financial institutions, and money order companies.

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 2004, Panamanian Customs continued a 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. Bulk cash shipments, including through Tocumen Airport, continue to be of great concern, with smugglers often under-declaring the amount of cash being brought into the country.

Executive Order No. 163 of October 3, 2000, which amended the June 1995 decree that created the UAF, also allows the UAF to provide information related to possible money laundering directly to the Office of the Attorney General for investigation. Panama has brought cases for domestic prosecution, and the UAF routinely transfers cases to the Unidad de Inteligencia Financiera (UIF) for investigation. During 2004 the Financial Fraud Prosecutor's office investigated 2,459 cases related to financial crimes, 86 of which led to a conviction. These included credit card fraud and fraud involving banking institutions.

GOP cooperation in the investigation of the Western Hemisphere's largest Black Market Peso Exchange money laundering scheme was instrumental in the U.S. conviction in 2002 of Yardená

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. In 2004, Panamanian officials charged former Nicaraguan President Arnoldo Aleman with money laundering crimes. The GOP received cooperation in the investigation from the Government of Nicaragua. Also during 2004, there were investigations into possible money laundering crimes of high-level Costa Rican government officials. Finally, GOP investigators are looking into corruption allegations made against former government officials.

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.

Decree No. 22 of June 2003 gave the Presidential High Level Commission against Narcotics Related Money Laundering responsibility for combating terrorist financing. Law No. 50 of July 2003 criminalizes terrorist financing and gives the UAF responsibility for prevention of this crime. There are no legal impediments to the GOP's ability to prosecute or extradite suspected terrorists. Panama Public Force (PPF) and the judicial system have limited resources to deter terrorists due to insufficient personnel and lack of expertise in handling complex international investigations. On January 18, 2003, the GOP entered into a border security cooperation agreement with Colombia and also increased funds to the PPF to help secure the frontier. In response to United States efforts to identify and block terrorist-related funds, the GOP continues to monitor suspicious financial transactions.

Also, the GOP created the Department of Analysis and Study of Terrorist Activities. This department is tasked with working with the United Nations and the Organization of American States to investigate transnational issues, including money laundering. Panama has an implementation plan for compliance with the Financial Action Task Force (FATF) Forty Recommendations on Money Laundering and its Special Recommendations on Terrorist Financing.

Panama and the United States have a Mutual Legal Assistance Treaty that entered into force in 1995. The GOP has also assisted numerous countries needing help in strengthening their anti-money laundering programs, including Guatemala, Costa Rica, Russia, Honduras, and Nicaragua. Panama also hosted the Seventh Hemispheric Congress on the Prevention of Money Laundering in August 2003. Executive Decree No. 163 authorizes the UAF to share information with FIUs of other countries, subject to entering into a memorandum of understanding or other information exchange agreement. The UAF has signed more than 27 memoranda of understanding with FIUs, including the U.S. FIU, FinCEN.

Panama is active in the multilateral Black Market Peso Exchange Group Directive. In March 2002, the GOP signed the cooperation agreement issued by the working group as part of a regional effort against the black market system. Panama is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD), and is the current Chair of the Caribbean Financial Action Task Force. Panama is also a member of the Offshore Group of Banking Supervisors, and the UAF is a member of the Egmont Group. Panama is a party to the 1988 UN Drug Convention. Panama is a signatory to 11 of the UN terrorism conventions and protocols. During 2002, the GOP became a party to the UN International Convention for the Suppression of the Financing of Terrorism and, in 2004, of the UN Convention against Transnational Organized Crime.

The Government of Panama should continue its regional assistance efforts. It should also 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. In particular, Panama should institute controls over the transfer of bearer bonds.

Papua New Guinea

Papua New Guinea is not a regional financial center. Its banking sector is relatively small. There are currently no laws against money laundering or terrorist financing. However, according to the Government of Papua New Guinea's (GPNG's) September 2003 report to the UN Counter-Terrorism Committee that monitors implementation of UN Security Council Resolution 1373 (CTC) money laundering in Papua New Guinea will be criminalized pursuant to the proposed "Proceeds of Crime Bill." The bill would obligate financial institutions to retain essential financial documents for a specific period of time. Covered transactions will include transmission of funds between Papua New Guinea and a foreign country. The proposed legislation also calls for the communication of suspicious information by financial institutions to the police.

The GPNG continues to consider amending the Criminal Code Act that will cover the collection, recruiting, or soliciting of funds from other countries for terrorists/terrorist purposes. In addition, the National Intelligence Organization (NIO) is in the process of submitting a Plan of Action on counterterrorism and other transnational crimes. The Plan of Action will focus on coordination and sharing of intelligence. Currently interagency coordination does exist to some extent with regard to narcotics, and task force "Centre-points" have also been established to monitor and share intelligence information on drug trafficking, arms smuggling, human trafficking, and other border concerns. However, "financial tracking" is not yet fully developed.

Papua New Guinea is not a party to any bilateral or multilateral treaties on mutual assistance in criminal matters. Reportedly, the GPNG plans legislation in this area. Papua New Guinea is an observer to the Asia/Pacific Group on Money Laundering. The GPNG is not a party to the 1988 UN Drug Convention but is a party to the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Papua New Guinea should enact a comprehensive anti-money laundering regime that criminalizes money laundering related to all serious crimes. Specific counterterrorism legislation implementing UNSCR 1373 and the UN International Convention for the Suppression of the Financing of Terrorism should also be adopted, including criminalizing terrorism and the funding of terrorism. Papua New Guinea should also become a party to the 1988 UN Drug Convention. Papua New Guinea should become a member of the Asia/Pacific Group on Money Laundering.

Paraguay

Paraguay is a principal money laundering center, involving both the banking and non-banking financial sectors. The multi-billion dollar contraband re-export trade that occurs largely on the border shared with Argentina and Brazil facilitates much of the money laundering in Paraguay. Paraguay is a major drug-transit country. The Government of Paraguay (GOP) suspects that proceeds from narcotics-trafficking are often laundered, but is it difficult to determine what percentage of laundered funds is directly generated from narcotics sales. Weak controls in the financial sector, an open border, and minimal enforcement activity for financial crimes allow money launderers and terrorist financiers to take advantage of Paraguay's financial system. Although the Government of Paraguay (GOP) has made some progress in 2004, it will need to pursue more aggressive policies in 2005 in order to increase its effectiveness in combating money laundering and terrorist financing.

Paraguay is particularly vulnerable to money laundering, as little personal background information is required to open a bank account or to make financial transactions in Paraguay. Paraguay is an attractive financial center for neighboring countries, particularly Brazil. Foreign banks are registered in Paraguay and nonresidents are allowed to hold bank accounts, but current regulations forbid banks from advertising or seeking deposits from outside the country. Paraguay is not considered to be an offshore financial center, but the GOP does allow representative offices of offshore banks to maintain

a presence in the country. Shell companies are not permitted; trusts, however, are permitted and are regulated by the Central Bank. The Superintendent of Banks audits financial institutions and supervises all banks under the same rules and regulations. However, there are few effective controls over businesses, and a large informal economy exists outside the regulatory scope of the GOP.

Money laundering in Paraguay is facilitated by the multi-billion dollar contraband re-export trade that occurs largely in the Triborder Area shared by Paraguay, Argentina, and Brazil. Ciudad del Este (CDE), on the border between Brazil and Paraguay, represents the heart of Paraguay's informal economy. The area is well known for arms and narcotics-trafficking, as well as crimes against intellectual property rights. A wide variety of counterfeit goods, including cigarettes, CDs, DVDs, and computer software, are imported from Asia and transported primarily across the border into Brazil, with a significantly smaller amount remaining in Paraguay for sale in the local economy. Some senior government officials, including members of Congress, have been accused of involvement in the smuggling of contraband or pirated goods. To date there have been few criminal investigations, much less prosecutions of senior GOP officials involvement in smuggling contraband or pirated goods) Government officials, in both Paraguay and the United States, also suspect the area to be a source of terrorist financing. Raids in CDE have led to the seizure of 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 develop strategies to implement a formal, diversified economy.

In 2003, the GOP noted that it was trying to introduce "maquilas" (assembly line industries) but had not done so in 2004. The GOP is trying to strengthen its tourism industry by proposing advances to its tourism infrastructure such as the international airport in Asuncion, making it a regional transportation hub for cargo and possibly passenger airlines.) Although currently no formal free trade zones are located within the country, the new customs code implemented in early 2004 provides for the creation of these zones. One is currently being planned in the town of Villeta, near Asunción. These free trade zones will not help reduce money laundering in Paraguay-in fact, the addition of free trade zones may provide additional venues for money laundering.

There are no effective controls on the amount of currency that can be brought into or out of Paraguay. Cross-border reporting requirements are limited to those issued by airlines at the time of entry into Paraguay. Persons transporting \$10,000 into or out of Paraguay are required to file a customs report, but these reports are often not actually collected or checked. Customs operations at the airports or land ports of entry provide no control of the cross-border movement of cash. The non-bank financial sector, particularly exchange houses, are used to move illegal proceeds both from within and outside of Paraguay into the formal banking system of the United States. Most of these funds move from Brazil through Ciudad del Este to the banking sector. Paraguay exercises a dual monetary system in which most high-priced goods are paid for in U.S. dollars. Large sums of dollars generated from normal commercial activity and suspected illicit commercial activity are transported physically from Paraguay through Uruguay to the banking centers in the United States. Within the past year, the GOP has begun to recognize and address the problem of the international transportation of currency and monetary instruments derived from illegal sources.

Bank fraud, which has led to several bank failures, and other financial crimes related to corruption are serious problems in Paraguay. Following bank failures in 2002 and 2003, Paraguay continues to experience problems in the banking industry. In 2004, Citibank decided to end its participation in small-consumer banking in Paraguay, and subsequently closed almost all of its branches nationwide. The GOP continues to work with the U.S. Treasury and Justice Departments to trace, account for, and return the missing \$16 million diverted from the Central Bank in 2002 to private accounts allegedly linked to the family of former President Luis Gonzalez Macchi.

Money laundering is a criminal offense under Paraguay's two anti-money laundering statutes, Law 1015 of 1996 and Article 196 of Paraguay's Criminal Code, adopted in 1997. The existence of the two laws has led to substantial confusion due to overlapping provisions. Under Article 196, the scope of predicate offenses includes only offenses that carry a maximum penalty of five years or more; Law 1015 includes additional offenses. Article 196 also establishes a maximum penalty of five years for money laundering offenses, while Law 1015 carries a prison term of two to ten years. This is particularly significant because, under the 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. Since a defendant cannot be charged with money laundering unless he or she has first been convicted of the predicate offense, many judges are apparently reluctant to prosecute any defendant on money laundering charges because a sentence has already been issued for a predicate offense.

Law 1015 of 1996 also contains "due diligence" and "banker negligence" provisions and applies money laundering controls to non-banking financial institutions, such as exchange houses. Bank secrecy laws do not prevent banks and financial institutions from disclosing information to bank supervisors and law enforcement entities. Additionally, bankers and others are protected under the anti-money laundering law with respect to their cooperation with law enforcement agencies.

Additional provisions of Law 1015 require banks and financial institutions to know and record the identity of customers engaging in significant currency transactions and to report those, as well as suspicious activities, to Paraguay's Financial Intelligence Unit (FIU), the Unidad de Análisis Financiera (UAF). The UAF began operating in 1997 within the Secretary for the Prevention of Money Laundering (SEPRELAD), under the auspices of the Ministry of Industry and Commerce (MIC). However, for many years the UAF had been regarded as ineffective, and was hampered by a burdensome bureaucratic structure, lack of financial support, and the inability to keep trained personnel.

The UAF's weaknesses were reflected in the small number of cases presented to the Public Ministry (Attorney General's office) for prosecution. Before 2001, only one case went to trial, and it was dismissed on procedural grounds. The majority of the cases prepared by the UAF were incomplete and were returned to the UAF by prosecutors for more information or investigation. Serious concerns also exist with regard to UAF's personnel, its handling of confidential information, cumbersome record keeping, and concerns about possible corruption within the FIU. Efforts were made to by the GOP to improve its anti-money laundering capabilities, and in 2003, existing personnel began to be vetted and replaced as appropriate. However, there remains limited exchange of information between U.S. law enforcement agencies and GOP entities on money laundering cases, as a result of a leak of information in 2002. Information is now exchanged on a case-by-case basis.

The banking "Risk Control Division," created in 2003 to replace the Superintendent of Banks' FIU, and eliminate its duplicative function with the UAF, has the primary responsibility of reviewing the records of national financial institutions for suspected terrorist activity. The Risk Control Division is empowered to coordinate information exchange with the Central Banks of other MERCOSUR countries, but has no authority to conduct investigative work associated with financial suspicious activity reports. That remains the purview of the UAF. According to SEPRELAD officials, there has been little coordination or cooperation between the UAF and the Risk Control Division. The two groups are collaborating on a memorandum of understanding (MOU), which will lay out the provisions for increased cooperation. The MOU is scheduled to come into effect early this year. In 2004, the RCD suffered some growing pains, since its inception last year, and is off to a slow start. The division is working on several *casas de cambio* cases among its current caseload.

In 2004 SEPRELAD made significant efforts to improve the UAF's personnel, analytical capabilities, infrastructure, and technical capabilities. All UAF personnel are now vetted and receive significant

analytical training. The UAF is seeking to strengthen its relationship with other financial intelligence units; for example, the UAF is working with the U.S. financial intelligence unit, FinCEN, to re-establish information sharing procedures, which were suspended following an unauthorized disclosure by the GOP of U.S. financial information in 2001. In 2004, SEPRELAD helped to create and coordinate an interagency money laundering working group, whose members include the director of the UAF, the director of the National Anti-Drug Secretariat (SENAD), the assistant attorney general for economic crimes, the director of the customs agency and a criminal appellate judge.

The UAF also increased its role in regional and international anti-money laundering groups, including the Egmont Group and the Financial Action Task Force for South America (GAFISUD). The UAF's director now participates in the GAFISUD FIU Working Group and a committee within the Egmont Group, further expanding Paraguay's role in these organizations. Paraguay will undergo its second mutual evaluation by GAFISUD in 2005.

The new law to improve the effectiveness of Paraguay's anti-money laundering regime, drafted in late 2003, was formally introduced to Congress in May 2004, where it now remains under consideration by legislative committees. The draft law should come before the full Congress for consideration in 2005. The GOP is also in the process of drafting an counterterrorism bill to address terrorist financing issues.

The new money laundering legislation, if approved, will institute important national reforms. In addition to confirming the UAF's role as the sole FIU, it establishes SEPRELAD an independent secretariat or agency reporting directly to the Office of the President. The draft law also establishes money laundering as an autonomous crime punishable by a prison term of five to 20 years. It establishes predicate offenses as any crimes that are punishable by a prison term exceeding six months, and specifically criminalizes money laundering tied to the financing of terrorist groups or acts. The full range of covered institutions will be required to report suspicious transactions to the UAF and to maintain registries of large currency transactions that equal or exceed \$10,000. Under the draft legislation, those institutions have been expanded to include, inter alia, banks; financial institutions; insurance agencies; currency exchange houses; securities companies and brokers (stock exchange); investment companies; money transmitters; administrators of mutual investment and pension funds; credit unions; operators of gambling facilities; real estate agencies; nongovernmental organizations; pawnshops; and dealers in jewels, precious stones and metals, automobiles, art, and antiques. Other provisions of the draft law include penalties for failure to file or falsify reports, "know-your-client provisions," and standardized record keeping for a minimum of seven years. The UAF will continue to refer cases as appropriate for further police (SENAD) investigation and to the Attorney General's Office for prosecution. It will also serve as the central entity for related information exchanges with other concerned foreign entities. The law further specifies that the investigative unit of SENAD is the principal authority for carrying out all counternarcotics and other financial investigations, and will also have the authority to initiate investigation of cases on its own.

There are other challenges, however, that the new money laundering legislation, when passed, will not address. With only eight prosecutors dedicated to financial crimes, Paraguay currently has limited resources to investigate and prosecute money laundering and financial crimes. Moreover, prosecutors have little experience working with the UAF, and unless the new law is enacted, most judges have little incentive to investigate money laundering cases because many believe that sentencing on predicate offenses is sufficient punishment. Thus, there have not been any successful money laundering prosecutions in Paraguay so far, and improvement is unlikely until the new law becomes a reality. As it is, those individuals implicated in money laundering are prosecuted on tax evasion charges. In May 2004, Assad Barakat—widely alleged to be involved in money laundering—was convicted of tax evasion and sentenced to six and one-half years in prison. In late 2004, prosecutors were investigating several tax evasion cases involving suspected money laundering by both legal and illegal money exchange offices in Ciudad del Este.

Another serious problem for money laundering investigations that will not be corrected by the new law is the obligation of federal prosecutors to notify a suspect in writing that he/she is the subject of an investigation. Suspects must be notified within six months of the start of an investigation, and may have access to all information gathered through the investigation. This is mandated by Paraguay's penal code.

Under current laws, the GOP has limited authority to freeze, seize, and/or forfeit assets of suspected money launderers. In most cases, assets that the GOP is permitted to freeze, seize, and/or forfeit are limited to transport vehicles, such as planes and cars, and normally do not include bank accounts. However, authorities may not auction off these assets until a conviction is announced by the judicial system. At best, the GOP can establish a "preventative embargo" against assets of persons under investigation for a crime in which the state risks loss of revenue from furtherance of a criminal act, such as tax evasion. However, in those cases the limit of the embargo is set as the amount of liability of the suspect to the government. As the government entity primarily responsible for the tracing and seizing of assets, SENAD is required to split the proceeds of the forfeiture with the Public Ministry. SENAD currently has no figure for the amount of assets seized and/or forfeited in 2004, as it does not place a value on these assets before auction. Under current provisions of the law, significant legal loopholes exist, allowing criminals to hide their assets under another person's name.

The new anti-money laundering legislation will, when passed, allow prosecutors to recommend that judges freeze or confiscate assets connected to money laundering and its predicate offenses. The draft law also provides for the creation of a special asset forfeiture fund to be administered by a consortium of national governmental agencies, which will support programs for crime prevention and suppression, including combating money laundering, and related training.

The GOP currently has no authority to freeze, seize, and/or forfeit assets related to the financing of terrorism. A recent attempt to freeze the assets of a suspected terrorist financier for tax evasion failed because prosecutors perceived that the Paraguayan constitution prohibits the confiscation of personal property. The financing of terrorism is not criminalized under current Paraguayan law. However, the Ministry of Foreign Affairs often provides the Central Bank and other government entities with a list of groups or individuals included on the UNSCR 1267 Sanctions Committee consolidated list; to date, the GOP has not identified, seized, or forfeited any such assets linked to these groups or individuals. The current law also does not provide any measures for thwarting the misuse of charitable or non-profit entities that can be used as conduits for the financing of terrorism. Following the submission of the draft anti-money laundering law to Congress in May 2004, a working group of GOP and U.S. officials began drafting legislation to address terrorism and terrorist financing. The draft legislation will allow the GOP to conform to international standards on the suppression of terrorist financing. The draft anti-money laundering legislation will also specifically criminalize money laundering tied to the financing of terrorist groups or acts.

The GOP ratified the UN International Convention for the Suppression of the Financing of Terrorism in November 2004 and the Organization of American States Inter-American Convention on Terrorism in January 2005. Paraguay has also signed, but not ratified, the UN Convention against Corruption. In September 2004, the GOP ratified the UN Convention against Transnational Organized Crime. Paraguay is party to the 1988 UN Drug Convention, and participates in Summit of the Americas and Inter-American Drug Abuse Control Commission (CICAD)-related meetings on money laundering. Paraguay is a member of the South American Financial Action Task Force (GAFISUD), the Egmont Group, and the "3 Plus 1" Counter-Terrorism Dialogue between the United States and the Triborder Area countries.

While the Government of Paraguay took a number of positive steps in 2004, there are other initiatives that should be pursued in 2005 to increase the effectiveness of Paraguay's efforts to combat money laundering and terrorist financing. Most important is enactment of the new money laundering law that

meets international standards. Paraguay should also continue efforts to combat corruption, and increase information sharing among concerned agencies when and if the corruption issues are resolved. Paraguay does not have an counterterrorism law or a law criminalizing terrorist financing. While the new money laundering law would increase the Government of Paraguay's abilities to combat terrorist financing, it should also take steps as quickly as possible to ensure that comprehensive counterterrorism legislation is passed. Reforms to the criminal procedure code that would allow prosecutors to carry out long-term criminal investigations should be considered. Reforms to the customs agency are also necessary in order to allow for increased inspections and interdictions at ports of entry and to develop strategies targeting the physical movement of bulk cash. It is essential that the Unidad de Análisis Financiera continue to receive the financial and human resources necessary to operate as an effective, fully functioning Financial Intelligence Unit capable of effectively combating money laundering, terrorist financing, and other financial crimes.

Peru

Peru is not a major regional financial center, nor is it an offshore money laundering haven. Peru is a major drug producing and drug-transit country. Narcotics-related and other money laundering does occur, and the Government of Peru (GOP) has taken several steps to improve its money laundering legislation and enforcement abilities. Nevertheless, more effort is necessary to better assess the scale and methodology of money laundering in Peru. Peru is the world's second largest producer of cocaine, and, although no reliable figures exist regarding the exact size of the narcotics market in Peru, conservative estimates indicate that the cocaine trade generates between 1.5 to two billion dollars per year. As a result, money laundering occurs on a significant scale to integrate the illegal proceeds generated from the cocaine trade into the Peruvian economy.

Money laundering has historically been facilitated by a number of factors. Peru's economy is heavily dependent upon the U.S. dollar and approximately 65 percent of the economy is dollarized, allowing traffickers to handle large bulk shipments of U.S. currency with minimal complications. Currently no restrictions exist on the amount of foreign currency an individual can exchange or hold in a personal account, and until recently, there were no controls on bulk cash shipments coming into Peru.

A number of former government officials, most from the Fujimori administration, are under investigation for corruption-related crimes, including money laundering. These officials have been accused of transferring tens of millions of dollars in proceeds from illicit activities (e.g., bribes, kickbacks, or protection money) into offshore accounts in the Cayman Islands, the United States, and/or Switzerland. The Peruvian Attorney General, a Special Prosecutor, the office of the Superintendent of Banks (SBS) and the Peruvian Congress have conducted numerous investigations, some of which are ongoing, involving dozens of former GOP officials. In 2004, the 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. However, there have been no convictions for money laundering offenses to date in Peru.

On June 1, 2004, the United States Department of the Treasury's Office for Foreign Assets Control (OFAC) initiated an investigation of Fernando Zevallos Gonzales, founder and de facto owner of Peru's largest airline, Aero Continente. Because of Zevallos's suspected links to narcotics-trafficking and money laundering, all of his assets in the United States were frozen by OFAC. OFAC formally added Aero Continente, now known as Nuevo Continente, to its Specially Designated Nationals (SDN) list pursuant to the Foreign Narcotics Kingpin Designation Act.

Prior to 2002, Peru had a relatively weak anti-money laundering legislative and regulatory framework. The previous system criminalized only the laundering of proceeds directly associated with narcotics trafficking and "narcoterrorism," and mandated that all unusual or suspicious financial transactions be

reported directly to the Public Ministry. Only banks and other financial institutions were required to report suspicious transactions or large cash transactions, and the requirement to report cash transactions was suspended in August 1998, one month after it went into effect.

In 2002, the GOP strengthened its anti-money laundering regime by creating a Financial Intelligence Unit (FIU), expanding the type of institutions required to file suspicious transaction reports, increasing the number of predicate crimes, criminalizing willful blindness, and reinstating reporting requirements for large cash transactions. In April and June of that year, Laws 27.693 and 27.765 were adopted. Law 27.765 expands the predicate offenses for money laundering to include the laundering of assets related to all serious crimes, such as narcotics-trafficking, terrorism, corruption, trafficking of persons, and kidnapping.

The penalties for money laundering were also revised. Instead of a life sentence for the crime of laundering money, Law 27.765 sets prison terms of up to 15 years for convicted launderers, with a minimum sentence of 25 years for cases linked to narcotics-trafficking, terrorism, and laundering through banks or financial institutions. In addition, revisions to the Penal Code criminalize “willful blindness,” the failure to report money laundering conducted through one’s financial institution when one has knowledge of the money’s illegal source, and imposes a three to six year sentence for failure to file suspicious transaction reports.

Law 27.693 provided for the creation of Peru’s financial intelligence unit, the Unidad de Inteligencia Financiera (UIF), an autonomous body reporting to the Office of the Prime Minister. The law also expanded the entities obligated to report suspicious transactions beyond just banks and financial institutions. Stock funds or brokers, credit and debit card companies, exchange houses, mail and courier services, travel and tourism agencies, hotels and restaurants, notaries, the customs agency, casinos, auto dealers, construction or real estate firms, and other sectors, in addition to banks and financial institutions, are all required to report suspicious transactions to the UIF within 30 days.

These entities are required to maintain registries of suspicious transaction reports (STRs) sent to the UIF. Law 27.693 also reinstated reporting requirements for large cash transactions, and requires the reporting of individual cash transactions exceeding \$10,000 or transactions totaling \$50,000 in one month. Nonfinancial institutions, such as exchange houses, casinos, lotteries or others, must report individual transactions over \$2,500 or monthly transactions over \$10,000. These cash transaction reports (CTRs) must be maintained in internal databases for a minimum of five years and be made available to the UIF upon request. Major institutions are required to appoint supervisory-level compliance officials to ensure that all reporting requirements for STRs and CTRs are met.

Law 27.693 also enables the UIF to request information from the following entities: the National Superintendence for Tax Administration, Customs, the Securities and Exchange Commission, the Public Records Office, the Public or Private Risk Information Centers, and the National Identification Registry and Vital Statistics Office. However, the UIF can only share information with other agencies—including foreign entities—if there is a joint investigation underway.

In July 2004, the GOP demonstrated further efforts to strengthen its anti-money laundering and terrorist financing system with the passage of Law 28.306. Law 28.306, which entered into effect on July 30, 2004, mandated that covered entities report suspicious transactions related to terrorist financing, and expanded the UIF’s functions to include the ability to analyze reports related to terrorist financing. Terrorist financing is criminalized under Executive Order 25.475, but Law 27.693 did not require covered entities to report suspicious transactions related to the financing of terrorism, nor did it enable the UIF to analyze such reports.

Law 28.306 also increased the number of individuals and entities required to file CTRs or STRs and expanded the number of government agencies from which the UIF may request information. A new reporting requirement was added as well: individuals or entities transporting more than \$10,000 in

currency or monetary instruments into or out of Peru must file reports with the customs agency, and the UIF may have access to those reports upon request. The law also gives the UIF the power to sanction entities for failure to report suspicious transactions, large cash transactions, or the transportation of currency or monetary instruments. Under Law 28.306, the UIF now has regulatory responsibilities for all covered entities that do not fall under the supervision of another regulatory body (such as the Superintendence of Banks).

The UIF began operations in June 2003 and today has 41 personnel. Reporting requirements entered into effect in September 2003, and as of October 2004 the UIF has received approximately 190 STRs. The FIU cannot receive STRs electronically; covered entities must hand-deliver STRs to the UIF.

The UIF has requested additional information from the covered entities on roughly 30 percent of the STRs. The UIF currently does not receive cash transactions reports or reports on the international transportation of currency or monetary instruments. CTRs are maintained in internal registries within the obligated entities, and reports on the international transportation of currency or monetary instruments are maintained by the customs agency. If the UIF receives an STR and determines that the STR warrants further analysis, it contacts the covered entity that filed the report for additional background information—including any CTRs that may have been filed—and/or the customs agency to determine if the subject of the STR had reported the transportation of currency or monetary instruments.

The UIF cannot receive CTRs without specifically requesting them from the covered entities, and there is no regular CTR reporting. Some requests for reports of transactions over \$10,000—such as those that are deposits into savings accounts—are protected under the constitution by bank secrecy provisions and require an order from the Public Ministry or SUNAT, the tax authority. A period of 15-30 days is required to lift the bank secrecy restrictions. All other types of cash transaction reports, however, may be requested directly from the reporting institution.

Once the UIF has completed the analysis process and determined that a case warrants further investigation or prosecution, the case is sent to the Public Ministry. Within the counternarcotics section of the Public Ministry, two specialized prosecutors are responsible for dealing with money laundering cases. As of December 2004, 19 cases had been sent to the Public Ministry for further investigation and all have been investigated by the two prosecutors. However, only three are ready for trial, and there have been no money laundering prosecutions in Peru to date.

In addition to being able to request any additional information from the UIF in their investigations, the Public Ministry may also request the assistance of the Directorate of Counternarcotics (DINANDRO) of the Peruvian National Police. With the passage of Law 28.306 in July 2004, DINANDRO and the UIF are now able to collaborate on investigations, although each agency must go through the Public Ministry in order to do so. DINANDRO may provide the UIF with intelligence for the cases the UIF is analyzing, while it provides the Public Ministry with assistance on cases that have been sent to the Public Ministry by the UIF.

The UIF was given regulatory responsibilities in July 2004 under Law 28.306. Most covered entities fall under the supervision of the Superintendence of Banks and Insurance (banks, the insurance sector, financial institutions), the Peruvian Securities and Exchange Commission (securities, bonds), and the Ministry of Tourism (casinos). All entities that are not supervised by these three regulatory bodies, such as auto dealers, construction and real estate firms, etc., fall under the supervision of the UIF.

However, some covered entities remain unsupervised. For instance, although money remittance businesses are regulated by the Superintendence of Banks, the Superintendence is not required to supervise any money remittance business that does less than 1,240,000 soles (about \$400,000) in transfers per year. There is also difficulty in regulating casinos, as roughly 60 percent of that sector is informal. An assessment of the gaming industry conducted by GOP and U.S. officials in 2004

identified alarming deficiencies in oversight, and described an industry that is vulnerable to being used to launder large volumes of cash. Approximately 580 slot houses operate in Peru, with less than 65 percent or so paying taxes. Estimates indicate that under 42 percent of the actual income earned is being reported, while official gaming revenues totaled \$650 million in 2003. This billion-dollar cash industry continues to operate with little supervision.

Peru currently lacks comprehensive and effective asset forfeiture legislation. The Financial Investigative Office of DINANDRO has seized numerous properties over the last several years, but few were turned over to the police to support counternarcotics efforts. While Peruvian law does provide for asset forfeiture in money laundering cases, and these funds can be used in part to finance the UIF, no clear mechanism exists to distribute seized assets among government agencies. The government's "Fedadoi" fund currently holds around \$75 million in monies recovered after having been stolen or diverted during the Fujimori administration.

As one of four countries participating in the G-8 Anti-Corruption and Transparency initiative, the GOP has committed itself to create a specialized office within the Public Ministry to provide advice on locating and recovering stolen public assets. Also as part of the initiative, the UIF will pursue activities to raise public awareness of money laundering, research money laundering trends in specific sectors of the economy, further improve the legal framework addressing money laundering, and promote better GOP interagency cooperation in pursuing cases.

Terrorism is considered a problem in Peru, which is home to the terrorist organization Shining Path. Although the Shining Path has been designated by the United States as a foreign terrorist organization pursuant to Section 219 of the Immigration and Nationality Act and under Executive Order (E.O.) 13224, and the United States and 100 other countries have issued freezing orders against its assets, the GOP has no legal authority to quickly and administratively seize or freeze terrorist assets. In the event that such assets are identified, the Superintendent for Banks must petition a judge to seize or freeze them. A final judicial decision is then needed to dispose of or use such assets.

Foreign Ministry Officials are working with other GOP agencies to complete the necessary legal revisions that will permit asset-freezing actions. The Office of the Superintendent of Banks routinely circulates to all financial institutions in Peru updated lists of individuals and entities that have been included on the UNSCR 1267 Sanctions Committee's consolidated list as being linked to Usama Bin 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.

Peru also has not yet taken any actions to thwart the misuse of charitable or non-profit entities that can be used as conduits for the financing of terrorism. However, with the passage of Law 28.306, the GOP did make some improvements with regard to terrorist financing legislation in 2004. Law 28.306 mandates that covered entities report suspicious transactions related to terrorist financing, and enables the UIF to analyze those reports. The financing of terrorism is criminalized under Executive Order 25.475.

Peru ratified the UN International Convention for the Suppression of the Financing of Terrorism on November 10, 2001, and the Organization of American States Inter-American Convention on Terrorism in 2003. Peru is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime, and ratified the UN Convention against Corruption in November 2004. Peru is a member of the Organization of American States Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Peru is also a member of the South American Financial Action Task Force (GAFISUD), and was elected in July 2004 to hold the GAFISUD presidency in 2005. Peru is expected to become a member of the Egmont group of international FIUs in mid-2005. An extradition treaty between the U.S. Government and the GOP entered into force in 2003.

The Government of Peru has made serious advances in strengthening its anti-money laundering regime in 2004. However, some progress is still required. Anticorruption efforts in Peru should be a priority, and the need for strong confidentiality protocols for the Unidad de Inteligencia Financiera should be stressed. However, there are still a number of weaknesses in Peru's anti-money laundering system: bank secrecy must be lifted in order for the Unidad de Inteligencia Financiera to have access to certain cash transaction reports, smaller financial institutions are not regulated, and the Unidad de Inteligencia Financiera is not able to work directly with law enforcement agencies; rather, the Public Ministry must coordinate any collaboration between the Unidad de Inteligencia Financiera and the other agency. Peru should also enact legislation that allows for administrative as well as judicial blocking of terrorist assets. These issues should be addressed in order to strengthen Peru's ability to combat money laundering and terrorist financing.

Philippines

The Philippines is a regional financial center. In the past few years, the illegal drug trade in the Philippines reportedly has evolved into a billion-dollar industry. The Philippines continues to experience an increase in foreign organized criminal activity from China, Hong Kong, and Taiwan. Insurgency groups operating in the Philippines fund their activities, in part, through the trafficking of narcotics and arms and engage in money laundering through alleged ties to organized crime. The proceeds of corrupt activities by government officials are also a source of laundered funds.

In June 2000, the Financial Action Task Force (FATF) placed the Philippines on its list of Non-Cooperative Countries and Territories (NCCT) for lacking basic anti-money laundering regulations, including customer identification and record keeping requirements, and excessive bank secrecy provisions. Following its placement on the NCCT list, the U.S. Government issued an advisory to all U.S. financial institutions instructing them to give "enhanced scrutiny" to transactions involving the Philippines.

The Government of the Republic of the Philippines (GRP) initially established an anti-money laundering and counterterrorist financing regime by passing the Anti-Money Laundering Act of 2001 (AMLA). The GRP enacted Implementing Rules and Regulations (IRR) for the AMLA in April 2002. The AMLA criminalized money laundering, an offense defined to include the conduct of activity involving the proceeds from unlawful activity in any one of 14 major categories of crimes, and imposes penalties that include a term of imprisonment of up to 14 years and a fine no less than 3,000,000 pesos (\$54,000) but no more than twice the value or property involved in the offense. The Act also imposed identification, record keeping and reporting requirements on banks, trusts and other institutions regulated by the Central Bank, insurance companies, securities dealers, foreign exchange dealers and money remitters, as well as any other entity dealing in valuable objects or cash substitutes regulated by the Securities and Exchange Commission.

The AMLA also established the Anti-Money Laundering Council (AMLC) as the country's Financial Intelligence Unit (FIU). The Council is composed of the Governor of the Central Bank, the Commissioner of the Insurance Commission, and the Chairman of the Securities and Exchange Commission. By law, the AMLC Secretariat is an independent agency responsible for receiving, maintaining, analyzing, and evaluating covered and suspicious transactions. It provides advice and assistance to relevant authorities and issues relevant publications. The AMLC's responsibilities include the investigation and prosecution of money laundering. AMLC has the ability to seize terrorist assets involved in money laundering on behalf of the Republic of the Philippines after a money laundering offense has been proven beyond a reasonable doubt. In order to freeze assets allegedly connected to money laundering, the AMLC must establish probable cause that the funds relate to an offense enumerated in the Act, such as terrorism. The Court of Appeals then may freeze the bank account for 20 days. The AMLC may apply to extend a freeze order prior to its expiration. The AMLC

is required to obtain a court order to examine bank records for activities not listed in the Act, except for certain serious offenses such as kidnapping for ransom, drugs, and terrorism-related crimes. The AMLC and the courts are working to shorten the time needed so funds are not withdrawn before the freeze order is obtained. The AMLC has finalized, and will soon issue, implementing regulations on the forfeiture of assets related to money laundering, including provisions for third party claims.

However, the Financial Action Task Force (FATF) deemed the original legislation inadequate and pressured the Philippines to amend the legislation to be more in line with international standards. The Government of the Republic of the Philippines (GRP) subsequently made important progress in developing its anti-money laundering and terrorist financing regime, with the enactment of amendments to the Anti-Money Laundering Act of 2001 (AMLA) in March 2003. The FATF deemed those amendments to have sufficiently addressed the main legal deficiencies in the original Philippines anti-money laundering regime, and decided not to apply any formal countermeasures.

The major purposes of the amendments to the AMLA are the following: to lower the threshold amount for covered transactions (cash or other equivalent monetary instrument) from 4,000,000 pesos to 500,000 pesos (\$80,000 to \$10,000) within one banking day; to expand financial institution reporting requirements to include the reporting of suspicious transactions, regardless of amount; to authorize the Central Bank (Bangko Sentral ng Pilipinas or BSP) to examine any particular deposit or investment with any bank or non-bank institution in the course of a periodic or special examination (in accordance with the rules of examination of the BSP), to ensure institutional compliance with the Anti-Money Laundering Act; and, to delete the prohibitions against the Anti-Money Laundering Council's examining particular deposits or investments opened or created before the Act. The AMLC is now able to respond to a request from foreign authorities regarding deposits and investments made prior to the coming into effect of the AMLA.

Over the last year, the Philippines also made progress in tracking, seizing, and blocking terrorist assets. The AMLC completed the first phase of its information technology upgrades in 2004. This is a significant milestone that allowed AMLC to electronically receive, store, and search CTRs filed by regulated institutions. Through 2004, the AMLC had received well over six hundred suspicious transaction reports (STRs) involving 5,451 suspicious transactions, and had received covered transaction reports (CTRs) involving over 22 million covered transactions. In October 2004, the FATF met with the Philippines during the Asia/Pacific Review Group on Money Laundering to discuss progress addressing the remaining vulnerabilities. A FATF team conducted an on-site visit to the Philippines in January 2005 in order to determine if effective implementation of the AML reforms has taken place.

The Philippines is a member of the Asia/Pacific Group on Money Laundering. It is a party to the 1988 UN Drug Convention. The GRP has signed and ratified all 12 international conventions and protocols related to terrorism, including the UN Convention against Transnational Organized Crime (2002) and the UN International Convention for the Suppression of the Financing of Terrorism (2004). The Anti-Money Laundering Council is able to freeze funds and transactions identified with or traced to designated terrorist organizations or individuals upon request of the United Nations Security Council, the United States, and other foreign governments. The AMLC has responded to numerous requests for assistance from the U.S. and other countries. In a recent joint corruption investigation, conducted by U.S. and Philippine law enforcement, Philippine authorities expeditiously identified and froze over 40 accounts containing in excess of \$1 million total. Its follow-up investigations identified more accounts in the United States that were subsequently pursued by U.S. authorities (the Philippines and the U.S. have a Mutual Legal Assistance Treaty that entered into force in 1996). The United Kingdom recently praised the AMLC for assisting in the identification and repatriation of proceeds from money laundering. A number of money laundering related investigations are underway, most of which involve a failure to report covered transactions. In addition, a number of money laundering related cases are currently being heard a different regional trial courts throughout the Philippines.

In 2004, for the third straight year, the Philippines failed to enact new counterterrorism legislation. Lawmakers introduced several counterterrorism bills in the new Congress in July 2004; however, the executive branch has yet to develop a strategy to identify the most effective legislation or complete the draft of its version and mobilize resources to lobby for its passage. In lieu of specific counterterrorist legislation, the government has broadly criminalized terrorist financing through Republic Law legislation, which defines “hijacking and other violations under Republic Act No. 6235; destructive arson and murder, as defined under the Revised Penal Code, as amended, included those perpetrated by terrorists against non-combatant persons and similar targets” as one of the violations under the definition of unlawful acts. The Revised Implementing Rules and Regulations R.A. No. 9160, as amended by R.A. No.9194 further state that any proceeds, derived or realized from an unlawful activity includes all material and monetary effects will be deemed a violation against the law.

The Government of the Republic of the Philippines has made impressive progress enhancing and implementing its amended anti-money laundering legislation. It should continue to focus on effective implementation of the laws and procedures already enacted, in part by expanding its financial and human resources to properly equip and train law enforcement and regulatory personnel. Finally, Philippines should enact and implement new legislation that criminalizes terrorism and terrorist financing.

Poland

Poland’s geographic location places it directly along one of the main routes between the former Soviet Union republics and Western Europe used by narcotics-traffickers and organized crime groups. According to Polish government estimates, narcotics-trafficking, organized crime activity, auto theft, smuggling, extortion, counterfeiting, burglary, and other crimes generate criminal proceeds in the range of \$2-3 billion yearly. The Government of Poland (GOP) estimates the unregistered or gray economy, used primarily for tax evasion, may be as high as 15 percent of Poland’s \$230 billion GDP; it believes the black economy is only one percent of GDP. Poland’s entry into the European Union (EU) in May 2004 increased its ability to control its eastern borders, thereby allowing Poland to become more effective in its efforts to combat all types of crime, including narcotics-trafficking and organized crime.

Poland’s banks serve as transit points for the transfer of criminal proceeds. As of December 2004, 60 commercial banks were licensed for operation in Poland, as were slightly less than 600 “cooperative banks” that serve the rural and agricultural community. The GOP considers the nation’s banks, insurance companies, and brokerage houses to be important venues of money laundering. Polish casinos may likewise be sites for money laundering activity. According to the GOP, fuel smuggling, during which local companies and organized crime groups seek to avoid excise taxes by forging gasoline delivery documents, is a major source of proceeds to be laundered. It is also believed that some money laundering in Poland derives from Russia and/or other countries of the former Soviet Union.

The Criminal Code criminalizes money laundering. Article 299 of the Criminal Code addresses self-laundering and criminalizes tipping off. In June 2001, the parliament passed amendments that broadened the definition of money laundering to encompass all serious crimes (“Act on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources,” known as the “Act of 16 November”). In March 2003, Parliament further amended the law to broaden the definition of money laundering to include assets originating from illegal or undisclosed sources.

The National Security Strategy of Poland has labeled the anti-money laundering effort as a top priority. The GOP has worked diligently to bring its laws into full conformity with EU obligations. On November 16, 2000, a law went into effect that improves Poland’s ability to combat money laundering

(entitled “the November 2000 Act on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources”). The GOP has updated this law several times to bring it into conformity with EU standards and to improve its operational effectiveness. This law increases penalties for money laundering and contains safe harbor provisions that exempt financial institution employees from normal restrictions on the disclosure of confidential banking information. The law also provides for the creation of a Financial Intelligence Unit (FIU), the General Inspectorate of Financial Information (GIIF), housed within the Ministry of Finance, to collect and analyze large and suspicious transactions.

A major weakness of Poland’s initial money laundering regime was that it did not cover many non-bank financial institutions that had traditionally been used for money laundering. To remedy this situation, between 2002 and 2004, the Parliament passed several amendments to the 2000 money laundering law. The amendments expand the scope of institutions subject to identity verification, record keeping, and suspicious transaction reporting requirements. Financial institutions subject to the reporting requirements prior to March 2004 amendments included banks, the National Depository for Securities, post offices, auction houses, antique shops, brokerages, casinos, insurance companies, investment and pension funds, leasing firms, private currency exchange offices, real estate agencies, and notaries public. The March 2004 amendments to the money laundering law widen the scope of covered institutions to include lawyers, legal counselors, auditors, and charities, as well as the National Bank of Poland in its functions of selling numismatic items, purchasing gold, and exchanging damaged banknotes. It also requires casinos to report the purchase of chips worth 1,000 euros or more. The law’s extension to the legal profession was not without controversy. Lawyers strongly opposed the new amendments, claiming that the law violates client/attorney confidentiality privileges.

In 2002, Parliament adopted measures to bring the nation’s anti-money laundering legislation into compliance with EU standards regarding the reporting threshold, and also amended Poland’s customs law to require the reporting of any cross-border movement of more than 10,000 euros in currency or financial instruments. In addition to requiring that the GIIF be notified of all financial deals exceeding 15,000 euros, covered institutions are also required to file reports of suspicious transactions, regardless of the size of the transaction. Polish law also requires financial institutions to put internal anti-money laundering procedures into effect—a process that is overseen by the GIIF.

The GIIF began operations on January 1, 2001. In its first year of existence, the GIIF received over 350 suspicious transaction reports (STRs). In 2002, the GIIF received 670 STRs, from which prosecutors prepared 70 cases. In 2003, the GIIF received 965 STRs, resulting in the development of 152 cases by the Prosecutor’s Office. Between January and November 2004, the GIIF received 1,240 STRs, resulting in the creation of 136 cases. Banks filed eighty percent of the STRs submitted in 2004. At a minimum, all reports submitted by the GIIF to the Prosecutor’s Office have resulted in the instigation of initial investigative proceedings. Although there were only four convictions under the money laundering law in 2004 (this figure is twice the number from 2003), many of the investigations begun by the GIIF have resulted in convictions for other non-financial offenses. As of December 2004, the GIIF received 7.5 million reports on transactions exceeding the threshold level. The GIIF receives approximately 1.5 million reports per month.

The vast majority of required notifications to the GIIF are sent through a newly developed electronic reporting system, which is Europe’s most technically sophisticated and collects more complete information than the previously required report regarding the transaction in question (e.g., how payment was made—cash or credit, where and when). Only a small percentage of notifications are now submitted by paper, mainly from small institutions, which lack the IT capacity to use the electronic system. Although the new system is an important advance for Poland’s anti-money laundering program, the processing and analyzing of the large number of reports that are sent to the GIIF will prove to be a challenge for the understaffed FIU. To help improve the FIU’s efficiency in

handling the large volume of reports filed by obliged institutions, the GIIF plans to install new analytical software that will permit advanced and detailed analysis of financial information.

The GIIF also does on-site training and compliance monitoring investigations. In 2004, the GIIF carried out 15 compliance investigations and received several hundred follow-up reports from institutions responsible for routinely supervising covered institutions. In January 2004, the GIIF introduced a new electronic learning course designed to familiarize obliged institutions with Poland's anti-money laundering regulations.

The Polish Code of Criminal Procedure, Article 237, allows for certain Special Investigative Measures. However, money laundering investigations are not specifically covered, although the organized crime provisions might apply in some cases. Two main police units deal with the detection and prevention of money laundering: the General Investigative Bureau and the Unit for Combating Financial Crime. Overall, both police units cooperate well with the GIIF. The Internal Security Agency (ABW) may also investigate the most serious money laundering cases.

A recognized need exists for an improved level of coordination and information exchange between the GIIF and law enforcement entities, especially with regard to the suspicious transaction information that the GIIF forwards to the National Prosecutor's Office. To alleviate this problem the GIIF and the National Prosecutor's Office signed a "cooperation agreement" in 2004. The agreement calls for the creation of a computer-based system that would facilitate information exchange between the two institutions. Work on the development of this new system is currently underway.

The GIIF is authorized to put a suspicious transaction on hold for 48 hours. The Public Prosecutor then has the right to suspend the transaction for an additional three months, pending a court decision. In 2004, Article 45 of the criminal code was amended to further improve the government's ability to seize assets. On the basis of the amended article, an alleged perpetrator must prove that his assets have a legal source; otherwise, the assets are presumed to be related to the crime and as such can be seized. Both the Ministry of Justice and the GIIF desire to see more aggressive asset forfeiture regulations. However, because the former communist regime employed harsh asset forfeiture techniques against political opponents, lingering political sensitivities make it difficult to approve stringent asset seizure laws. In 2003, the GIIF suspended 20 transactions worth 9 million euros and blocked 9 accounts worth 5.2 million euros. During the first eleven months of 2004, the GIIF suspended 5 transactions worth 650,000 euros and blocked 12 accounts worth 2.1 million euros.

The GOP recently created an office of counterterrorist operations within the National Police. The office coordinates and supervises regional counterterrorism units and trains local police in counterterrorism measures. Poland has also created a terrorist "watch list" of entities suspected of involvement in terrorist financing. The list contains data based on information derived from similar lists published by the UN, the EU, and the United States Treasury Department. All covered institutions are required to verify that their customers are not included on the watch list. In the event that a covered institution discovers a possible terrorist link, the GIIF has the right to suspend suspicious transactions and accounts. Despite these efforts, Poland has not yet criminalized terrorist financing, arguing that all possible terrorist activities are already illegal and serve as predicate offenses for money laundering and terrorist financing investigations. The Ministry of Justice has completed draft amendments to the criminal code that would criminalize terrorist financing as well as elements of all terrorism-related activity. The amendments have been presented to the Minister of Justice, but have not yet been approved by Parliament.

Poland is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the European Convention on Extradition and its Protocols, the European Convention on Mutual 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 was in fact a Polish initiative.

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) and has undergone first and second round mutual evaluations by that group. The GIIF is an active participant in the Egmont Group and in FIU.NET, the EU-sponsored information exchange network for FIUs. Poland has expressed an interest in joining the Financial Action Task Force (FATF).

A Mutual Legal Assistance Treaty between the United States and Poland came into force in 1999. In addition, Poland has signed bilateral mutual legal assistance treaties with Sweden, Finland, Ukraine, Lithuania, Latvia, Estonia, Germany, Greece, and Hungary. Polish law requires the GIIF to have memoranda of understanding (MOUs) with other international competent authorities before it can participate in information exchanges. The GIIF has been diligent in executing MOUs with its counterparts in other countries, signing a total of 20 MOUs between 2002 and 2003. The GIIF-FinCEN MOU was signed in fall 2003. An additional seven memoranda on exchange of financial information with Andorra, Cyprus, Monaco, Germany, Portugal, Thailand, and Ukraine were signed in 2004. Because Poland is an EU member state, the exchange of information between the GIIF and the FIUs of other member states is regulated by the EU Council Decision of October 17, 2000. All information exchanged between the GIIF and its counterparts in other EU states takes place via FIU.NET. For the first eleven months of 2004, 40 requests regarding 124 entities were received by the GIIF from foreign authorities. During the same time period, the GIIF made 104 requests regarding 227 entities to foreign authorities.

Over the past several years, the Government of Poland has worked diligently to implement a comprehensive anti-money laundering regime that meets international standards. Further improvements could be made by promoting additional training at the private sector level and by working to improve communication and coordination between the General Inspectorate of Financial Information and relevant law enforcement agencies. The Code of Criminal Procedure should also be amended to allow the use of Special Investigative Measures in money laundering investigations. This would help to attain a better record of prosecutions and convictions. Poland should also pass specific counterterrorist financing legislation.

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 currency exchanges, wire transfers, and real estate purchases are used for laundering criminal proceeds.

Portugal has a comprehensive anti-money laundering regime that criminalizes money laundering and other serious offenses, including terrorism, arms trafficking, kidnapping, and corruption. Act 5/2002 describes specific measures for combating organized and economic crime, particularly with regard to the gathering of evidence in relation to several crimes. All cross-border movements of currency that exceed 12,500 euros 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 12,500 euros. Non-bank 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.

In February 2002, the law governing money laundering (Act 10/2002) was brought into force. This law expands money laundering to include as predicate crimes arms trafficking, extortion, prostitution,

trafficking in nuclear materials, trafficking in persons, trafficking in human organs or tissues, child pornography, trafficking in listed species, and tax fraud. Act 10/2002 also extends the list of entities obliged to report large transactions, to include account officers, external auditors, tax consultants, lawyers, solicitors, notaries, registrars, and money carriers. It also includes any other independent 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; transfer and buy rights with regard to professional sportsmen and women; and the execution of any financial operation. In addition, the obligated entities have the duty to report any suspicious operation, independent of the transaction amount.

In November 2003, the GOP passed a law revising and tightening the legal framework for foreign currency exchange transactions, including gold, subjecting them to the reporting requirement for transactions exceeding 12,500 euros. Beyond the requirements to report large transactions, foreign exchange bureaus are not subject to any special requirements to report suspicious transactions. The law does, however, give the GOP the authority to investigate suspicious transactions without notifying targets of the investigation.

On March 27, 2004, Portugal implemented the European Union's (EU) Second Money Laundering Directive through a new law, Act No. 11/2004 Establishing the Regime for Prevention and Repression of the Laundering of Benefits of Illicit Origin. The new law expands police access to information about bank accounts and financial transactions of individuals or companies under investigation. These rules also apply to bank branches outside of Portugal. Under the new rules, which supersede previous legislation, if a bank suspects or knows about a suspicious or illegal transaction, or has concerns about the amount, means, or payment used in the transaction, or any other suspicious fact, the bank must inform the Attorney General's Office. The Attorney General may order the bank not to complete the transaction. If stopping the transaction is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, the Attorney General also may allow the bank to proceed with the transaction but require it to provide complete details to the government. Another provision requires banks to provide full access to investigators with a judicial warrant. Until March 2004, banking secrecy laws made it extremely difficult for investigators to obtain information about bank accounts and financial transactions of individuals or companies without their permission.

In addition, new rules, which take effect January 2005, permit tax authorities to lift secrecy rules without authorization from the target of an investigation. The rules require companies to have at least one bank account and, for companies with more than 20 employees, to conduct their business through bank transfers, checks, and direct debits rather than cash. These rules are mainly designed to help the GOP investigate possible cases of tax evasion but may ease enforcement of other financial crimes as well.

Portugal has established regulatory agencies, including the Central Bank of Portugal, the Portuguese Insurance Institution, the Gambling Inspectorate General, the Economic Activities Inspectorate General, the Securities Market Commission, the Registries and Notaries General Directorate, the National Association for Certified Public Accountants and the Association for Assistant Accountants, the Bar Association, and the Chamber of Solicitors, to monitor and enforce the reporting requirements of the obliged entities.

Suspicious transaction reports (STRs) are forwarded for analysis to the Unidade de Informação Financeira (UIF), formerly the Central Unit for Money Laundering Investigation, which began operating as the Financial Intelligence Unit (FIU) for Portugal in June 2003. If money laundering is indicated, the Portuguese Judicial Police will conduct an investigation. The UIF received 251 STRs in 2001, 256 STRs in 2002, and 488 STRs in 2003 from banks and other financial entities.

The Portuguese Madeira Islands International Business Center (MIBC) has a free trade zone, an international shipping register, offshore banking, trusts, holding companies, stock corporations, and private limited companies. The latter two business groups, of which there are approximately 6,500 companies registered in Madeira, are similar to international business corporations. 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 nonresidents or other Madeiran offshore entities, and "international branches" that conduct both offshore and domestic business. Although Madeira has some local autonomy, Portuguese and EU legislative rules regulate its offshore sector, and the competent oversight authorities supervise it. Exchange of information agreements contained in double taxation treaties allow for the disclosure of information relating to narcotics or weapons trafficking. Bearer shares are not permitted.

Portuguese laws provide for the confiscation of property and assets connected to money laundering, and authorize the Judicial Police to trace illicitly obtained assets (including those passing through casinos and lotteries), even if the predicate crime is committed outside of Portugal. Police may request files of individuals under investigation and, with a court order, can obtain and use audio and videotape as evidence in court. The law allows the Public Prosecutor to request that a lien be placed on the assets of individuals being prosecuted, in order to facilitate asset seizures related to narcotics- and weapons-trafficking, terrorism, and money laundering. Act 10/2002 shifted the burden of proof in cases of criminal asset forfeiture from the government to the defendant; an individual must prove that his assets were not obtained as a result of his illegal activities. The law defines criminal assets as those owned by an individual at the time of indictment and thereafter. The law also presumes that assets transferred by an individual to a third party within the previous five years still belong to the individual in question, unless proven otherwise. GOP law enforcement agencies seized a total of 2.4 million euros in cash and accounts in 2003 and 5.1 million euros in 2004 in association with drug and money laundering investigations. Portugal has comprehensive legal procedures that enable it to cooperate with foreign jurisdictions and share seized assets.

In August 2003, Portugal passed Act 52/2003, which specifically defines money laundering and criminalizes the transfer of funds related to the commission of terrorist acts. Portugal has created a Terrorist Financing Task Force that includes the Ministries of Finance and Justice, the Judicial Police, the Security and Intelligence Service, the Bank of Portugal, and the Portuguese Insurance Institution. Portugal has applied all of the Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing. Names of individuals and entities included on the UNSCR 1267 Committee's consolidated list, or that the United States and EU have linked to terrorism, are passed to private sector organizations through the Bank of Portugal, the Stock Exchange Commission, and the Portuguese Insurance Institution. In practice, the actual seizure of assets would only occur once the EU's clearinghouse process agrees to the EU-wide seizure of assets of terrorists and terrorist-linked groups. Portugal is actively cooperating in the search and identification of assets used for terrorist financing. To date, no significant assets have been identified or seized.

Portugal is a member of the Council of Europe, the European Union, and the FATF. Portugal is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Portugal is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, and became a party to the UN International Convention for

the Suppression of the Financing of Terrorism on October 18, 2002. The Money Laundering Investigation Unit of Portugal's Judicial Police is a member of the Egmont Group.

The Government of Portugal has put into place a comprehensive and effective regime to combat money laundering. Laws passed in 2002 strengthen its ability to investigate and prosecute, and the steps taken in 2003 extend the regime's reach to terrorist financing. Portugal 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 15 licensed financial banks, including two Islamic banks and a Qatar Industrial Development Bank. Qatar has 19 exchange houses, three investment companies and one commercial finance company. 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 by Qatari law.

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 15 years. The law also gives the QCB greater powers to inspect suspicious bank accounts, and grants the authorities the right to confiscate money in illegal transactions. Article 17 permits Qatar to extradite convicted criminals in accordance with international or bilateral treaties.

The Anti-Money Laundering Law established the National Anti-Money Laundering Committee (NAMLC) to oversee and coordinate money laundering combating efforts. It is chaired by the Deputy Governor of the Qatar Central Bank, in addition to ten other members from the Ministries of Interior, Civil Service Affairs and Housing, Economy and Commerce, Finance, Justice, QCB, Customs and Ports Authority and the State Security Bureau.

In February 2004, passed the Combating Terrorism Law. According to Article Four of the new law, any individual or entity that provides financial or logistical support, as well as raises money for activities considered terrorist crimes according to this statute are to be punished. The punishments are listed in Article Two of the law, which include the death penalty, life imprisonment, and 10 or 15 year jail sentences depending on the crime.

On October 17, 2004 the Government of Qatar appointed a member of the ruling Al-Thani family as director of the Financial Intelligence Unit (FIU). The FIU is responsible for reviewing all financial transaction reports, identifying suspicious transactions and financial activities of concern, ensuring that all government ministries and agencies have procedures and standards to ensure proper oversight of financial transactions, and recommending actions to be taken by the NAMLC if suspicious transactions or financial activities of concern are identified. Qatar's FIU has been active during the new director's appointment. The FIU is coordinating closely with the Doha Securities Market (DSM) to establish procedures and standards to monitor all financial activities that occur in Qatar's stock

market. In November 2004, the FIU established monitoring standards in coordination with the National Post Office to ensure that post offices throughout the country monitor carefully all cash transfers. The FIU is also taking steps to monitor financial activities that take place in the Ministry of Justice's Registration Department and Qatar's camel market.

In addition to reporting suspicious transactions, all financial institutions (including businesses conducting hawala transactions) must report transactions Qatari Riyals (QR) 100,000 (approximately \$33,000) or above to the QCB. Any repeated cash transactions of QR 30,000 (approximately \$10,000) or higher made by an individual or entity must be reported. Any transaction of QR 100,000 or higher and repeated transactions of QR 30,000 or higher will be investigated by the FIU in coordination with the Ministries of Justice and Interior. Exchange houses must report any transaction of QR 40,000 or higher. All financial institutions also must identify the person entering into a business relationship or conducting a transaction. In December 2004, QCB installed a central reporting system to assist the FIU in monitoring all financial transactions made by banks.

All accounts must be opened in person. (Only Qatari citizens, legal 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 has taken steps to combat the financing of terrorism, including requiring banks to freeze the assets of the individuals and entities listed on the UN 1267 Sanctions Committee's consolidated list. In 2002, the GOQ established a national committee, to review the consolidated designation lists and to recommend any necessary actions against individuals or entities found in Qatar. On August 24, 2003, the Anti-Money Laundering law was amended (amendment 21/2003) and published in the official gazette. Amendment 21 revised three articles in the anti-money laundering law. Article 2 was amended to broaden the definition for money laundering to include any activities related to terrorist financing. Article 8 added the customs and ports authority to the NAMLC. Article 12 authorized the Central Bank governor to freeze suspicious accounts up to ten days and to inform the attorney general within three days of any action taken. The Attorney General may renew or nullify the freeze order for a period of up to three months. After this process, a freeze order may not be renewed unless authorized by court order.

In March 2004, The Government of Qatar passed a law to establish the Qatar Authority for Charitable Works, which monitors all charitable activity in and outside of Qatar. This law incorporates the Charitable Societies Law (Law No. 8/1998), which outlines the monitoring and supervision of Qatar's charities. The Secretary General of the Authority will approve all international fund transfers by the charities. The Authority will have primary responsibility for monitoring overseas charitable, development, and humanitarian projects that were previously under the oversight of several government agencies such as the Ministry of Foreign Affairs, the Ministry of Finance and the Ministry of Economy and Commerce. Overseas activities must be undertaken in collaboration with a non-governmental organization (NGO) that is legally registered in the receiving country. The Authority will prepare an annual report on the status of all projects and submit the report to relevant ministries. The Authority is in the process of developing concrete measures to exert more control over domestic charity collection.

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 FIU receives all suspicious transaction reports and conducts an initial analysis. The FIU also 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 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. The Government of Qatar has established a subcommittee under the NAMLC to implement cross-border reporting requirements. The subcommittee is composed of the QCB, Customs Authority, FIU, and members of the NAMLC. In 2003, the Government of Qatar (GOQ) concluded the investigation of a seizure that occurred in November 2002, involving approximately \$400,000 worth of gold that had been smuggled into the country. The GOQ confiscated all the gold.

Qatar is a party to the 1988 UN Drug Convention but not the UN Convention for the Suppression of the Financing of Terrorism or the UN Convention against Transnational Organized Crime. Qatar is one of the original signatories of the memorandum of understanding governing the establishment of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body that promotes best practices to combat money laundering and terrorist financing in the region. MENAFATF was inaugurated on November 30 in Bahrain by 14 Arab countries. Qatar also participates in the activities of the FATF through its membership in the Gulf Cooperation Council (GCC).

The passage of the Combating Terrorism Law and the establishment of a Financial Intelligence Unit (FIU) demonstrate the Government of Qatar's commitment to fight terrorist financing. Implementation and enforcement of the new law and regulations are essential to the success of Qatar's efforts. Qatar has demonstrated a willingness to work with other countries in the fight against terrorist financing and other financial crimes. Qatar should continue to work to ensure that law enforcement, prosecutors, and customs authorities receive the necessary training and technical assistance to improve their capabilities in recognizing and pursuing various forms of terrorist financing, money laundering and other financial crimes. Qatar should become a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

Romania

Romania's geographic location makes it a natural transit country for trafficking in narcotics, arms, stolen vehicles, and persons. As such, the nation is vulnerable to financial crimes. Romania's National Bank estimates the dollar amount of financial crimes to range from \$1 billion to \$1.5 billion per year. Tax evasion and value-added tax (VAT) fraud constitute approximately 45 percent (\$500-\$600 million per year) of this total. Financial sector fraud, fraudulent bankruptcy claims, and smuggling of illicit goods are additional types of financial crimes prevalent in Romania. Romania also has one of the highest occurrences of online credit card fraud in the world.

Laundered money comes primarily from domestic criminal activity carried out by international crime syndicates, which often launder money through limited liability companies set up for this purpose. The

U.S. dollar is the preferred currency. Endemic corruption in Romania and its neighboring countries abets money laundering. The proceeds from the smuggling of cigarettes, alcohol, coffee, and other dutiable commodities are also laundered in Romania. From Romania, most of the laundered funds go to offshore financial shelters in locations such as the U.S. Virgin Islands, Cayman Islands, and Cyprus.

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 requires customer identification, record keeping, reporting transactions of a suspicious or unusual nature, and currency transaction reporting for transactions over 10,000 euros.

The law also establishes a Financial Intelligence Unit (FIU), known as the National Office for the Prevention and Control of Money Laundering (NOPCML), and mandates that the NOPCML oversee the implementation of internal anti-money laundering procedures and training for all domestic financial institutions covered by the law. The list of entities subject to money laundering controls includes banks, non-bank financial institutions, attorneys, accountants, and notaries. However, in practice, the controls on non-bank financial institutions have not been as rigorous as those imposed on banks.

In December 2002, the Law on the Prevention and Sanctioning of Money Laundering went into effect, changing the list of predicate offenses to the “all-crimes” approach. Every cash operation and every external wire transfer involving a sum exceeding 10,000 euros must be reported to the NOPCML and be monitored. NOPCML is authorized to participate in inspections and controls in conjunction with supervisory authorities.

In addition, the new law expands the number and types of entities required to report to the NOPCML. Some of these new entities include art dealers, travel agents, privatization agents, postal officials, money transferors, and real estate agents. Training for these entities is necessary to ensure compliance with reporting, record keeping, recognition of suspicious transactions, and development of internal controls. The new law also provides for both suspicious transaction reports (STRs) and currency transaction reports (CTR) to be forwarded to the NOPCML, with the CTR amounts conforming to European Union (EU) standards.

In keeping with new international standards, The National Bank of Romania (BNR) introduced Norm No. 3, “Know Your Customer,” in December 2003 to strengthen information disclosure for external wire transfers and correspondent banking. When sending out wire transfers, banks must include information about the originator’s name, address, and account. The same information is required for incoming wires as well. Banks are further required to undertake proper due diligence before entering into international correspondent relations, and are prohibited from opening correspondent accounts with shell banks. The BNR is currently working on a project to strengthen its anti-money laundering (AML) and counterterrorist financing (CTF) regulations through the introduction of improved bank examination procedures. Plans are also underway to replicate the project in the insurance industry.

The know your customer identification requirements have also been honed, so that identification of the client becomes necessary upon account opening and when single or multiple transactions meet or approach 10,000 euros. In accordance with a new national strategy on money laundering, lawyers are now obligated to report to the NOPCML. In addition, and in line with the Second EU Directive, tipping off has been prohibited. Romanian law permits the disclosure of client and ownership information to bank supervisors and law enforcement authorities, and protects banking officials with respect to their cooperation with law enforcement.

In June 2004, the Government of Romania (GOR) appointed a new director to head the NOPCML. As a result of this new appointment, there has been a concerted effort to increase the NOPCML’s operational efficiency and to bring greater visibility to the importance of AML and CTF efforts in Romania. To date, some of the most significant improvements made include the approval of a new

organizational structure for the FIU (as mandated by Governmental Decision No. 1078/2004), as well as the passage of legislation that is designed to improve the procedures for analyzing STR information and the suspension of suspicious accounts and transactions.

Thus far, it appears that these efforts have achieved a degree of success. In the four months following the appointment of the new FIU director, 10 transactions amounting to approximately \$1.5 million were suspended (during the last five years, only five transactions had been suspended). Also, from January 1, 2004 to October 2004, 400 cases have been forwarded to the General Prosecutor's Office, 201 of which were forwarded after June 2004. Despite these improvements, the NOPCML is still hampered by a lack of sufficient resources (outdated IT systems) and personnel who are in need of comprehensive training regarding AML/CTF issues, as well as training in advanced analytical research methodologies. The Law on the Prevention and Sanctioning of Money Laundering increased the powers of NOPCML, but it did not provide for an increase in administrative capacity. NOPCML has begun a process of international cooperation to exchange information with other FIUs, and has also been working closely with Italy to improve its efficiency and effectiveness through an EU PHARE Project.

In 2003, the number of STRs increased to 882, and during the first three quarters of 2004, 1,241 reports were filed. Out of the 1,241 STRs received by the NOPCML, 1,134 were filed by reporting entities and 107 by the supervisory institutions. The law also provides for feedback to be given, upon request, to NOPCML from the General Prosecutor's Office.

However, efforts to prosecute these cases have been hampered by delays in reporting suspicious transactions, by a lack of resources in some regions, and by insufficient training in conducting complex historical financial investigations. The Directorate of Economic and Financial Crimes of the national police also has a mandate to pursue money laundering. However, despite hundreds of money laundering cases investigated since 2001, the interface with the justice system remains deficient.

Romanian law has some, but limited, provisions for asset forfeiture in the Law on Combating Corruption, No. 78/2000, and the Law on Combating Tax Evasion, No. 87/1994.

On November 24, 2004, the GOR approved a draft amendment to the anti-money laundering law, which is expected to be passed in 2005. The new law provides for a uniform approach to combating and preventing money laundering and terrorist financing. The purpose of the law is to achieve the standard contained in EU Directive 2001/97/EC. The draft law provides that money laundering and terrorist financing will be regulated under the same law to ensure consistent and effective measures against these crimes. The draft recommends the expansion of the types of individuals and institutions which are subject to reporting requirements. These obligations include not only reports on specific suspicious transactions, but also generalized intelligence involving financial patterns and typologies. The new law will also provide for better seizure proceedings, the employment of undercover investigators, and the surveillance of financial accounts and communications.

The GOR announced a national anticorruption plan in early 2003 and passed a law against organized crime in April 2003. A new Criminal Procedure Code was passed and became effective on July 1, 2003. The new Code contains provisions for authorizing wiretapping, intercepting, and recording telephone calls for up to 30 days, in certain circumstances. These circumstances, as provided for within the new Code, include terrorist acts and money laundering.

Romania's political leadership has consistently and unequivocally condemned acts of terrorism. 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 the taking of measures, or the production or acquisition of means or instruments with an intention to commit terrorist acts, are offenses of exactly the same level as terrorist acts themselves. These offenses are punishable with imprisonment ranging from five to 20 years.

In April 2002, the GOR's Supreme Defense Council of the Country (CSAT) adopted a National Security Strategy, which includes a General Protocol on the Organization and Functioning of the National System on Preventing and Combating of Terrorist Acts. This system, effective July 2002 and coordinated through the Intelligence Service, brings together and coordinates a multitude of agencies, including 14 ministries, the General Prosecutor Office, the National Bank, and the NOPCML. The GOR has also set up an inter-ministerial committee to investigate the potential use of the Romanian financial system by terrorist organizations.

The Romanian Government and the BNR in particular have been fully cooperative in seeking to identify and freeze terrorist assets. Emergency Ordinance 159, also passed in 2001, includes provisions for preventing the use of the financial and banking system to finance terrorist attacks, and sets forth the parameters for the government to combat such use. The BNR, which oversees all banking operations in the country, also issued Norm No. 5 in support of Emergency Ordinance 159. Emergency Ordinance 153 was passed to strengthen the government's ability to carry out the obligations under UNSCR 1373, including the identification, freezing, and seizure of terrorist funds or assets.

In November 2004, the Parliament adopted law 535/2004 on preventing and combating terrorism, which abrogates some of the previous government ordinances and takes over most of their provisions. The law includes a chapter on combating the financing of terrorism by prohibiting financial and banking transactions with persons included on international terrorist lists, and requiring authorization for transactions conducted with entities suspected of terrorist activities in Romania.

The BNR receives lists of individuals and terrorist organizations from the United States, the UNSCR 1267 Sanctions Committee, and the EU, and circulates these to banks and financial institutions. The new law on terrorism provides that the assets used or provided to terrorist entities will be forfeited, together with finances resulting from terrorist activity. To date, in regard to terrorist financing, no arrests, seizures, or prosecutions have been carried out.

The EU's Europe Agreement with Romania provides for cooperation in the fight against drug abuse and 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). A mutual evaluation in April 1999 by that Committee 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 has been working to address these concerns, bringing in legal experts from the EU to consult. In late 2003, Romania also underwent a Financial Sector Assessment Program (FSAP) by the World Bank as part of that organization's pilot program.

The GOR recognizes the link between organized crime and terrorism. Bucharest is the site of the Southeast European Cooperative Initiative's Center for Combating Transborder Crime, a regional center that focuses on intelligence sharing related to criminal activities, including terrorism. Romania also participates in a number of regional initiatives to combat terrorism. Romania has worked within SEEGROUP (a working body of the NATO initiative for Southeast Europe) to coordinate counterterrorist measures undertaken by the states of Southeastern Europe. The Romanian and Bulgarian interior ministers signed an inter-governmental agreement in July 2002 to cooperate in the fight against organized crime, drug smuggling, and terrorism.

The 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. The GOR has demonstrated its commitment to international anticrime initiatives by participating in regional and global anticrime efforts. Romania is a party to the 1988 UN Drug Convention, the Agreement on Cooperation to Prevent and Combat Transborder Crime, and the UN Convention against Transnational

Organized Crime. Romania also is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the Council of Europe's Criminal Law Convention on Corruption; and the UN International Convention for the Suppression of the Financing of Terrorism. On November 2, 2004, Romania became a party to the UN Convention against Corruption.

Although legislation and regulations designed to combat financial crime are fairly new developments, they are quite comprehensive in scope. Nevertheless, implementation lags, while reporting and investigations are not as timely or as effective as desired. The Government of Romania should continue addressing the concerns of the Council of Europe evaluators by making further improvements in its anti-money laundering regime. Romania should ensure non-bank entities are fully aware of their reporting and record keeping responsibilities and are adequately supervised. Romania should adopt procedures for the timely freezing, seizure, and forfeiture of criminal- or terrorist-related assets. Romania should adopt reporting requirements for the cross-border movement of currency and monetary instruments.

Russia

Russia has enjoyed rapid economic growth in recent years, mainly driven by high world oil prices and the pursuit of sound fiscal policies. Yet, Russia has been slow to complete structural reforms of the banking sector, and overall public confidence in Russian banks remains low. Consequently, Russia's financial system is unattractive to both legal and illegal depositors, and therefore Russia is not considered an important regional financial center. Over the past three years, however, Russia has committed significant resources to improve its ability to combat the laundering of criminal financial proceeds domestically and internationally. Through aggressive enactment and implementation of comprehensive money laundering and counterterrorism financing legislation, Russia now has well-established legal and enforcement frameworks to deal with money laundering and terrorism financing.

Despite notable progress and demonstrated political will to combat these phenomena aggressively, Russia remains vulnerable to criminal financial activity because of a number of contributing factors, namely: vast natural resource wealth, pervasiveness of organized crime, and a high level of corruption. Other factors include porous borders, Russia's role as a geographic gateway to Europe and Asia, a weak banking system, and under-funding of regulatory and law enforcement agencies. Criminal elements from Russia and neighboring countries continue to use Russia's financial system to launder money, because of familiarity with the language, culture, and economic system. The majority of the funds do not appear to be from activities related to narcotics production or trafficking, although these activities likely occur. Experts believe that most of the dirty money flowing through Russia derives from domestic criminal or quasi-criminal activity, including evasion of tax and customs duties and smuggling operations.

Net flows of money out of the country have slowed noticeably since the 1998 financial crisis. Although net capital outflows for the first three quarters of 2004 totaled \$10.9 billion, compared with \$3.8 billion in 2003, the long-term trend in outflows continues to drift downward. This year's anomalous increase was largely attributed to instability in the banking sector and uncertainties in the investment climate. The majority of these outflows involve legitimate movement of money to more secure and profitable destinations abroad, but at least a portion of this money undoubtedly involves the proceeds of criminal activity.

Russia has the legislative and regulatory framework in place to pursue and prosecute financial crimes, including money laundering and terrorism finance. The Russian Federation's (RF's) Federal Law No. 115-FZ "On Combating Legalization (Laundering) of Criminally Gained Income and Financing of Terrorism" became effective on February 1, 2002, with subsequent amendments to the laws on banking, the securities markets, and the criminal code taking effect in October 2002, January 2003,

and December 2003. RF 115-FZ obligates banking and non-banking financial institutions to monitor and report certain types of transactions, keep records, and identify their customers. Article 8 of Law 115-FZ provides for the establishment of Russia's financial intelligence unit as an independent executive agency administratively subordinated to the Ministry of Finance. In March 2004, President Putin issued a decree to upgrade the unit, formerly called the Financial Monitoring Committee, to a service, now called the Federal Service for Financial Monitoring (FSFM). All financial institutions with an obligation to report certain transactions must send this information to the FSFM. The FSFM is also responsible for coordinating all of Russia's anti-money laundering and counterterrorism financing efforts, but has no law enforcement investigative powers.

Consistent with Financial Action Task Force (FATF) recommendations, the criminal code was amended in December 2003 to remove a specific monetary threshold for crimes connected with money laundering, thus paving the way for prosecution of criminal offenses regardless of the sum involved.

According to the original language of RF 115-FZ, those institutions legally required to report included: banks, credit organizations, securities market professionals, insurance and leasing companies, federal postal service, jewelry and precious metals merchants, betting shops, and companies managing investment and non-state pension funds. Amendments to the law that came into force on August 31, 2004, extend the reporting duty to real estate agents, lawyers and notaries, and persons rendering legal/accountancy services that involve certain transactions (e.g., preparing/executing transactions with immovables; managing money, securities, or other property; managing bank accounts or securities accounts; attracting or managing money for organizations; or incorporating, managing, and buying/selling organizations).

Various regulatory bodies ensure compliance with Russia's anti-money laundering and counterterrorism finance laws. The FSFM is specifically responsible for regulating leasing companies, pawnshops, and gambling services. The CBR supervises credit institutions; the Ministry of Finance oversees insurance companies, entities managing non-government pension and investment funds, and entities buying and selling precious metals or stones; the Federal Service for Financial Markets supervises professional participants in the securities sector.

The CBR has issued guidelines regarding anti-money laundering practices within credit institutions, including "know your customer" (KYC) and bank due diligence programs. Banks are required to obtain and retain for five years information regarding individuals and legal entities and beneficial owners of corporate entities. Further, banks must adopt internal compliance rules and procedures and appoint compliance officers. In July 2004, Russia amended Law 115-FZ to require banks to identify the original source of funds and to report to the FSFM all suspicious transactions, as opposed to only transactions containing certain features, as previously mandated. Institutions that fail to meet mandatory reporting requirements face revocation of their licenses to carry out relevant activity, limits on certain banking operations, and possible criminal or administrative penalties. An administrative fine of up to \$16,700 can be levied against an institution, with a fine of up to \$700 on an officer of an institution. The maximum criminal penalty is 10 years in prison with applicable fines.

The CBR instituted a number of regulatory measures in 1999 to scrutinize offshore financial transactions. In the six months following the implementation of these regulations, wire transfers from Russian banks to offshore financial centers dropped significantly. At the same time the CBR curtailed establishing correspondent relations with offshore banks by raising the standards for "eligible" offshore financial institutions, thereby reducing their number. In August 2003 the CBR issued Order 1317-U, which regulates the relations of Russian financial institutions with their counterparts in offshore zones. In addition to requiring Russian financial institutions to report all related transactions, offshore banks are in some cases subject to enhanced due diligence and maintenance of additional mandatory reserves to offset potential risks undertaken by the Russian institution for specific transactions.

Foreign financial entities, including those from known offshore havens, are not permitted to operate directly in Russia: they must do so solely through subsidiaries incorporated in Russia, which are subject to domestic supervisory authorities. During the process of incorporating and licensing these subsidiaries, Russian authorities must identify and investigate each director of the Russian unit; therefore nominee or anonymous directors are, as a practical matter, not permitted under Russian law and regulation. As the CBR completes its review of banks' applications for admission into the newly created Deposit Insurance System, the CBR will verify that banks are carrying out these identification procedures before approving the application.

Russian businesses must obtain government permission before opening operations abroad, including in offshore zones. A department within the Ministry of Economic Development and Trade (MEDT) reviews such requests from Russian firms, and once MEDT approves, the CBR must then approve the overseas currency transfer. In either case, the regulatory body responsible for the offshore activity is the same as for domestic activity, i.e., the Federal Service for Financial Markets regulates brokerage and securities firms, while the CBR regulates banking activity.

All obligated financial institutions must monitor and report to the government: 1) any transaction that equals or exceeds 600,000 rubles (approximately \$20,000) and involves or relates to: cash payments, individuals or legal entities domiciled in states that do not participate in the international fight against money laundering, bank deposits, precious stones and metals, payments under life insurance policies, and/or gambling; 2) all transactions of extremist organizations or individuals included on Russia's domestic list; and 3) suspicious transactions.

Each of the FSFM's seven territorial offices corresponds with one of the federal districts that comprise the Russian Federation. The Central Federal District office is headquartered in Moscow; the remaining six are located in the major financial/industrial regions throughout Russia. The primary functions of the territorial offices are to establish cooperation with regional law enforcement and other authorities to enhance information that comes into the FSFM, and to supervise anti-money laundering and counterterrorism financing legislation compliance by institutions under FSFM supervision. Additionally, the satellite offices must identify and register at the regional level all of the pawnshops, leasing, and gaming entities under their jurisdiction. They also are charged with coordinating efforts between the Central Bank of Russia (CBR) and other supervisory agencies with respect to implementation of anti-money laundering and counterterrorist financing regimes.

Russia's anti-money laundering law, as amended, provides the FSFM with the appropriate authority to gather information regarding the activities of investment foundations, non-state pension funds, gambling businesses, real estate agents, lawyers and notaries, persons rendering legal/accountancy services, and sales of precious metals and jewelry. Virtually all financial institutions submit reports to the FSFM via encrypted software provided by the FSFM. To date, Russia's national database contains approximately three million reports. The FSFM receives six to seven thousand transaction reports daily. Of these daily reports, approximately 75 percent result from mandatory (currency) transaction reports, and the remaining 25 percent relate to suspicious transactions. Among these, 130 to 150 typically merit further investigation, with 20 to 30 of these cases potentially involving terrorism financing. The FSFM has received approximately 400 reports potentially related to terrorism financing since its inception. Depending on the nature of the activity, the FSFM provides information to the appropriate law enforcement authorities for further investigation, i.e., the Ministry of Internal Affairs (MVD) for criminal matters, the Federal Drug Control Service (FSKN) for narcotics-related activity, or the Federal State Security Service (FSB) for terrorism-related cases.

As part of President Putin's recent administrative reforms, the FSKN now has a full division committed to money laundering, staffed by agents with experience in counternarcotics and economic crimes. This division cooperates closely with the FSFM in pursuing narcotics-related money laundering cases. Over the past year, the FSKN has initiated over 50 such investigations.

With its legislative and enforcement mechanisms in place, Russia has begun to prosecute a number of high-level money laundering cases. As of mid-December 2004, the CBR had revoked the licenses of 28 banks for failure to observe banking regulations. Of these 28, two banks were specifically charged with money laundering—Sodbiznesbank and Novocherkassk City Bank. When the CBR announced on May 13, 2004, that it was revoking the license of Sodbiznesbank because of money laundering charges—the first public announcement of such allegations—it touched off a minor crisis of confidence in the banking system and triggered a depositor run. In October 2004 a series of unconfirmed press articles reported that a Moscow bank was under investigation for financing terrorist acts, including the seizure of the Moscow Theater in 2002. Based on these examples and statistics, Russia has demonstrated a broad-based commitment to enforcing its anti-money laundering and counterterrorism financing legislation and is beginning to see an improvement in compliance levels as a result of its actions.

Russia has a legislative and financial monitoring scheme that facilitates the tracking and seizure of all criminal proceeds. None of this legislation, however, is specifically tied to narcotics proceeds. Russia's laws criminalizing money laundering and terrorist financing also provide for the forfeiture of criminal proceeds. Russian legislation provides for a variety of investigative techniques such as search, seizure, and compelling the production of documents, as well as the identification, freezing, seizing, and confiscation of funds/assets. Where sufficient grounds exist to suppose that property was obtained as the result of a crime, investigators and prosecutors can apply to the court to have the property frozen or seized. Law enforcement agencies have the power to identify and trace property that is, or may become, subject to confiscation or is suspected of being the proceeds of crime or terrorist financing. Moreover, the law allows the FSFM, in concert with banks, to freeze possible terrorist-related financial transactions up to one week. Banks may freeze transactions for two days and the FSFM may follow up with an additional five days.

In accordance with its international agreements, Russia recognizes rulings of foreign courts relating to the confiscation of proceeds from crime within its territory and can fully or partially transfer confiscated proceeds of crime to the foreign state whose court issued the confiscation order. However, Russian law still does not provide for the seizure of instruments of crime. Businesses can be seized only if it can be shown that they were acquired with criminal proceeds. Legitimate businesses cannot be seized solely on the basis that they were used as "instruments" to facilitate the commission of a crime. While Russian law enforcement has adequate police powers to trace and seize assets, most Russian law enforcement personnel lack experience and expertise in these areas.

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 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. Further, Article 205.1 of the criminal code, which was enacted in October 2002, criminalizes terrorist financing. On October 31, 2002, the Federation Council, Russia's upper house, approved a supplemental article to the 2003 federal budget, allocating from surplus government revenues an additional 3 billion rubles (\$100 million) in support of federal counterterrorism programs and improvement of national security.

In February 2003, at the request of the General Procuracy, the Russian Supreme Court issued an official list of 15 terrorist organizations. According to press reports, the financial assets of these organizations were immediately frozen. In addition, Russia has assisted the United States in investigation of terrorist financing, providing vital financial documentation and other evidence

establishing the criminal activities of the Benevolence International Foundation (BIF). Russian authorities have also provided U.S. federal law enforcement authorities with valuable evidence relating to terrorist fundraising activities of an individual currently being prosecuted in the U.S. for possession of counterfeit currency.

Following an aggressive campaign to reform Russia's anti-money laundering regime, Russia became a full FATF member in June 2003. During its first plenary as a full-fledged FATF member, Russia announced its intention to create a Central Asian FATF-style Regional Body (FSRB). In October 2004, Russia successfully kicked off the FSRB, the Eurasian Group on Combating Legalization of Proceeds from Crime and Terrorist Financing (EAG), which includes Belarus, China, Kazakhstan, Kyrgyzstan, Tajikistan and Russia as members, and several other nations and multilateral organizations as observers to the group, including the United States. Concurrent with the first plenary meeting of the EAG, Russia also hosted the annual FATF Typologies meeting in Moscow in early December 2004.

The United States and Russia signed a Mutual Legal Assistance Treaty in 1999, which entered into force on January 31, 2002. To date, the FSFM has signed cooperation agreements with the Financial Intelligence Units (FIUs) of the United States, Poland, Britain, the Czech Republic, Belgium, Italy, Panama, France, Estonia, Ukraine, Colombia, Cyprus, Finland, Latvia, Luxembourg, Switzerland, and the United Kingdom. Additionally, the FSFM is an active member of the Egmont Group, having taken on sponsorship of several candidate countries for 2004. U.S. law enforcement agencies exchange operational information with their Russian counterparts on a regular basis.

In addition to membership in the FATF, Russia holds membership in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). Russia ratified the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime in January 2001. Russia is a party to the 1988 UN Drug Convention and on May 26, 2004, became a party to the UN Convention against Transnational Organized Crime. In November 2002, Russia ratified the UN International Convention for the Suppression of the Financing of Terrorism. Russia also became a signatory to the UN Convention against Corruption.

Russia has developed a solid legislative and regulatory foundation for combating money laundering and terrorism financing. Given its role in spearheading the creation of the EAG, Russia has demonstrated both the political will and a capability to play a more proactive role in improving the region's capacity for countering money laundering and terrorism financing. Nevertheless, vulnerabilities continue. Russia has committed to improving CBR oversight of shell companies as well as closer scrutiny of banks that do not carry out traditional banking activities. Further, the Government of Russia has drafted a national money laundering strategy, which is currently under review and will likely be enacted in 2005. Finally, endemic and high-level corruption continues to undermine Russia's best efforts. Persistent and significant deficiencies in Russia's overall business operating environment pose formidable challenges to Russia's efforts to establish a well functioning and comprehensive anti-money laundering/counterterrorism financing regime.

The Government of Russia should strive to contain official corruption and increase transparency in the corporate environment. Russia should commit adequate resources to its regulatory and law enforcement entities to enable them to fulfill their responsibilities. Russia should also enact legislation that would provide for the seizure of instruments, as opposed to merely the proceeds, of criminal activity. Finally, Russia should continue to play a leadership role in the region with regard to anti-money laundering and counterterrorist finance regime implementation.