

Samoa

Samoa does not have major organized crime, fraud, or drug problems. The most common crimes that generate revenue within the jurisdiction appear to be low-level fraud and theft. The domestic banking system is very small, and there is relatively little risk of significant money laundering derived from domestic sources. Samoa's offshore banking sector is relatively small but insufficiently regulated. The Government of Samoa (GOS) enacted the Money Laundering Prevention Act (the Act) in June 2000. This law criminalizes money laundering associated with numerous crimes, sets measures for the prevention of money laundering and related financial supervision. Newly adopted regulations and guidelines fully implementing this legislation came into force in December 2002. Under the Act, a conviction for a money laundering offense is punishable by a fine not to exceed WST \$1 million (approximately \$354,000), a term of imprisonment not to exceed seven years, or both.

The Act requires financial institutions to report transactions considered suspicious to a Money Laundering Prevention Authority (MLPA), the Samoa Financial Intelligence Unit (FIU) currently working under the auspices of the Governor of the Central Bank. The MLPA receives and analyzes disclosures, and if it establishes reasonable grounds to suspect that a transaction involves the proceeds of crime, it refers the information to the Attorney General and the Commissioner of Police. In 2003, Samoa established under the authority of the Ministry of the Prime Minister, an independent and permanent Transnational Crime Unit (TCU). The TCU is staffed by personnel from the Samoa Police Service, Immigration Division of the Ministry of the Prime Minister and Division of Customs. The TCU is responsible for intelligence gathering and analysis and investigating transnational crimes, including money laundering, terrorist financing and the smuggling of narcotics and people.

The Act requires financial institutions to record new business transactions exceeding WST \$30,000 (approximately \$10,000), to retain records for a minimum of seven years, and to identify all parties to the transactions. This threshold reporting system exposes the financial institutions to potential abuse. As it is written, financial institutions are under no obligation to maintain any record for single transactions where the amount is under WST \$30,000, so numerous small transactions could avoid detection. Nevertheless, Section 4.3(a) of the Money Laundering Prevention Regulations 2002 requires financial institutions to identify their customers when "there are reasonable grounds for believing that the one-off transaction is linked to one or more other one-off transactions and the total amount to be paid by or to the applicant for business in respect to all of the linked transactions is Samoan Tala \$30,000, or the equivalent in another currency." Section 12 of the Act establishes that all financial institutions have an obligation under this law to "develop and establish internal policies, procedures and controls to combat money laundering, and develop audit functions in order to evaluate such policies, procedures and controls." The new Regulations and Guidelines also remedy the lack of specificity in the Act about the obligation of financial institutions to establish the identity of the beneficial owner of an account managed by an intermediary. Specifically, Section 12.06 of the new Money Laundering Prevention Guidelines for the Financial Sector provides that "...If funds to be deposited or invested are being supplied by or on behalf of a third party, the identity of the third party (i.e., the underlying beneficiary) should also be established and verified." The law requires individuals to report to the MLPA if they are carrying with them WST \$10,000 (approximately \$3,300) or more, in cash or negotiable instruments, upon entering or leaving Samoa.

The Act removes secrecy protections and prohibitions on the disclosure of relevant information. Moreover, it provides protection from both civil and criminal liability for disclosures related to potential money laundering offenses to the competent authority.

The Central Bank of Samoa, the Office of the Registrar of International and Foreign Companies, and the MLPA regulate the financial system. There are three locally incorporated commercial banks, supervised by the Central Bank. The Office of the Registrar of International and Foreign Companies

has responsibility for regulation and administration of the offshore sector. There are no casinos, but two local lotteries are in operation.

Samoa is an offshore financial center, with six offshore banks licensed. For entities registered or licensed under the various Offshore Finance Centre Acts there are no currency or exchange controls or regulations, and no foreign exchange levies payable on foreign currency transactions. No income tax or other duties, nor any other direct or indirect tax or stamp duty is payable by registered/licensed entities. In addition to the six offshore banks, Samoa currently has 10,502 international business corporations (IBCs), three international insurance companies, five trustee companies, and 181 international trusts. Section 16 of the Offshore Banking Act does not prohibit persons who have been sentenced for an offense involving dishonesty from applying to be employed as directors or managers of offshore banks. The Act only requires prior approval, in writing, of the Minister, without setting any criteria to guide the decision. In addition, there is no provision in the Act that specifies the qualifications for an owner/shareholder of an offshore bank. IBCs may be registered using bearer shares and shelf companies that conceal the identity of the beneficial owner and the date of incorporation. Corporate entities may be listed as officers and shareholders because Samoan IBCs have all the legal powers of a natural person. There are no requirements to file annual statements or annual returns. These provisions make IBCs particularly attractive to money launderers, and Samoan authorities have not yet addressed them.

International cooperation can only be provided when Samoa has entered into a mutual cooperation agreement with the requesting nation. Under the Act, the MLPA has no powers to exchange information with overseas counterparts. The inability of the MLPA simply to exchange information on an administrative level is a material weakness of the current system. However, according to a 2003 Samoa Report to the UN Counter Terrorism Committee, Samoa is currently reviewing the legal framework for the effective operation of the MLPA in order to strengthen domestic and international information exchange. In addition, the Office of the Attorney General, in conjunction with the Central Bank of Samoa, the Ministry of Police and the Division of Customs of the Ministry for Revenue, is currently preparing amendments to the Money Laundering Prevention Act of 2000 for purposes of strengthening and complementing legislation that is being drafted or developed, including the Proceeds of Crime Bill, the Mutual Assistance in Criminal Matters Bill, and the Extradition Amendment Bill.

Samoa signed the UN International Convention for the Suppression of the Financing of Terrorism in November 2001, and ratified it on September 27, 2002. In April 2002, Samoa became a party to the Prevention and Suppression of Terrorism Act. This legislation defines and provides for terrorist offenses, including offenses dealing specifically with the financing of terrorist activities. The combined effect of the Money Laundering Prevention Act of 2000 and the Prevention and Suppression of Terrorism Act of 2002 is to make it an offense for any person to provide assistance to a criminal to obtain, conceal, retain or invest funds or to finance or facilitate the financing of terrorism.

Samoa is a member of the Asia/Pacific Group on Money Laundering and the Pacific Island Forum. Samoa has not signed the 1988 UN Drug Convention.

Since the passage of the Money Laundering Prevention Act in June 2000, Samoa has continued to strengthen its anti-money laundering regime and has issued regulations and guidelines to financial institutions so that they have a clear understanding of their obligations under the Act. Particular emphasis should be directed toward regulation of the offshore financial sector, principally the establishment of due diligence procedures for owners and directors of banks and the elimination of anonymous accounts for onshore and offshore banks. The GOS should enact legislation to identify the beneficial owners of IBCs to help ensure that criminals do not use them for money laundering or other financial crimes. Samoa should adopt its pending legislation to allow for international cooperation and information sharing.

San Marino

San Marino, a small independent enclave located within Italy, is the 3rd smallest country in Europe after the Holy See and Monaco. San Marino claims to be the oldest republic in the world founded in 301 A.D. San Marino's policies and social trends closely track those of its larger neighbor. San Marino has a small economy but a rather large financial sector. The Government of San Marino (GOSM) passed money laundering legislation in 1998. In June 2003 a law was passed that provides functional integration between the Office of Banking Supervision and the Central Bank, strengthening the supervisory system that will help counter money laundering and terrorist financing. Also in 2003, the Office of Banking Supervision issued Circular No. 33 addressed to banks and financial companies that obligates the collection of customers' personal data and their business/professional activity. The GOSM has also introduced a draft law on the "Provisions of Anti-Terrorism, Anti-Money Laundering and Anti-Insider Trading." The draft legislation criminalizes terrorism; introduces rules supplementing the Anti-Money Laundering law of 1998 by incorporating modifications recommended by the FATF and the Council of Europe; provides for the freezing of financial assets or property; allows special investigative techniques; and contains rules on insider trading. In April 2003, San Marino had its second round of mutual evaluations by MONEYVAL.

The GOSM is a party to the UN International Convention for the Suppression of the Financing of Terrorism. It should become a party to the UN convention against Transnational Crime.

Sao Tome and Principe

Sao Tome, which has a small economy and only one commercial bank, is not a regional financial center.

Sao Tome is a party to the 1988 UN Drug Convention.

Sao Tome should criminalize money laundering and terrorist financing. Sao Tome should also enact legislation allowing the GOSTP to freeze assets related to money laundering and terrorist financing. Sao Tome should become a party to both the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Crime.

Saudi Arabia

Saudi Arabia is a growing financial center in the Gulf Region of the Middle East. There is little known money laundering enforcement in Saudi Arabia related to traditional predicate offenses. However, Saudi donors and unregulated charities have been a major source of financing to extremist and terrorist groups over the past 25 years. Following the al-Qaida bombings in Riyadh on May 12, 2003, the government of Saudi Arabia has taken steps to help counteract terrorist financing.

All ten commercial banks in Saudi Arabia operate as standard "western-style" financial institutions. There are no "Islamic" banks in Saudi Arabia. In 2003 Saudi Arabia approved a new anti-money laundering law that for the first time contains criminal penalties for money laundering and terrorist financing. The law bans conducting commercial or financial transactions with persons or entities using pseudonyms or acting anonymously; requires financial institutions to maintain records of transactions for a minimum of ten years and adopt precautionary measures to uncover and prevent money laundering operations; requires banks and financial institutions to report suspicious transactions; authorizes government prosecutors to investigate money laundering and terrorist financing; and allows for the exchange of information and judicial actions against money laundering operations with countries with which Saudi Arabia has official agreements. Saudi Arabia did pursue anti-money laundering investigations prior to the enactment of the 2003 law. It is believed 70-80 percent of those cases involved narcotics related money laundering.

Saudi Arabian Monetary Authority (SAMA) guidelines correspond to the forty anti-money laundering recommendations of the Financial Action Task Force (FATF). On May 27, 2003 SAMA issued updated anti-money laundering and counter terrorist finance guidelines for the Saudi banking system. The guidelines require that banks have mechanisms to monitor all types of “Specially Designated Nationals” as listed by SAMA; that fund transfer systems be capable of detecting specially designated names; that SAMA circulars on opening accounts and dealing with charity and donation collection be strictly adhered to; and that the banks be able to provide the remitter’s identifying information for all outgoing transfers. Saudi law prohibits nonresident individuals or corporations from opening bank accounts in Saudi Arabia without the specific authorization of the SAMA.

All banks are also required to report any suspicious transactions to the recently created Saudi Financial Intelligence Unit (FIU), which is under the authority of the General Security Department of the Interior Ministry. The Saudi FIU is in its early formative stages, but it appears the FIU will collect and analyze suspicious transaction reports and other available information and decide to make referrals the Mabahith or other entities for action. The FIU will be staffed by officers from the Mabahith, SAMA, the Ministry of Commerce, and the Ministry of Interior’s Bureau of Investigation and Prosecution.

Saudi Arabia appears to be implementing UN Security Council Resolutions on terrorist financing. It has frozen accounts of individuals and organizations in response to information provided by the USG. The Government of Saudi Arabia (GOSA) signed a multilateral agreement under the auspices of the Arab League to fight terrorism. Saudi Arabia has signed but not ratified the UN International Convention for the Suppression of the Financing of Terrorism. In September 2003, the FATF and the GCC carried out a “mutual evaluation” of Saudi Arabia to assess compliance with the FATF anti-money laundering and terrorist finance recommendations.

Hawala transactions outside banks and licensed moneychangers are illegal in Saudi Arabia. Reportedly, some money laundering cases that SAMA has investigated in the past decade involved the hawala system. In order to help counteract the appeal of hawala, particularly to many of the approximately six million expatriates living in Saudi Arabia, Saudi banks have taken the initiative and created fast, efficient, high quality, and cost-effective fund transfer systems. An important advantage for the authorities in combating potential money laundering and terrorist financing is that the senders and users of fund transfers through this formal financial sector are clearly identified.

Contributions to charities in Saudi Arabia are usually Zakat, which is an Islamic religious duty with specified humanitarian purposes. However, over the past decade, according to a 2002 report to the United Nations Security Council, al-Qaida and other jihadist organizations collected between \$300 and \$500 million and the majority of those funds originated from Saudi charities and private donors.

To help address this problem, in 2003, Saudi Arabia established a High Commission for oversight of all charities. Charities in Saudi Arabia are to be licensed, registered, audited, and supervised. New rules announced in 2003 include stipulations that accounts can be only opened in Saudi Riyals; there are enhanced customer identification requirements; there is one main consolidated account for each charity; there are no cash disbursements—payments may be made only by checks payable to the first beneficiary and deposited in a Saudi bank; the use of ATM and credit cards for charitable purposes will not be permitted; there will be no transfers outside of Saudi Arabia. The Saudi government is still working to implement these measures.

Saudi Arabia took specific legal and regulatory steps in 2003 to combat money laundering and terrorist financing. Progress is being made in establishing an operational Financial Intelligence Unit. However, as in many countries in the region there is an over-reliance on Suspicious Transaction Reporting to generate money laundering investigations. Law enforcement agencies should take the initiative and proactively generate investigations. Saudi Arabia should move rapidly to monitor and enforce the new anti-money laundering and terrorist finance laws, regulations and guidelines. The new requirements relating to charities are far reaching. However, significant loopholes remain including

the definition of a charitable organization and the ability of a group or individual previously affiliated with suspect charitable organizations to simply cease referring to itself as a charity. Saudi Arabia should take affirmative steps to close loopholes and should ratify the UN International Convention for the Suppression of the Financing of Terrorism.

Senegal

Senegal's banking system and formal and informal money-exchange systems are vulnerable to the laundering of proceeds from corruption, narcotics trafficking, illegal gems and arms-trafficking, and trafficking in persons, all of which are prevalent in West Africa. Numerous foreign banks, including several French and African banks, have branches in Senegal.

Article 102 of Senegal's 1997 drug code criminalizes narcotics-related money laundering as a misdemeanor punishable by up to 10 years in prison. The last money laundering prosecution under this law was in 1999. The drug code requires banks to report suspicious transactions believed to be linked to narcotics trafficking. Banks are required to keep records between one and ten years, depending on the type of record. The drug law authorizes the seizure of assets related to narcotics trafficking. Banking secrecy provisions can only be waived by a judge's order as part of case involving narcotics. There is no requirement to report cross-border currency transactions.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA), based in Dakar, Senegal. GIABA recently hosted a self-evaluation exercise on anti-money laundering capabilities in conjunction with the International Monetary Fund and ECOWAS member states. A Senegalese magistrate is the acting head of GIABA. The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the countries in the West African Economic and Monetary Union (WAEMU): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal, and Togo, all of which use the French-backed CFA franc currency, which is also linked to the euro. All bank deposits over approximately \$7,700 made in BCEAO member countries must be reported to the BCEAO, along with customer identification information.

Although current law limits money laundering to drug-related activities, a draft law is being prepared which will make money laundering a crime unto itself. The law would apply to banks, nonbank financial institutions, and intermediaries. The proposed law would criminalize money laundering for many serious crimes. Under the law, banking information could be shared with law enforcement authorities, and individuals could be held legally responsible if they do not report suspicious activity. The law would also expand current asset seizure provisions so that authorities could seize assets related to the laundering of proceeds from many serious crimes.

Senegal is expected to soon adopt a Uniform Act on Money Laundering that implements standards drafted by the WAEMU member states in conjunction with GIABA and the BCEAO. Under the harmonized WAEMU standards, Senegal will join the other seven WAEMU countries and ultimately the 15 members of ECOWAS in updating the judicial and penal code concerning money laundering and crimes of corruption, establishing a Financial Intelligence Unit (FIU), and strengthening law enforcement and detection capability of money laundering and corruption. Senegal is working closely with the Department of Treasury, multilateral organizations such as the World Bank, and other donors on providing training on money laundering to the financial community, law enforcement professionals, and the judiciary.

In September 2002, the WAEMU Council of Ministers, which oversees the BCEAO, approved an anti-money laundering regulation applicable to banks and other financial institutions, casinos, travel agencies, art dealers, gem dealers, accountants, attorneys, and real estate agents. The regulation is

subject to review by member countries, which would be responsible for implementing many provisions of the regulation.

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

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

The WAEMU Council of Ministers issued another directive in September 2002 requesting member countries to pass legislation requiring banks to freeze the accounts of any persons or organizations designated by the UN 1267 Sanctions Committee.

In 2001 the BCEAO hosted a conference on money laundering. In July 2002 Senegal participated in the 2002 West African Joint Operation Conference (WAJO) that promotes regional law enforcement cooperation against drug trafficking, terrorism, and money laundering.

Senegal is a party to the 1988 UN Drug Convention and has signed and ratified, the UN Convention against Transnational Organized Crime. The Government of Senegal has also indicated that the ratification of the UN International Convention for the Suppression of Financing of Terrorism is underway.

Senegal should criminalize terrorist financing and money laundering for all serious crimes. The GOS should work with its counterparts in GIABA and its partners in WAEMU to establish a comprehensive anti-money laundering regime in the region. Senegal should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Serbia and Montenegro

At the crossroads of Europe and on the highway known as the “Balkan route,” narcotics trafficking; smuggling of persons, drugs, weapons and pirated goods; money laundering; and other criminal activities continue in Serbia and Montenegro (SAM, formerly the Federal Republic of Yugoslavia (FRY)). The 2001 Foreign Currency and Foreign Trade Laws, as well as more effective enforcement of intellectual property rights laws, have reduced the volume of smuggled and pirated goods in the SAM substantially. Nonetheless, the country still has a significant black market for such goods. Income from narcotics trafficking, however, is typically not used to support this black market but instead is laundered in the real estate market, one of the most popular ways to legalize criminal proceeds in SAM. Trade-based money laundering, in the form of over- and under-invoicing, is another of the most common methods of money laundering. The Government maintains that the majority of criminal proceeds from narcotics trafficking laundered in the country are derived from illegal activities of the Kosovar “Narco-Mafia,” and Serbian officials estimate that up to half of all financial transactions in SAM may be connected in some way to money laundering. SAM has had an uphill battle against an entrenched problem; estimates of money laundered by Yugoslavia’s former president Slobodan Milosevic and his associates go as high as one billion U.S. dollars.

The European Union has an ongoing lawsuit in New York against the U.S. tobacco company RJ Reynolds. The EU accuses RJR of knowingly selling cigarettes to criminal networks, which paid for

their purchases using money earned in drug and arms smuggling. Among the claims made by the EU plaintiffs is that Republic of Montenegro Prime Minister Djukanovic was a witting participant and profiteer in this smuggling and money laundering scheme. The lawsuit alleges, inter alia, that the Italian Mafia established Montenegrin Tabak Transit (MTT) in the mid-1990s under the official sanction of the Montenegrin Foreign Investment Agency and the special protection of Djukanovic. MTT in turn funneled mafia payments—in the form of “licensing payments”—to then Yugoslav President Milosevic’s regime and to Djukanovic and other officials, using banks in Switzerland and Liechtenstein.

It is also worth noting that Serbian judicial authorities have an ongoing investigation against two former high-ranking civil servants on money laundering charges, the former security adviser to the Serbian Prime Minister, and the former director of the Serbian Bank Rehabilitation Agency, who allegedly were involved in laundering money through offshore accounts in several financial safe haven countries. The two officials have stepped down from their government posts.

State Union: In March 2002, the leadership of the FRY, Serbia and Montenegro signed the Belgrade Agreement on restructuring the relationship between the two republics. On February 4, 2003, the FRY parliament voted to adopt a new Constitutional Charter that established the state union of “Serbia and Montenegro.” Under this state union structure, most governmental authority previously addressed by federal Yugoslav authorities devolved to the individual republics. As a result, responsibility for the laws and institutions determining policies and legislation has been shifted. Consequently, both the Republic of Serbia (Serbia) and the smaller Republic of Montenegro (Montenegro) have addressed money laundering and terrorism financing—but each has done so in its own way. Banks in both republics have demonstrated remarkable tolerance for and compliance with the laws in their respective jurisdictions.

In 2001, the federal Yugoslav authorities prepared a national strategy to fight terrorism and established a national coordinating body. However, this body fell into abeyance when the FRY transformed into the state union in February 2003. Ratification to international Conventions as well as treaties currently lies at the overarching State Union level.

Serbia: The Yugoslav Federal Assembly adopted an anti-Money Laundering Law in September 2001; it came into effect in July 2002. The law defines money laundering to mean depositing, or introducing into the financial system in any other manner, money which has been acquired through illegal activity. This includes money derived from the gray market economy and from arms and narcotics trafficking. Criminal penalties for money laundering violations range from six months’ to eight years’ imprisonment, while civil penalties range from 45,000 to 450,000 dinars (\$650 to \$6,500) per offense.

Among the entities required to take actions and measures aimed at uncovering and preventing money laundering under the law are: commercial and savings banks and other financial credit institutions, the postal savings bank, the post office, commercial enterprises, all government entities, the National Bank of Yugoslavia and its clearing and payments department, foreign exchange bureaus, casinos, pawnshops, stock exchanges, and national lottery organizers. The obliged entities are required to identify persons opening an account “or establishing any other kind of lasting business cooperation with the client” and to report on every cash transaction exceeding 10,000 euros or 600,000 dinars, as well as any suspicious transaction. Similar reporting thresholds apply to insurance policies and cross-border currency transactions. The law also provides for record keeping and established special procedures for tracking terrorist financing.

The law also provides for the establishment of a financial intelligence unit (FIU), the Federal Commission for the Prevention of Money Laundering (FCPML), to assume responsibility for receiving and disseminating currency and suspicious transaction reports; it also has responsibility for countering the financing of terrorism via its Department for the Suppression of the Financing of Terrorism. FCPML is authorized to suspend a suspicious transaction or freeze assets for 48 hours.

In March 2002, the FCPML was established as an independent federal body by governmental decree; it became operational on July 1, 2002. At its founding, both the law and the FIU were at the federal level, and in name were applicable to both Serbia and Montenegro. On February 4, 2003, reflecting the dissolution of the centralized federal state into the two republic entities, and pursuant to Article 13 of the Constitutional Charter and Implementation Law, the FCPML, up until then a federal FIU, became the FIU for the Serbian Republic. In its first year of existence, FCPML has received over 60,000 reports, and 162 suspicious cases were disseminated to law enforcement. In its first 18 months, the Serbian Administration has forwarded eight cases of possible money laundering to the prosecutor's office, with four still being investigated and two now in court proceedings. In July 2003, FCPML became a member of the Egmont Group and participates actively in information exchange with counterpart FIUs.

On July 18, 2003, Serbia passed a new law codifying the powers of the Central Bank, decreasing its independence and establishing parliamentary control over its operations. Bank supervision in the National Bank of Serbia was inactive for a three-month period due to turnover, but a new Director of Bank Supervision has since arrived.

A new draft money laundering law implementing all international standards, extending the list of obligated entities to include attorneys and accountants and harmonizing legislation with all European Union (EU) Directives, was under review and submitted in the beginning of October 2003. The new law was approved by all of the relevant authorities, but then a parliamentary crisis broke out, and the procedure was suspended. On December 28, 2003, Serbia held a parliamentary election and as a result, the ratio between parties in the Parliament has changed. Once a new government is formed, an urgent procedure for the adoption of the draft law will be requested. However, there is still the possibility that the bill will need to pass to the relevant authorities for approval once again.

The Serbian FCPML is the authority charged with enforcing the UN terrorism sanction lists; although it routinely checks for accounts, it has found no evidence of terrorism financing within the banking system and no evidence of alternative remittance systems in use. The Department for Combating Organized Crime (UBPOK), in the Ministry of Interior, is the law enforcement body responsible for countering terrorism. UBPOK cooperates and shares information with its counterpart agencies in all of the countries bordering Serbia and Montenegro.

Serbia has no terrorism financing law consistent with the standards contained in international conventions, and its legislative and institutional framework for combating terrorism financing remains weak. Draft legislation is pending. Despite the fact that according to the Serbian Criminal Code, business licenses of legal or natural persons may be revoked and business activities banned if the subject is found guilty of criminal activities, including narcotics trafficking or terrorism financing, Serbia is hamstrung with regard to international assistance in investigating terrorism financing. Serbia's police may not make use of the Mutual Legal Assistance Treaty (MLAT) process in terrorism financing cases, and therefore forfeit any available international assistance, because under Serbian law, the MLAT process is restricted to crimes with penal sentences equal to or exceeding ten years. Under current law, the maximum term for a money laundering or terrorism financing offense is eight years. Under Serbia's Criminal Procedure Code, an MLAT request for assistance in investigating terrorism activities requires the approval of an investigative judge. However, investigative judges, for a number of reasons, often do not grant these requests. Serbia is currently in the process of amending its Criminal Procedure Code to bring it into conformity with Council of Europe standards. Serbia has no asset seizure or forfeiture law. Actual asset seizures can only be carried out by court order.

Montenegro: In 1996, in an effort to lure needed funds, Montenegro proclaimed itself an offshore area and allowed financial intermediaries to do business—without controls—for a percentage of the profit. Hundreds of millions of dollars worth of money passed through Montenegrin offshore accounts annually; speculation is that much of the money came from criminal activity.

Montenegro has changed in a very short time. In August 2002, the Central Bank of Montenegro (CBCG) issued a decree that required banks and other financial institutions to report suspicious transactions, establish anti-money laundering control programs and train their employees on money laundering matters. Finally, in response to the proliferation of its offshore sector in the past decade, the Montenegrin government required offshore banks to re-register, post a one million Euro bond or fee, and to reestablish themselves as regular banks. Since none of the offshore entities has done this, the Central Bank considers them all dissolved. The Finance Ministry has not released complete information about the disposition of the 400 offshore entities whose names they turned over to CBCG.

Montenegro passed anti-money laundering legislation on September 24, 2003. The new law obligates banks, post offices, state entities, casinos, lotteries and betting houses, insurance companies, jewelers, travel agencies, auto and boat dealers, and stock exchange entities to file reports on all transactions exceeding 15,000 euros as well as on any related transactions that aggregate 15,000 euro or more, even if each particular transaction does not exceed the threshold. Failure to report, according to the law, could result in fines up to 20,000 euros as well as sentences of up to 12 years. The new law establishes record keeping requirements and provides for the establishment of an FIU that would receive, analyze, and disseminate the reports to the competent authorities. The Government of the Republic of Montenegro adopted "The Act on Forming FIU" in December of 2003 and had a deadline of the end of January 2004 for naming the head of this agency.

Money laundering was also criminalized in a new Criminal Code. Montenegro amended its Criminal Code in June 2003 to enable the government to confiscate money and property involved in criminal activity. Additionally, according to the Code, business licenses of legal or natural persons may be revoked and business activities banned if the subject is found guilty of criminal activities, including narcotics trafficking or terrorism financing. Montenegro is currently in the process of amending its Criminal Procedure Code to bring it into conformity with Council of Europe standards. Montenegro has no asset seizure or forfeiture law. Actual asset seizures can only be carried out by court order.

Montenegro has no antiterrorism financing law that approaches international standards, nor does Montenegro's anti-money laundering legislation include the detection and prevention of terrorism financing within the scope of the FIU's responsibilities. Rather, the Sector for Bank Control, within the Montenegrin Central Bank (CBCG), will take this responsibility. CBCG has the authority to suspend a transaction or freeze assets on suspicion of money laundering or terrorism financing for up to 72 hours. No terrorism financing has been detected within the Montenegrin banking system.

Kosovo: Since 1999, Kosovo has been governed by the United Nations Interim Administration in Kosovo (UNMIK). It does not fall under the jurisdiction of either Serbia or Montenegro. Recognizing that as Kosovo's neighbors tighten their anti-money laundering regimes, Kosovo itself could become a haven for money laundering, the UN has determined that Kosovo must adopt a strict approach to the fight against money laundering. As part of the transition toward autonomous governance, the UN has focused on involving the Kosovar-run Provisional Institutions of Self-Governance (PISG) in ten areas, including the operations of a financial intelligence unit.

Currently, the operative law in Kosovo incorporates laws in effect in Kosovo prior to 1989, supplementary UNMIK regulations, as well as laws promulgated from the Kosovo Assembly. However, none of these laws provides any clear prohibition of money laundering or requires that suspicious transactions be reported. Additionally, it is unclear whether UNMIK can designate organizations or persons involved in terrorist acts or freeze/confiscate assets of such entities. Legal advisors were seeking to resolve these issues at the close of 2003. A draft law was drawn up in February 2003, called "On the Deterrence of Money Laundering and Related Offenses"; this law appears to be approximately as comprehensive as similar laws in Kosovo's Balkan neighbors. However, the draft regulation has been in internal UN legal review and was not yet promulgated by the end of 2003. If the Regulation is implemented as drafted, a Kosovo Financial Intelligence Centre

(KFIC) will be established to ensure compliance with the proposed Regulation's record keeping and reporting requirements. The Regulation, as drafted, would also regulate financial accounting of nongovernmental organizations, which has been an area of terrorist financing concern in Kosovo.

SAM has no laws governing its cooperation with other governments, related to narcotics, terrorism, or terrorist financing. Cooperation is instead based on participation in Interpol, bilateral cooperation agreements, and agreements concerning international legal assistance. There are no laws at all governing the sharing of confiscated assets with other countries, nor is any legislation under consideration; SAM may at this time enter into bilateral agreements for this purpose.

Serbia and Montenegro has a legal assistance arrangement with the U.S., governed by the 1901 Convention on Extradition of Offenders. SAM has signed 34 bilateral agreements on mutual legal assistance with 25 countries: Albania, Algeria, Austria, Belgium, Bulgaria, the Czech Republic, Denmark, France, Greece, The Netherlands, Croatia, Iraq, Italy, Cyprus, Germany, Poland, Romania, Hungary, Mongolia, Russian Federation, Slovakia, Spain, Switzerland, Turkey, the United Kingdom, and the United States. These agreements authorize extradition of suspected terrorists. Both SAM and its constituent republics cooperate with their counterparts and neighbors. In April 2003, SAM joined eight other participants in the South Eastern Europe Cooperation Process, in adopting a joint "Belgrade Declaration" to call for the continuation of regional cooperation and the intensification of the fight against terrorism and organized crime. SAM worked with Interpol to set up an office for that organization in Belgrade as part of its efforts to contribute to the fight against terrorism and other transnational crimes.

Serbia and Montenegro is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. On October 9, 2003, SAM ratified the Council of Europe's Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, and the Convention will go into full force on February 1, 2004. SAM has ratified eight of the 12 UN Conventions or Protocols dealing with terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism, although the domestic implementation procedures are not providing the framework for full application in either republic. In December 2003, SAM became a signatory to the UN Convention Against Corruption. As a new member of the Council of Europe, SAM is a full and active member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), and underwent a first-round evaluation by a team from that Committee in October 2003.

Montenegro should establish its FIU and both Serbia and Montenegro should work to ensure that resources are available for the FIUs to work effectively and efficiently. Both republics should expand their anti-money laundering legislation to include all serious crimes, and enact legislation to establish asset seizure and forfeiture regimes. Both should also continue to participate in international fora that offer training and technical assistance for police, customs, and judiciary officials involved with combating money laundering and terrorist financing. They should also both criminalize terrorism financing specifically and implement a comprehensive framework to support an antiterrorism regime of international standards.

Seychelles

Seychelles is not a major financial center, but it does have a developed offshore financial sector, which makes the country vulnerable to money laundering.

The Government of Seychelles (GOS), in efforts to diversify its economy beyond tourism, has taken steps to develop an offshore financial sector to increase foreign exchange earnings. The GOS actively markets Seychelles as an offshore financial and business center that allows the registration of nonresident companies. There are currently over 4,800 registered international business companies

(IBCs) in Seychelles that pay no taxes in Seychelles, and are not subject to foreign exchange controls. The Seychelles International Business Authority (SIBA), which acts as the central agency for the registration for IBCs, promotes the fact that IBCs need not file annual reports. The SIBA is part of the Ministry of International Trade, and also manages the Seychelles International Trade Zone.

In addition to IBCs, Seychelles permits offshore trusts (registered through a licensed trustee), offshore insurance companies, and offshore banking. Three offshore insurance companies have been licensed, but no mutual fund companies. The International Corporate Service Providers Act 2003 will be entering into force very soon. This act is designed to regulate all the activities of the corporate service providers as well as the trustee service providers. It will strengthen existing legislation regarding due diligence and know your customer rules.

A major weakness of the Seychelles' offshore program is that it still permits the issuance of bearer shares, a feature that can facilitate money laundering by making it extremely difficult to identify the beneficial owners of an IBC. Seychelles officials stated in 2000 that they were reviewing the question of bearer shares and intended to outlaw them. In the interim, the GOS has indicated that it will not approve the issuance of any more bearer shares.

No offshore casinos or Internet gaming sites have yet been licensed; if they are, they will be subject to stringent legislation modeled on the Australian Internet Gaming Act. There are no cross-border currency reporting requirements, but the point of entry at the international airport is under constant supervision by Customs and the Police, who search suspicious incoming or outgoing passengers.

In 1995, the GOS passed the Economic Development Act (EDA), which provided concessions (protection from asset seizure and immunity from prosecution for crimes committed abroad and most crimes, other than violent crimes and narcotics trafficking, committed in the Seychelles) to individuals investing more than \$10 million in the Seychelles. As a result of the enactment of the EDA, FinCEN issued an advisory to U.S. banks and financial institutions calling on them to exercise enhanced scrutiny with respect to transactions involving Seychelles. The GOS repealed the EDA in 2000. In May 2003, FinCEN withdrew its advisory, since the repeal of the EDA effectively addressed the concerns that had prompted the issuance of the advisory.

In 1996, the GOS enacted the Anti-Money Laundering Act (AMLA), which criminalizes the laundering of funds from all serious crimes, requires financial institutions and individuals to report to the Central Bank transactions involving suspected cases of money laundering, and establishes safe harbor protection for individuals and institutions filing such reports. There are no bank secrecy laws in Seychelles. The AMLA imposes record keeping and customer identification requirements for financial institutions, and also provides for the forfeiture of the proceeds of crime.

Under the AMLA, money laundering controls are applied to nonbanking financial institutions, including exchange houses, stock brokerages, casinos, and insurance agencies, but not to lawyers and accountants. No arrests and/or prosecutions have been made for money laundering and terrorist financing since January 1, 2003.

Under the AMLA, anyone who engages directly or indirectly in a transaction involving money or other property (or who receives, possesses, conceals, disposes of, or brings into Seychelles any money or property) associated with a crime, knowing or having reasonable grounds to know that the money or property is derived from an illegal activity, is guilty of money laundering. In addition, anyone who aids, abets, procures, or conspires with another person to commit the crime, while knowing, or having reasonable grounds for knowing that the money was derived from an illegal activity, is likewise guilty of money laundering.

In 1998, the Central Bank of Seychelles issued a comprehensive set of guidance notes that further elucidated and strengthened the provisions of the AMLA. The Central Bank of the Seychelles receives and analyzes suspicious activity reports and disseminates them to the competent authorities. In

November 2002 the Central Bank circulated to all local commercial banks a document on due diligence issued by the Basel Committee

The Government of Seychelles intends to enact early in 2004 the Prevention of Terrorism Bill 2004. The proposed legislation will recognize the government's authority to identify, freeze, and seize terrorist finance-related assets. Currently the Mutual Assistance in Criminal Matters Act of 1995 empowers the Seychelles Central Authority to search and seize anything relevant to a proceeding or investigation relating to a criminal matter involving a serious offense under a written law of a requesting state.

The proposed Prevention of Terrorism Bill will strengthen the government's hand in this area. It will specifically provide for the forfeiture of assets. Even now the Seychelles authorities can work with states that are members of the Commonwealth, or have a treaty for bilateral mutual legal assistance with the Seychelles regarding criminal matters. Under current legislation assets used in the commission of a terrorist act can be seized, and legitimate businesses can be seized if used to launder drug money, support terrorist activity, or are otherwise related to criminal activities. Both civil and criminal forfeiture are allowed under current legislation. To date, no assets have been identified, frozen, or seized pertaining to terrorist financing, upon request of such a foreign state.

The transactions of charitable and nonprofit entities are scrutinized by the authorities to prevent their misuse, and such systems as hawala are regulated.

The Seychelles is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. The Seychelles implements fully the FATF Forty Recommendations on money laundering and its Eight Special recommendations on Terrorist Financing. The Seychelles is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. The Seychelles has signed the UN International Convention for the Suppression of the Financing of Terrorism. The Seychelles circulates to relevant authorities the updated lists of designations under Executive Order 13224. The Seychelles is in ongoing discussions with Kenya and Mauritius regarding a memoranda of understanding on drug trafficking.

The GOS should expand its anti-money laundering efforts by moving to immobilize bearer shares and requiring complete identification of beneficial owners of IBCs. The GOS should establish a financial intelligence unit to collect, analyze, and share financial data with foreign counterparts, in order to effectively combat money laundering and other financial crimes. Seychelles should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism and actively participate in ESAAMLG.

Sierra Leone

Sierra Leone, which has a small commercial banking sector, is not a regional financial center. Loose oversight of financial institutions, weak regulations, rampant corruption, and a prevalent informal money-exchange system create an atmosphere conducive to money laundering. Given the importance of the large diamond sector to the economy, the prevalence of money laundering in the diamond sectors of neighboring countries and the loose oversight of the financial sector, Sierra Leone's diamond sector is particularly vulnerable to money laundering. There are also allegations that the diamond trade intersects terrorist financing operations. The diamond trade is susceptible at many levels of exploitation, including cross-border trade, secondary level traders and agents, and suspect buyers. Furthermore, law enforcement and customs have limited understanding and capability to effectively investigate and control money laundering.

There is no specific legislation concerning money laundering. However, the Ministry of Justice is in the process of developing such laws. Progress towards implementing these laws has been stymied by severe lack of knowledge and technical capacity on behalf of the relevant Government of Sierra Leone

Ministries. Under the proposed laws, banks are required to record the identity of customers engaging in large currency transactions and to maintain adequate records necessary to reconstruct significant transactions in order to respond to government information requests. Banks are also required to report suspicious transactions, although they do not usually adhere to this requirement. Bank secrecy laws prevent the disclosure of client and ownership information except under court order.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA), based in Dakar, Senegal. Sierra Leone is currently meeting with members of (ECOWAS) to develop a draft model money laundering law.

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

Sierra Leone should criminalize money laundering and terrorist financing, enforce existing financial laws and regulations, and provide legal authority for the seizure of criminal and terrorist assets.

Singapore

As a significant international financial and investment center, and in particular as a major offshore financial center, Singapore is attractive to potential launderers. Bank secrecy laws and the lack of routine currency reporting requirements make Singapore an attractive destination to foreign drug traffickers, other foreign criminals, and terrorist organizations and their supporters seeking to launder their money, and for flight capital. Money laundering occurs mainly in the offshore sector, but may also occur in the nonbank financial system, including large numbers of money changers and remittance agencies.

Singapore has a sizeable offshore financial sector. In 2003, there were 116 commercial banks in Singapore, of which 50 were offshore banks, down significantly from 83 in December 2000. There are also 27 full banks and 39 wholesale banks in Singapore. All offshore banks are branches of foreign banks. Singapore does not permit shell banks, either in the domestic or offshore sectors. There are no offshore trusts, although banks may open trust, nominee, and fiduciary accounts. All banks in Singapore, whether domestic or offshore, are subject to the same regulation, record keeping, and reporting requirements, including regarding money laundering and suspicious transactions. Any person who wishes to engage in business, whether local or foreign, must register under the Companies Act. Every Singapore-incorporated company must have at least two directors, one of whom must be ordinarily resident in Singapore, and one or more company secretaries, who must be resident in Singapore. There is no nationality requirement. A company incorporated in Singapore has the same status and powers as a natural person. Bearer shares are not permitted. Casinos and Internet gaming sites are illegal in Singapore.

The Monetary Authority of Singapore (MAS) performs extensive checks on all applicants for banking licenses. These include a check to see if the bank is under adequate home country banking supervision, how long the bank has been in business, and its general reputation within the financial community. The MAS will need to revise its regulations, in line with the Revised FATF 40 Recommendations, to proscribe banks from entering into correspondent relationships with prohibited shell banks.

As a matter of policy, Singapore strongly opposes money laundering and terrorist financing. The Corruption, Drug Trafficking, and other Serious Crimes (Confiscation of Benefits) Act of 1999 (CDSA) criminalizes the laundering of proceeds from narcotics and over 180 other serious offenses, including foreign offenses which would be serious offenses if they had been committed in Singapore. The list of offenses may need to be revised to ensure consistency with the expanded list of predicate crimes under Recommendation 1 of the FATF's Revised Forty Recommendations in adopted in June,

2003. Financial institutions must report suspicious transactions and positively identify customers engaging in large currency transactions. Financial institutions are required to maintain adequate records to respond quickly to Government of Singapore (GOS) inquiries in money laundering cases. However, there are no reporting requirements on amounts of currency brought into or taken out of Singapore.

The Monetary Authority of Singapore, a semi-autonomous entity under the Ministry of Finance, serves as Singapore's Central Bank and financial sector regulator. MAS performs extensive prudential and regulatory checks on all applicants for banking licenses, including a check to see if the bank is under adequate home country banking supervision. Banks must have clearly identified directors. It is illegal to perform banking transactions without a license. In 2000, MAS first issued a series of regulatory guidelines (i.e., "Notices") requiring banks to apply "know your customer" standards, adopt internal policies for staff compliance, and cooperate with Singapore enforcement agencies on money laundering cases. These Notices are regulatory in nature and are enforceable by prosecution. Similar guidelines exist for securities dealers and other financial service providers. Banks must obtain documentation, such as passports or identity cards, from all personal customers so that the bank can verify their names, permanent contact addresses, dates of birth, and nationalities, and conduct inquiries into the bona fides of company customers..

The regulations specifically require that financial institutions obtain evidence of the identity of the beneficial owners of offshore companies or trusts. The guidelines also mandate specific record keeping and reporting requirements, outline examples of suspicious transactions that should prompt reporting, and establish mandatory intra-company point-of-contact and staff training requirements. MAS Notice 626 applies to banks, Notice 824 applies to finance companies, Notice 1014 applies to merchant banks, and Notice 314 to direct life insurers and brokers. MAS issued similar guidelines for securities dealers and investment advisors, and futures brokers and advisors.

In November 2002, the MAS revised its Notices to banks to enhance customer identification and record keeping requirements. The requirements to obtain satisfactory evidence of the identity of intermediary and/or beneficial owners apply to all accounts, including trust, nominee and fiduciary accounts. Additional identification requirements also apply to account applicants that are shell companies, clubs, societies or charities. The MAS recognizes that the Notices to banks will have to be further adapted to reflect the revised FATF Forty Recommendations adopted in June 2003.

The Suspicious Transaction Reporting Office (STRO) is Singapore's financial intelligence unit (FIU). Part of the Singapore Police Force's Commercial Affairs Department, it began operating on January 10, 2000. In the first ten months of 2003, the STRO received 1372 suspicious transaction reports (STRs), up from 1118 reports in 2002 and 549 reports in 2001. Of the reports received, 334 resulted in investigations in the first ten months of 2003, as compared to 436 resultant investigations during the whole of 2002, and just 264 resultant investigations during the whole of 2001.

As a leading financial center in Southeast Asia, Singapore has been a key player in the regional effort to stop terrorist financing in Southeast Asia. The Terrorism (Suppression of Financing) Act, passed in 2002, criminalizes terrorist financing, although the provisions of the Act are actually much broader. In addition to making it a criminal offense to deal with terrorist property (including financial assets), the Act criminalizes the provision or collection of any property (including financial assets) with the intention that the property be used, or having reasonable grounds to believe that the property will be used, to commit any terrorist act or for various terrorist purposes. The Act also provides that any person in Singapore, and every citizen of Singapore outside Singapore, who has information about any transaction or proposed transaction in respect of terrorist property, or who has information that he/she believes might be of material assistance in preventing a terrorism financing offense, must immediately inform the police. The Act gives the authorities the power to freeze and seize terrorist assets. The Act, which supplements and extends interim legislation enacted in November 2001, took effect January 29,

2003. In January 2003, the Singapore Government released a white paper describing its investigations into the Jemaah Islamiyah (JI) terrorist network. The government is known to have detained five persons in 2003 as suspected terrorists; one of these was later released with restrictions placed on his associations and movements

Separate legislative authority, Section 27A(1)(b) of the Monetary Authority of Singapore Act, as amended in 2002, provides MAS with broad powers to direct financial institutions to comply with international obligations, including UN Security Council Resolutions 1267, 1333, 1373, 1390 and other similar resolutions. Regulations issued by the MAS to implement this authority took effect September 30, 2002. The regulations—the MAS (Anti-Terrorism Measures) Regulations 2002—bar banks and financial institutions from providing resources and services of any kind which will benefit terrorists and from doing “anything that . . . assists or promotes” terrorist financing. Financial institutions must notify the MAS immediately if they have in their possession, custody or control any property belonging to terrorists or any information on transactions involving terrorists’ funds. The regulations apply to all branches and offices of any financial institution incorporated in Singapore, or incorporated outside of Singapore but which are located in Singapore. The regulations include a list of terrorists that is based on the UNSCR 1267 consolidated list. Singapore updates the regulations periodically to include additional names added by the UNSCR 1267 Committee. The most recent update is S 606/2003, the MAS (Anti-Terrorism Measures) Regulations 2003, dated December 22, 2003.

The MAS, on October 9, 2001, issued Circular FSG 48/2001, instructing financial institutions in Singapore to comply with a series of circulars intended to implement UNSCR 1373, including a freeze on assets possessed or controlled by any person known to have committed or attempted to commit acts of terrorism. MAS previously issued Circular FSG 5/2001 to implement UNSCR 1267, and FSG 6/2001 to implement UNSCR 1333. MAS issues revised circulars updating the freeze order after new names were added to the UNSCR 1267 consolidated list, although the process is not always immediate. Singapore officials say they have not identified any assets in Singapore of persons included in the UNSCR 1267 consolidated list.

Alternative remittance systems exist, and are used mainly by the approximately 600,000 foreign workers in Singapore. All remittance agents, formal or informal, must be licensed and are subject to the same laws and regulations, including requirements for record keeping and the filing of suspicious transaction reports. In 2002 the regulations were strengthened. The firms now have to submit a financial statement every three months, and report the largest amount transmitted on a single day. Firms must also answer questions about the way they conduct business and about their overseas partners. Informal networks, such as hawalas, that are not licensed are considered illegal.

Charities in Singapore are subject to extensive government regulation, including close oversight and reporting requirements, and restrictions that limit the amount of funding which can be transferred out of Singapore. A total of 1,564 charities were registered as of December 31, 2002. With a few exceptions, all charities must register with the Government, and must, as part of the registration process, submit governing documents outlining the charity’s objectives and particulars on all trustees. The Commissioner of Charities has the power to investigate charities, including authority to search and seize records, and to restrict the transactions the charity can enter into, suspend charity staff or trustees, and/or establish a scheme for the administration of the charity. Charities must keep detailed accounting records, and retain them for at least seven years.

Under the Charities (Fund-raising Appeals for Foreign Charitable Purposes) Regulations 1994, any charity or person who wishes to conduct or participate in any fund raising for any foreign charitable purpose must apply for a permit. The applicant has to show that at least 80 percent of the funds raised will be used in Singapore, although the Commissioner of Charities has discretion to allow a lower percentage to be applied within Singapore. Permit holders are subject to additional record keeping and

reporting requirements, including details on every item of expenditure disbursed, amounts transmitted to persons outside Singapore, and to whom the money was transmitted. A total of 37 permits were issued in 2002 for fund raising for foreign charitable purposes. There do not appear to be any restrictions or reporting requirements on foreign donations to charities in Singapore.

Singapore is party to the 1988 UN Drug Convention, and in December 2000 signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. In 2003, Singapore ratified the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention on the Marking of Plastic Explosives. It also passed legislation in November 2003 enabling it to comply with the UN Convention on the Suppression of Unlawful Acts Against Maritime Navigation. Singapore is a member of the Financial Action Task Force (FATF), the Asia/Pacific Group on Money Laundering, the Egmont Group, and the Offshore Group of Banking Supervisors. In addition, as of January 2004, the IMF and the World Bank were in the final stages of conducting an assessment of Singapore's anti-money laundering and counterterrorist financing framework.

To bolster law enforcement cooperation and facilitate information exchange, Singapore enacted the Mutual Assistance in Criminal Matters Act (MACMA) in March 2000. The MACMA provides for international cooperation on any of the 182 predicate "serious offenses" listed under the CDSA of 1999. The provisions of the MACMA apply to countries that have concluded treaties, memoranda of understanding, or other agreements with Singapore. In the first ten months of 2003, the STRO received 68 requests for information exchange from overseas law enforcement bodies, compared to 69 such requests received in 2002, and 45 requests in 2001. Singapore and the United States signed the Agreement Concerning the Investigation of Drug Trafficking Offenses and Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking in November 2000, the first agreement concluded pursuant to the MACMA. This agreement, which entered into force in early 2001, facilitates the exchange of banking and corporate information on drug money laundering suspects and targets, including access to bank records. It also entails reciprocal honoring of seizure/forfeiture warrants. This agreement applies only to narcotics cases, and does not cover nonnarcotics-related money laundering, terrorist financing, or financial fraud.

The Terrorism (Suppression of Financing) Act provides for mutual legal assistance in cases where there is no treaty, memorandum (MOU), or other agreement in force between Singapore and another country that is a party to the UN International Convention for the Suppression of the Financing of Terrorism. Singapore's FIU has concluded MOUs concerning cooperation in the exchange of financial intelligence with counterparts in Australia and Belgium, and continues to actively seek MOUs with additional FIUs. In May 2003 the Singapore Government issued a regulation pursuant to the Terrorism Act and the MACMA that will enable it to provide legal assistance to the United States and the United Kingdom in matters related to terrorism financing offenses. The U.S. and Singapore are currently discussing a possible mutual legal assistance treaty. Singapore concluded a mutual legal assistance agreement with Hong Kong in 2003.

Singapore should continue close monitoring of its domestic and offshore financial sectors. As a major financial center, it should also take measures to regulate and monitor large currency movements into and out of the country to ensure that narcotics traffickers, international criminals, terrorists, terrorist organizations or their supporters do not misuse Singapore's financial system. The conclusion of broad mutual legal assistance agreements would further Singapore's ability to work internationally to address these problem. In addition, Singapore may have to amend various laws to ensure consistency with the FATF's revised forty recommendations approved in June 2003.

Slovakia

The geographic, economic, and legal conditions that shape the money laundering environment in Slovakia are typical of those in other Central European transition economies. Slovakia's location along

the major lines of communication connecting Western, Eastern, and Southeastern Europe makes it a transit country for smuggling and trafficking in narcotics, arms, stolen vehicles, and illegal aliens. Organized crime activity and the opportunities to use gray market channels also lead to a favorable money laundering environment. Financial crimes have been quite problematic for Slovak authorities. In fact, the most frequent predicate offenses for money laundering break down as follows: 57 percent fraud, 21 percent tax evasion, and 5 percent embezzlement.

With the law “On Protection Against the Legalization of Proceeds from Criminal Activities,” also known as Act No. 367/2000, Slovakia criminalizes money laundering for all serious crimes and imposes customer identification, record keeping, and suspicious transaction reporting requirements on banks. In January 2001, nonbank financial institutions (casinos, post offices, brokers, stock exchanges, commodity exchanges, asset management companies, insurance companies, real estate companies, tax advisors, auditors, and credit unions), which have been particularly susceptible to laundering, became subject to suspicious transaction reporting requirements. A money laundering conviction does not require a conviction for the predicate offense, and a predicate offense does not have to occur in Slovakia to be considered as such. The failure of an obligated entity to report, as well as tipping off, are criminal offenses.

New anonymous passbook savings accounts are banned as of October 2000. In 2002, a new preventive law came into effect, and legislative amendments abolished all existing bearer passbooks. Owners of anonymous accounts had until December 31, 2003, to close them; however, the law offers a three-year noninterest-bearing grace period to collect money in the accounts before it is confiscated. As of January 1, 2007, bearer passbook accounts will cease to exist. The new law also extended reporting requirements to antique, art, and collectible brokers; dealers in precious metals or stones, or other high-value goods; legal advisors; consultants; securities dealers; foundations; financial managers and consultants; and accounting services. “Obligated persons” are required to identify all customers, including legal entities, if they find that the customers prepared or conducted transactions deemed as suspicious or involving a sum, or related sums exceeding 15,000 euros within a 12-month period. Insurance sellers must identify all clients whose premium exceeds 1,000 euros in a year or whose one-time premium exceeds 2,500 euros. Casinos are obligated to identify all customers. Transactions may be delayed by the entities up to 48 hours, with another 24-hour extension allowed if authorized by the Financial Police. If the suspicion is unfounded, the state assumes the burden of compensation for losses stemming from the delay.

In late 2003, the Slovak cabinet approved a law on measures against entities which acquired property through illegal income; the law is waiting for parliamentary approval. According to the law, an undocumented increase in property exceeding the minimum monthly wage multiplied by 200 is considered to be possibly illegal. Anyone with suspicions of illegally acquired property may report it to the police, who are then obliged to investigate the allegations, ultimately reporting it to the Office of the Attorney General if findings are conclusive.

As recommended in its second-round MONEYVAL evaluation in 2001, the Government of Slovakia (GOS) has replaced basic legislation, and Slovakian legislation is now in full harmony with the Second European Union (EU) Directive. The FATF’s 2002-3 Annual Report stated that the amended legislation provided a “basically sound preventive legal structure.” New and improved customer identification procedures were to be presented to Parliament no later than the end of 2003, and throughout 2003 the banking sector was being evaluated for compliance with laws and regulations. In a controversial move, “suspicious transactions” has been amended to read “unusual business activity.”

Slovakia’s financial intelligence unit (FIU), the OFiS of the Bureau of Financial Police (OFiS-UFP), has jurisdictional responsibilities over money laundering violations. Established in 1996, the OFiS-UFP receives and evaluates suspicious transaction reports (STRs), and collects additional information to establish the suspicion of money laundering. Once enough information has been obtained to warrant

suspicion that a criminal offense has occurred, the OFiS-UFP forwards the case to the State Prosecutor's Office for investigation and prosecution. In 2002, OFiS-UFP received 570 reports alleging unusual transactions totaling SKK 24.1 billion (\$719 million). Over 90 percent (517) of the reports came from banks, 44 from insurance companies, five from the central securities registrar, three from betting houses and one from the post office. Out of the total package, 157 reports were submitted to the OFiS-UFP for further inspection, 93 to police investigators for the purpose of criminal proceeding, 50 to the appropriate tax office and 158 were re-classified as "suspicious business operation." Criminal prosecutions have been proposed in 69 cases; of these, 46 have already been launched. During the first six months of 2003, OFiS-UFP received 213 financial disclosure reports, 90 percent of which came from the banking sector. (The GOS attributes a low level of reporting from some sectors to lack of supervision.) Of these, twelve were passed on for further investigation. Approximately seven percent of those reports led to criminal prosecutions. In 2002, the OFiS-UFP conducted 25 on-site inspections of obliged entities as follows: six insurance companies, 11 leasing companies, four foreign exchange houses, two securities brokers and two real-estate brokerages. According to available information, 17 inspections have been completed without penalties, three are yet unfinished and in five cases inspectors levied fines (cumulatively amounting to SKK 700,000, or \$20,895).

Recently, the FIU was divided into three departments. A receptor branch receives and disseminates reports from the obligated entities. A supervisory branch ensures the cooperation of the reporting entities as well as international cooperation. The analytical branch does the actual analysis. OFiS-UFP analysts participate regularly in international and domestic fora related to combating money laundering. The year 2003 saw no major changes to the FIU, which is still seeking to increase its administrative capacity. However, the newly created Bureau for the Fight Against Corruption has siphoned some staff from the FIU.

The GOS ratified the UN International Convention on the Suppression of the Financing of Terrorism on September 13, 2002. The Convention has been incorporated into amendments of the Bank Act, Penal Code, and Act No. 367/2000. However, Slovakia elected to pursue several optional terms of the convention that were fully incorporated in March 2003. All competent authorities in the Slovak Republic have full power to freeze or confiscate terrorist assets in accordance with UNSCR 1373. The GOS agreed to freeze all accounts owned by entities on the UN or U.S. lists immediately. No terrorist finance related accounts have been frozen or seized in Slovakia, but were a terrorism-related account to be identified, the Financial Police would hold any related financial transaction for up to 48 hours, and then gather evidence to freeze the account and seize any assets.

Slovakia is a party to the European Convention on Mutual Legal Assistance, and became a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime in 2001. Slovakia is a party to the 1988 UN Drug Convention, and in December 2003 it signed the UN Convention Against Corruption and ratified the UN Convention against Transnational Organized Crime. Slovakia became a member of the Organization for Economic Cooperation and Development (OECD) in December 2000, thereby expanding its opportunities for multilateral engagement. Slovakia is a member of the Council of Europe (COE) and participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). Slovakia sends experts to conduct mutual evaluations on fellow member countries; it also underwent mutual evaluations by this group in 1998 and 2001.

The OFiS-UFP is a member of the Egmont Group. Slovakia has MOUs with the FIUs of Slovenia, Belgium, Poland, and the Czech Republic, and a letter of exchange with the FIU of Slovenia. The OFiS-UFP is the responsible authority for international exchange of information regarding money laundering under the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

Slovakia should continue to improve its anti-money laundering regime. Continued implementation of the provisions of Slovakia's new anti-money laundering legislation will give the Slovak financial system greater protection by helping it prevent and detect money laundering in all financial sectors. Slovakia should also improve supervision of some nonbank sectors to ensure reporting requirements are followed. Slovakia should provide adequate resources to assure its FIU, law enforcement and prosecutorial agencies are adequately funded and trained to effectively perform their various responsibilities. Slovakia should criminalize terrorist financing.

Slovenia

While not a major money laundering country, Slovenia's economic stability and location on the Balkan drug route offer attractive opportunities for money laundering. Narcotics trafficking, especially heroin via the "Balkan route" smuggled by mainly Albanian and Serbian nationals, is a growing problem and the main source of illegal proceeds. Other significant sources of illegal proceeds are fraud, trafficking in weapons, illegal immigration, and currency and securities counterfeiting, as well as extraterritorial offenses such as tax evasion, tax and VAT fraud, and corruption. Organized crime is believed to be involved in both predicate crimes and laundering operations. Money laundering often tends to be undertaken by citizens of the other former state socialist countries, using nonresident accounts, and occurs through the banking system, foreign exchange houses, real estate transactions, and cross-border currency transport.

Slovenia's Law on the Prevention of Money Laundering was enacted in 1994 and amended in 2001. The law criminalizes money laundering and requires all financial institutions, casinos, and legal and natural persons to report suspicious transactions and currency transactions above 5 million Slovenian tolar (approximately \$24,000.) Records must be retained for a minimum of five years. Financial supervisory bodies include the Bank of Slovenia, the Securities Market Agency, the Insurance Supervisory Agency, and the Office for Gaming Supervision. The Bank of Slovenia has supervisory power over bureaux de change, and in February 2003 issued a handbook for those bodies complete with reporting requirements, auditing procedures, and indicators.

Slovenia's financial intelligence unit, the Office for Money Laundering Prevention (OMLP), was established in 1995 and has a staff of 17. It is a member of the Egmont Group. In 2002, OMLP received 92 cases of suspected money laundering and temporarily seized nearly 310 million tolar. In its eight years of operations, OMLP has received 831 suspicious cases and closed 732. Foreign nationals were involved in nearly half of the cases. A special financial crime division was established within the general police directorate in 2000. This unit is in charge of conducting preliminary investigations into money laundering cases and other economic crimes. However, the backlog of cases has become problematic in that about half of all cases fell outside of the statute of limitations before they could be tried. Of the procedures that made it to court in time, 90 percent ended in conviction. Law enforcement authorities, prosecutors, and judges all suffer from a lack of training and experience with regard to pursuing financial crime. Despite this, though, four money laundering cases were brought to fruition by July 2003. Of the four, one was acquitted, and the three convictions are currently on appeal. In two of these cases assets were confiscated.

In October 2001, the Slovenian Parliament passed an anti-money laundering law that updates the original 1994 law by, among other provisions, expanding the OMLP's sources of available financial information, extending OMLP's authority to temporarily halt suspect transactions, and requiring mandatory client identification for transactions exceeding 3 million Slovenian tolar (approximately \$14,400). December 2001 saw the passage of a new law that increases the power of supervisory authorities to prohibit the establishment of new bearer passbook accounts, as well as phases out already existing bearer passbook accounts. Further amendments to the law, which extend reporting obligations to lawyers, law firms, notaries, auctioneers, art dealers, gaming houses, and lottery

concessions, were passed and entered into force in July 2002. Additional identification requirements were also implemented, most notably beneficial owner identification in every case.

The 2002 amendments also gave OMLP more power and latitude in opening cases and sharing information. The amount of time during which transactions could be held was increased from 48 to 72 hours, and record keeping was extended from five to ten years. Another new change is the penal requirement of five years' imprisonment for money laundering. Negligent money laundering is criminalized, but there has never been a conviction for that. Slovenian legislation is now harmonized with the provisions outlined in the Second EU Directive.

Additional legislation was proposed in 2003. Laws concerning foreign currency exchange and banking were at the Parliament level; these laws would make changes to requirements for exchange offices and supervision. In addition, Parliament also received a draft Law on Criminal Procedure. In mid-2003, OMLP drafted a law on asset sharing in conjunction with the Ministries of Justice and Interior.

The 1902 extradition treaty between the U.S. and the Kingdom of Serbia remains in force between the U.S. and Slovenia. Slovenia is actively involved in regional efforts to combat money laundering and terrorism financing, working overall throughout the Balkans and Eastern Europe, especially with Serbia, Montenegro, Ukraine, and Russia. As a EU accession country slated to join in May 2004, Slovenia has been working to expand cooperation. It has run a regional counternarcotics conference with Croatian counterparts, and hosted a regional anti-money laundering conference for eight of its Balkan neighbors.

Slovenia is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and has undergone a mutual evaluation by the Committee, as well as lending its own experts to evaluate other member countries. Slovenia also actively participates in other programs combating money laundering and terrorism financing run through the EU, the Council of Europe, Interpol and the United Nations. Slovenia is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, and ratified the Civil Law Convention on Corruption in July 2003. Slovenia is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism. In July 2003 Slovenia signed the European Convention on the Suppression of Terrorism.

Slovenia should pass specific antiterrorist financing legislation and should continue to work with its law enforcement and judicial authorities to increase the levels of action and experience in pursuing financial crime.

Solomon Islands

The Solomon Islands is not a regional financial center. The Islands' banking system is small. The country has not criminalized money laundering. According to a report by the Solomon Islands to the UN Counter Terrorism Committee, in 2003 the Solomon Islands introduced a draft Bill on Money Laundering. The draft Bill provides a mechanism that prevents the movement of funds for terrorist purposes and enhances the exchange of financial intelligence with other countries.

The Solomon Islands is not a party to the 1988 UN Drug Convention.

The Solomon Islands should pass anti-money laundering and counter terrorism financing legislation that conforms to international standards. The Solomon Islands should become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

South Africa

South Africa's position as the major financial center in the region, its relatively sophisticated banking and financial sector, and its large cash-based market, all make it a very attractive target for transnational and domestic crime syndicates. Nigerian, Pakistani, and Indian drug traffickers, Chinese Triads, and Russian Mafia have all been identified as operating in South Africa along with native South African criminal groups. Although the links between different types of crime have been observed throughout the region, money laundering is primarily related to narcotics trade. The other dominating types of crimes related to money laundering are: fraud, theft, corruption, currency speculation, illicit dealings in precious metals and diamonds, human trafficking, and smuggling. South Africa is not an offshore financial center.

The Proceeds of Crime Act, No. 76 of 1996, criminalizes money laundering for all serious crimes. This Act was superseded by the Prevention of Organized Crime Act (No. 121 of 1998), which confirmed the criminal character of money laundering, mandated the reporting of suspicious transactions, and provided a "safe harbor" for good faith compliance. Violation of this Act, carries a fine of up to R 100 million or imprisonment for up to 30 years. Subsequent regulations direct that the reports be sent to the Commercial Crime Unit of the South African Police Service. Both of these Acts contain criminal and civil forfeiture provisions.

In November 2001 President Mbeki signed the Financial Intelligence Centre Act (FICA) into law. The FICA established both the Financial Intelligence Centre (FIC) and the Money Laundering Advisory Council to advise the Minister of Finance on policies and measures to combat money laundering. The mandate of the Financial Intelligence Center (FIC) is to coordinate policy and efforts to counter money laundering activities. The FIC similarly acts as a centralized repository of information and statistics on money laundering. The FICA requires a wide range of financial institutions and businesses to identify customers, maintain records of transactions for at least five years, appoint compliance officers to train employees to comply with the law, and report transactions of a suspicious or unusual nature. Such businesses include companies and businesses considered particularly vulnerable to money laundering activities such as banks, life insurance companies, foreign exchange dealers, casinos, and real estate agents. If the FIC has reasonable grounds to suspect that a transaction involves the proceeds of criminal activities, the FIC will forward this information to the investigative and prosecutorial authorities. If there is suspicion of terrorist financing, that information is to be forwarded to the National Intelligence Service. The FIC began operating in February 2003. In July 2003 the FIC was admitted as a member of the Egmont Group of financial intelligence units.

Because of the cash-driven nature of the South African economy, alternative remittance systems that bypass the formal financial sector exist. Currently, there is no legal obligation requiring alternative remittance systems to report cash transactions.

The House of Assembly passed a bill proposed by the South African Law Commission in 2001, criminalizing specifically the financing of terrorism, on November 21, 2003, under the title "The Constitutional Democracy Against Terrorism and Related Activities Act of 2004." According to this act, any person who engages in a terrorist activity is guilty of the offense of terrorism. There is a special provision criminalizing the financing of terrorism. This act will complement and amend the FICA of 2001. The FIC will combat terrorist financing as well as money laundering, based on this new act. The Act also calls for the jurisdiction's authority to identify, freeze and seize money laundering related assets.

As of December 2003, 30 money laundering cases are under investigation and only a very few actual cases have been prosecuted for money laundering or terrorist financing.

In June 2003, South Africa became the first African nation to be admitted into the Financial Action Task Force thus strengthening its money laundering control capacity. South Africa is also an active

member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) having signed the memorandum of understanding in 2003.

The GOSA is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. South Africa has signed, but not yet ratified, the UN Convention against Transnational Organized Crime.

In 2003, South Africa improved and strengthened its anti-money laundering regime and its overall legal capacity to combat money laundering in all its forms, and has made new efforts to prosecute a number of money launderers.

Spain

Money laundered in Spain is primarily from the proceeds of the Colombian cocaine trade, although money laundered through other Latin American countries also plays a role. Hashish proceeds from Morocco enter Spain as well as some heroin money from Turkish smugglers. There is also some concern about the black market smuggling of goods to avoid taxation, especially tobacco and electronics from Gibraltar. The majority of laundered money enters as bulk cash via individuals carrying cash in their luggage or hidden on their bodies when arriving at international airports; containers loaded with currency entering the larger ports (such as Algeciras); and money smuggled by small craft along the coastline. Money also enters and leaves Spain through the commercial banking system and informal nonbank outlets (such as “Locutorios”), which make small international transfers for the immigrant community. Although little of the money laundered in Spain is believed to be used for terrorist financing, money from the extortion of businesses in the Basque region is moved through the financial system and used to finance the Basque group ETA. Spain is aware of the problem; however the money is difficult to track.

The Government of Spain (GOS) remains committed to combating narcotics trafficking, terrorism, and financial crimes, and continues to work hard to tighten financial controls. The criminalization of money laundering was added to the penal code in 1988 when laundering the proceeds from narcotics trafficking was made a criminal offense. In 1995 the law was expanded to cover all serious crimes that required a prison sentence greater than three years. All forms of money laundering were made financial crimes in amendments to the code on November 25, 2003, which will take effect on October 1, 2004.

The penal code can also apply to individuals in financial firms if their institutions have been used for financial crimes. An amendment to the penal code in 1991 made such persons culpable for both fraudulent acts and negligence connected with money laundering.

Businesses and financial service suppliers operating in Spain or targeting Spanish markets are subject to a new law, Ley de Servicios de la Sociedad de Informacion y de Comercio Electronico (LSSICE), that came into force on October 12, 2002, for Internet marketing and distribution. The new law requires businesses to register their domain names, company registry, physical address, and other company details. Financial sector businesses such as online banks must still send written contracts to new customers for signature and obtain physical proof of their identity, in order to comply with existing banking regulations.

Royal Decree 998/2003 of July 5, 2003 modified the structure of the Ministry of Interior to facilitate more active combating of drug trafficking. This law creates an Advisory Committee on Observation that will attempt to follow the use of technologies by criminal organizations and money launderers and take measures to ensure that Spanish law enforcement authorities are able to meet the new challenges.

Specific measures to prevent money laundering were written to regulate the legal entities in the financial sector and individuals moving large sums of cash, in December 1993 (Law No. 19/1993), as

an expansion to the criminal code which previously applied only to physical persons. The regulations for enactment were established by Royal Decree 925/1995, which set the standards for regulation of the financial system. The regulations were amended in 2003 and cover money laundering linked to illicit drugs, terrorism, and organized crime. The financial sector is required to identify customers, keep records of transactions, and report suspicious financial transactions. The money laundering law applies to most entities active in the financial system, including banks, mutual savings associations, credit companies, insurance companies, financial advisers, brokerage and securities firms, postal services, currency exchange outlets, casinos, and individuals and unofficial financial institutions exchanging or transmitting money (alternative remittance systems). The 2003 amendments add lawyers and notaries as covered entities. Previously, notaries and lawyers were required to report suspicious cases, but now they are considered part of the financial system that is under the supervision of appropriate regulators.

Law 19/2003 obligates financial institutions to make monthly reports on large transactions. Banks are required to report all international transfers greater than 30,000 euros. The law also requires the declaration and reporting of internal transfers of funds greater than 80,500 euros.

In addition to suspicious transactions, individuals traveling internationally are required to report the importation or exportation of currency greater than 6,000 euros. Previously, the Spanish authorities could only keep 12 percent if they uncovered illegal activity, but had to return the remainder with a Bank of Spain check, which effectively laundered the money. Law 19/2003 increases the seizure to 100 percent if illegal activity under financial crimes ordinances can be proven. Spanish authorities claim they have seen a drop in cash carriers since the enactment in July 2003. For cases where the money can not be connected to criminal activity, but it also has not been declared, the authorities may keep between 25 and 100 percent, depending on the amount of the currency being carried.

The Commission for the Prevention of Money Laundering and Financial Crimes (CPBC) coordinates the fight against money laundering in Spain. The Secretary of State for Economy heads the commission and all of the agencies involved in the prevention of money laundering participate. The representatives include the National Drug Plan Office, the Ministry of Economy, the Federal Prosecutors (Fiscalia), Customs, the Spanish National Police, the Guardia Civil, CNMV (equivalent to the SEC), the Treasury, the Bank of Spain, and the Director General of Insurance and Pension Funds. Any member of the Commission may request an investigation, should suspicious activity be brought to his or her attention.

The CPBC delegates responsibility to two additional organizations. The first is a secretariat in the Treasury, located in the Ministry of Economy. Following investigation and a guilty verdict by a court, this regulating body carries out penalties. Sanctions can include closure, fines, account freezes, or seizures of assets. Changes in Law 19/2003 now allow seizures of assets of third parties in criminal transactions, and a seizure of real estate in an amount equivalent to the illegal profit. One weakness that remains in financial sanctions is that the joint owner may access joint accounts if he or she can show financial need.

The second organization is the Executive Service of the Commission for the Prevention of Money Laundering (SEPBLAC), which serves as Spain's financial intelligence unit. SEPBLAC receives and analyzes suspicious activity reports (SARs) and currency transaction reports. SEPBLAC has the primary responsibility for any investigation in money laundering cases and directly supervises the anti-money laundering procedures of banks and financial institutions. Incriminating information is turned over to the Federal Prosecutors for prosecution. Spanish banks are required by law to maintain fiscal information for five years and mercantile records for six years.

The Fund of Seized Goods of Narcotics Traffickers receives seized assets. This agency was established under the National Drug Plan. The proceeds from the funds are divided, with half going to

drug treatment programs and half to a foundation that supports the officers fighting narcotics trafficking.

Terrorist financing issues are governed by a separate code of law and commission, the Commission of Vigilance of Terrorist Finance Activities (CVAFT). This commission was created under Law 12/2003 on the Prevention and Blocking of the Financing of Terrorism. The commission is headed by the Ministry of Interior and includes representatives from the Fiscalia and Ministries of Justice and Economy. Currently, only the head of CVAFT can request information in terrorist financing cases, so other members must rely on the commission head to begin an investigation.

Crimes of terrorism are defined in Article 571 of the Penal Code, and penalties are set forth in Articles 572 and 574. Sanctions range from ten to thirty years' imprisonment with longer terms if the terrorist actions were directed against government officials. The Spanish are more active in freezing terrorist accounts, than drug money laundering accounts. Their ability to freeze accounts in the most recent law is more aggressive than that of most of their European counterparts. Though many laws are transposed from EU directives, Law 12/2003 goes beyond EU requirements.

All legal charities are placed on a register maintained by the Ministry of Justice. Responsibility for policing registered charities lies with the Ministry of Public Administration. If the charity fails to comply with the requirements, sanctions or other criminal charges may be levied.

Spain is a member of the FATF, and co-chairs the FATF terrorist finance working group. Spain is a participating and cooperating nation to the South American Financial Action Task Force (GAFISUD), and a cooperating and supporting nation to the Caribbean Financial Action Task Force (CFATF). Spain is a major provider of counterterrorism assistance. The GOS ratified the UN Convention against Transnational Organized Crime on March 2, 2002, and the UN International Convention for the Suppression of the Financing of Terrorism on April 9, 2002. Spain is also a party to the 1988 UN Drug Convention. SEPBLAC is a member of the Egmont Group.

The GOS has signed criminal mutual legal assistance agreements with Argentina, Australia, Canada, Chile, the Dominican Republic, Mexico, Morocco, Uruguay, and the United States. Spain's Mutual Legal Assistance Treaty with the United States has been in effect since 1993. Spain also has entered into bilateral agreements for cooperation and information exchange on money laundering issues with Bolivia, Chile, El Salvador, France, Israel, Italy, Malta, Mexico, Panama, Portugal, Russia, Turkey, Venezuela, Uruguay, and the United States. Spain actively collaborates with Europol, supplying and exchanging information on terrorist groups. In 2003, U.S. law enforcement authorities cooperated with the GOS in an investigation that resulted in the seizure of over \$10 million in cash, jewelry, planes, and real estate.

Seizures of assets involving more than one country and the division of the assets depend on the relationship with the third country. EU working groups will determine how to divide the proceeds for member countries. Outside of the EU, bilateral commissions are formed with countries that are members of FATF, FATF-like bodies and the Egmont Group, to deal with the division of seized assets. With other countries, negotiations are conducted on an ad hoc basis.

Spain should continue the strong enforcement of its anti-money laundering program and its leadership in the international arena. It should consider whether additional measures are required to address possible money laundering in the stock market to ensure that the sector is not used for financial crimes.

Sri Lanka

Sri Lanka is neither an important regional financial center nor a preferred center for money laundering. Money laundering currently is not a criminal offense. There are strict bank secrecy laws, under which

the Government of Sri Lanka is required to obtain a court order to obtain banking information of bank customers. In a bid to tackle money laundering and terrorist financing in the absence of a specific legal framework, in December 2001, the Central Bank introduced regulations on customer due diligence. These regulations apply to commercial banks and licensed specialized banks coming under the Central Bank. The Government is in the process of finalizing draft legislation to deal with money laundering. It is believed there will be three separate laws: 1. A financial transaction reporting law modeled on those in the Commonwealth; 2. A law on countering terrorist financing based on UN and FATF models; and 3. A law to criminalize proceeds from crimes. Currently, financial transactions relating to terrorism and narcotics are illegal under Central Bank regulations and banking laws.

Many areas of concern exist in Sri Lanka's anti-money laundering efforts. The Central Bank continues to allow the operation of bearer certificates of deposits. In July 2003, in order to check money laundering through bearer certificates, the Central Bank required banks to maintain a record of people purchasing these certificates. The Government offered a tax amnesty to Sri Lankans in 2003. Under the amnesty, individuals and companies could declare previously undisclosed wealth accrued from any source. The amnesty granted immunity from taxes and investigations. The amnesty was aimed at widening the tax base. Casinos are another area of concern as there is no law to regulate their operations. Sri Lanka has also become a transit point for illegal migration of Sri Lankans and other Asian nationals to Europe and the Gulf.

There is an indigenous alternative remittance system in the form of informal money transfer systems. Sri Lankan migrant workers, mainly in the Middle East, use a hawala-like system to remit their earnings. Various payments out of Sri Lanka also use this system. Sri Lankan commercial banks are increasing their presence and services in the Middle East in order to cater to this clientele.

Sri Lanka is not considered an offshore financial center. Offshore banking units are allowed to operate as a part of a commercial bank operating in the country in order to facilitate trade finance. They are subject to Central Bank supervision. Bearer shares are not permitted for banks and companies.

Regulations under the United Nations Act No. 45 of 1968 provide for freezing and forfeiture of assets of financiers of terrorism. There is no specific provision in law to freeze and forfeit narcotics related assets. Trafficking, possessing, importing or exporting of narcotics is punishable by death or life imprisonment under the Poisons, Opium and Dangerous Drugs Ordinance (OPDDO). Draft amendments to OPDDO and new money laundering legislation are expected to include asset forfeiture and seizure provisions for narcotics related crimes and money laundering.

Terrorist financing is an offense punishable by imprisonment for a period of five to ten years. The Central Bank of Sri Lanka has circulated the list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list with instructions to identify, freeze and seize terrorist assets. To date no such assets have been identified. Sri Lanka is a party to the UN International Convention for the Suppression of the Financing of Terrorism and to the 1988 UN Drug Convention. Sri Lanka has signed but not ratified the UN Convention against Transnational Organized Crime.

Sri Lanka should initiate a comprehensive anti-money laundering program that has as its foundation anti-money laundering and antiterrorist financing laws. The proceeds of all crime should be included as predicate offenses for money laundering. The practice of bearer certificates of deposit should be terminated. There should be a formalized system of reporting suspicious transactions from financial institutions to a Financial Intelligence Unit (FIU). Casinos should also be made subject to financial intelligence reporting to the FIU. Sri Lanka should devote adequate resources to train police and customs officials to recognize and investigate different forms of money laundering, including alternative remittance systems.

St. Kitts and Nevis

The Government of St. Kitts and Nevis (GOSKN) is a federation composed of two islands in the Eastern Caribbean, but each island has the authority to organize its own financial structure. The federation is at major risk for corruption and money laundering due to the high volume of narcotics-trafficking activity through and around the islands and the presence of known traffickers on the islands. An inadequately regulated economic citizenship program adds to the problem.

Most of the offshore financial activity in the federation is concentrated in Nevis in which there is one offshore bank (a wholly owned subsidiary of a domestic bank), approximately 13,800 international business companies (IBCs), and 950 trusts. The Nevis domestic structure consists of five domestic banks, four domestic insurance companies (all of which are subsidiaries of St. Kitts companies), and one money remitter. There are also 65 trust and company service providers. In St. Kitts, there are four domestic banks, two credit unions, four domestic insurance companies, two money remitters, and 15 company service providers. There are also four trusts and 450 exempt companies. A regional stock exchange, common to the members of the Organization of Eastern Caribbean States (OECS) and supervised by a regional regulator, is located in St. Kitts. There are two casinos in St. Kitts, and three casino licenses are pending. Applicants may apply as an IBC for an Internet gaming license, but none have been issued, despite the fact the Internet Gaming Commission indicates that St. Kitts and Nevis (SKN) has 42 Internet gaming sites.

The Eastern Caribbean Central Bank has direct responsibility for regulating and supervising the offshore bank in Nevis, as it does for the domestic sector in the entire St. Kitts and Nevis (SKN), and for making recommendations regarding approval of offshore bank licenses. The St. Kitts and Nevis Financial Services Commission, with regulators on both islands, regulates nonbank financial institutions for anti-money laundering compliance.

In June 2000, the Financial Action Task Force (FATF) placed St. Kitts and Nevis on the list of noncooperative countries and territories in the fight against money laundering (NCCT). The FATF in its report cited several concerns surrounding the anti-money laundering regime of SKN. Among the problems identified by FATF were the narrow definition of money laundering as a punishable offense, the absence of mandatory suspicious transaction reporting, and the lack of effective supervision of the Nevis offshore sector. In July 2000, the U.S. Treasury Department issued an advisory to U.S. financial institutions, emphasizing the need for enhanced scrutiny of certain transactions and banking relationships in St. Kitts and Nevis to ensure that appropriate measures are taken to minimize risk for money laundering. As a result of the legislative changes addressed below as well as the responsiveness of the GOSKN to requests for mutual legal assistance and other financial sector regulatory inquiries, the FATF, with certain ongoing follow-up conditions, removed the GOSKN from the NCCT list in June 2002. The U.S. Treasury Department removed its Financial Advisory in August 2002. In June 2003, the FATF stated that the GOSKN had adequately addressed all of its previously identified deficiencies and would no longer require monitoring by the FATF.

The Financial Intelligence Unit Act No. 15 of 2000 authorizes the creation of the Financial Intelligence Unit (FIU). The FIU began operations in 2001 and has a director, deputy director, and four police officers. The FIU receives, collects, and investigate suspicious activity reports (SARs). The FIU is also charged with liaising with foreign jurisdictions. By November 2003, the FIU had received 77 SARs. During its first two years of operation the FIU received over 100 SARs and froze over \$1.6 million. The Proceeds of Crime Act No. 16 of 2000 criminalizes money laundering for serious offenses (defined to include more than drug offenses) and imposes penalties ranging from imprisonment to monetary fines. The Act also overrides secrecy provisions that may have constituted obstacles to the access of administrative and judicial authorities to information with respect to account holders or beneficial owners. Other measures designed to remedy shortcomings in SKN's anti-money laundering regime include the Financial Services Commission Act No. 17 of 2000, the Nevis Offshore

Banking (Amendment) Ordinance No. 3 of 2000, the Anti-Money Laundering Regulations No. 15 of 2001, the Companies (Amendment) Act No. 14 of 2001, the Anti-Money Laundering (Amendment) Regulations No. 36 of 2001, the Nevis Business Corporation (Amendment) Ordinance No. 3 of 2001, and the Nevis Offshore Banking (Amendment) Ordinance No. 4 of 2001.

The GOSKN also issued regulations requiring financial institutions to identify their customers, to maintain a record of transactions, to report suspicious transactions to the FIU, and to establish anti-money laundering training programs. The Financial Services Commission has issued guidance notes on the prevention of money laundering pursuant to the Anti-Money Laundering Regulations. The Commission's Regulator is authorized to carry out anti-money laundering examinations. The GOSKN has separated the offshore marketing and regulatory functions. In particular, an offshore Marketing and Development Department, separate from the Financial Services Commission, was established in April 2001. Legislation requires certain identifying information to be maintained about bearer certificates, including the name and address of the bearer of the certificate, as well as its beneficial owner. In addition to these measures, Nevis issued regulations aimed at facilitating the identification of beneficial owners of corporations and corporate shareholders.

Financial Services (Exchange of Information) Regulations were promulgated in 2002. These regulations define the parameters for the exchange of information between domestic regulatory agencies and foreign regulatory agencies. Financial services officials in SKN have been seeking to educate relevant stakeholders as to their responsibilities related to anti-money laundering, e.g., using radio, television, newspapers and seminars. The GOSKN encouraged the founding of an association of compliance officers within relevant financial institutions and provided training in anti-money laundering to government financial services personnel. In 2003, the Nevis island administration announced plans to strengthen regulatory oversight of service providers.

St. Kitts and Nevis enacted the Anti-Terrorism Act No. 21, effective November 27, 2002. Sections 12 and 15 of the Act criminalize terrorist financing. The Act implements various UN Conventions against terrorism. The GOSKN has some existing controls that apply to alternative remittance systems, but has undertaken no initiatives that apply directly to the potential terrorist misuse of charitable and nonprofit entities. St. Kitts and Nevis circulates lists of terrorists and terrorist entities to all financial institutions. To date, no accounts associated with terrorists or terrorist entities have been found in SKN.

St. Kitts and Nevis is a member of the Caribbean Financial Action Task Force (CFATF) and the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). A mutual legal assistance treaty between St. Kitts and Nevis and the United States entered into force in early 2000. St. Kitts and Nevis is a party to the 1988 UN Drug Convention and in November 2001 signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. The GOSKN became a party to the UN International Convention for the Suppression of the Financing of Terrorism on November 16, 2001.

Notwithstanding its recent progress, SKN remains vulnerable to money laundering and other financial crimes. St. Kitts and Nevis should continue to devote sufficient resources to effectively implement its anti-money laundering regime. Specifically, the GOSKN also needs to determine the volume of Internet gaming sites present on the islands. Oversight of these entities is crucial as they are vulnerable to abuse by criminal and terrorist groups. Additionally, the GOSKN should adequately oversee, or should curtail its economic citizenship program.

St. Lucia

St. Lucia has developed an offshore financial service center that could potentially make the island more vulnerable to money laundering and other financial crimes. The Government of St. Lucia (GOSL) also is considering the establishment of gaming enterprises.

Money Laundering and Financial Crimes

Currently, St. Lucia has two offshore banks, 1,052 international business companies, 20 international trusts, 12 international insurance companies, 15 registered agents and trustees (service providers), two money remitters, two mutual fund administrators and four domestic banks. The GOSL has been cooperative with the USG in financial crime investigations.

The 1993 Proceeds of Crime Act criminalizes money laundering with respect to narcotics. The Proceeds of Crime Act also provides for a voluntary system of reporting account information to the police or prosecutor when such information may be relevant to an investigation or prosecution. In addition, the Act requires financial institutions to retain information on new accounts and details of transactions for seven years.

Many of the 1993 Proceeds of Crime Act provisions are superseded by the 1999 Money Laundering (Prevention) Act, which criminalizes the laundering of proceeds with respect to 15 prescribed offenses, including narcotics trafficking, corruption, fraud, terrorism, gambling and robbery. The Money Laundering (Prevention) Act mandates suspicious transaction reporting requirements and imposes record keeping requirements. In addition, the Money Laundering (Prevention) Act imposes a duty on financial institutions to take “reasonable measures” to establish the identity of customers, and requires accounts to be maintained in the true name of the holder. The Act also now requires an institution to take reasonable measures to identify the underlying beneficial owner when an agent, trustee or nominee operates an account. These obligations apply to domestic and offshore financial institutions, including credit unions, trust companies, and insurance companies. In April 2000, the Financial Services Supervision Unit issued detailed guidance notes, entitled “Minimum Due Diligence Checks, to be conducted by Registered Agents and Trustees.”

Pursuant to the Money Laundering (Prevention) Act, the Money Laundering (Prevention) Authority was established in early 2000. The Authority consists of five persons “who have sound knowledge of the law, banking or finance.” The Authority’s functions include receipt of suspicious transactions reports, subsequent investigation of the transactions, dissemination of information within (e.g., to the Director of Public Prosecutions) or outside of St. Lucia, and monitoring of compliance with the law. The Money Laundering (Prevention) Act imposes a duty on the Authority to cooperate with competent foreign authorities. Assistance includes the provision of documents, giving of testimony, undertaking of examinations, execution of search and seizure orders, and the provision of information and evidentiary items. The Authority has a number of regulatory powers, including the right to enter the premises of a financial institution during normal working hours to inspect transaction records or copy relevant documentation, issue guidelines to financial institutions, and instruct a financial institution to facilitate an investigation by the Authority.

In 1999, the GOSL also enacted a comprehensive inventory of offshore legislation, consisting of the International Business Companies (IBC) Act, the Registered Agent and Trustee Licensing Act, the International Trusts Act, the International Insurance Act, the Mutual Funds Act and the International Banks Act. An IBC may be incorporated under the IBC Act. Only a person licensed under the Registered Agent and Trustee Licensing Act as a licensee may apply to the Registrar of IBC’s to incorporate and register a company as an IBC. The registration process involves the Registered Agent submitting to the registrar the memorandum and articles of the company, payment of the prescribed fee and the Registrar’s determination of compliance with the requirements of the Act. IBCs can be registered online through the GOSL’s Pinnacle web page. IBCs intending to engage in banking, insurance or mutual funds business may not be registered without the approval of the Minister responsible for international financial services. An IBC may be struck off the register on the grounds of carrying on business against the public interest.

The Financial Intelligence Authority Act No. 17 of 2002 authorizes the establishment of a Financial Intelligence Unit (FIU) for St. Lucia, which became operational in October 2003. Some of the functions of the Money Laundering (Prevention) Authority have been transferred to the new Financial

Intelligence Unit (FIU). The FIU will receive suspicious transaction reports and will be able to compel the production of information necessary to investigate possible offenses under the 1993 Proceeds of Crime Act and the 1999 Money Laundering (Prevention) Act. Failure to provide information to the FIU is a crime, punishable by a fine or up to ten years imprisonment. The Financial Intelligence Authority Act permits the sharing of information obtained by the FIU with foreign FIUs. The Caribbean Anti-Money Laundering Program (CALP), which is funded jointly by the United States, the United Kingdom and the European Union, has trained St. Lucia's FIU personnel.

In September 2003, legislation was adopted merging the Money Laundering (Prevention) Authority with the FIU. The legislation also extends anti-money laundering compliance requirements to credit unions, money remitters and pawnbrokers, as well as strengthens criminal penalties for money laundering. There have been no money laundering convictions to date in St. Lucia.

The GOSL established the Committee on Financial Services in 2001. The Committee, which meets monthly, is designed to safeguard St. Lucia's financial services sector. The Committee is composed of the Minister of Finance, the Attorney General, the Solicitor General, the Director of Public Prosecutions, the Director of Financial Services, the Registrar of Business Companies, the Commissioner of Police, the Deputy Permanent Secretary of the Ministry of Commerce, the police officer in charge of Special Branch, the Comptroller of Inland Revenue and others. The GOSL announced in 2003 its intention to form an integrated regulatory unit to supervise the onshore and offshore financial institutions the GOSL currently regulates. The Eastern Caribbean Central Bank regulates St. Lucia's domestic banking sector.

Anti-terrorism and counterterrorist financing legislation is pending before the St. Lucia Parliament. The GOSL has not signed the UN International Convention for the Suppression of the Financing of Terrorism. In 2002, St. Lucia signed the Inter-American Convention Against Terrorism, which includes counterterrorist financing provisions. St. Lucia circulates lists of terrorists and terrorist entities to all financial institutions. To date, no accounts associated with terrorists or terrorist entities have been found in St. Lucia. The GOSL has not taken any specific initiatives focused on the misuse of charitable and nonprofit entities.

As a member of the Caribbean Financial Action Task Force (CFATF), St. Lucia underwent a first mutual evaluation immediately prior to the establishment of its offshore sector. St. Lucia underwent its Second Round evaluation in September 2003. St. Lucia is a party to the 1988 UN Drug Convention and a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. In February 2000, St. Lucia and the United States brought into force a Mutual Legal Assistance Treaty. On September 26, 2001, St. Lucia signed the UN Convention against Transnational Organized Crime. St. Lucia has a Tax Information Exchange Agreement with the United States.

The GOSL should ratify the UN International Convention for the Suppression of the Financing of Terrorism and adopt antiterrorism financing legislation. St. Lucia should continue to enhance and implement its money laundering legislation and programs.

St. Vincent and the Grenadines

Until its government fully implements the financial sector and anti-money laundering laws it has enacted, St. Vincent and the Grenadines (SVG) will remain vulnerable to money laundering and other financial crimes, as a result of the rapid expansion and inadequate regulation of its offshore sector in recent years.

SVG's offshore sector includes ten offshore banks (down from 42 in 2000), 6,342 international business companies (IBCs) (down from over 11,000 in 2000), four offshore insurance companies, nine mutual funds, and 394 international trusts. SVG's domestic sector comprises five commercial banks,

one development bank, two savings and loans, one building society, three credit unions, and one money remitter. There are also 21 insurance companies. The Eastern Caribbean Central Bank (ECCB) supervises SVG's five domestic banks. Beginning in October 2001 with an administrative agreement, and finalized in the International Banks (Amendment) Act No. 30 of 2002, the Government of SVG (GOSVG) has given the ECCB increasing authority to review and make recommendations regarding approval of offshore bank license applications and to directly supervise SVG's offshore banks in cooperation with the GOSVG's Offshore Finance Authority (OFA). The agreement includes provisions for joint on-site inspections to evaluate the financial soundness and anti-money laundering programs of offshore banks. The OFA alone continues to supervise and regulate the other offshore sector entities. The GOSVG has strengthened the structure and staffing of the OFA.

In June 2000, the Financial Action Task Force (FATF) placed SVG on the list of noncooperative countries and territories in the fight against money laundering (NCCT). The FATF in its report cited several concerns, including the fact that SVG had not put in place anti-money laundering regulations or guidelines with respect to offshore financial institutions. The FATF also cited obstacles to international cooperation, and rudimentary licensing and registration requirements for financial institutions in SVG. In July 2000, the U.S. Treasury Department issued an advisory to U.S. financial institutions, warning them to give enhanced scrutiny to all financial transactions originating in or routed to or through SVG, or involving entities organized or domiciled, or persons maintaining accounts in, SVG. In June 2003, the FATF recognized that GOSVG had sufficiently addressed deficiencies identified by the FATF through enactment and implementation of appropriate legal reforms, and SVG was removed from the NCCT list. The FATF encouraged GOSVG to consider tightening provisions relating to the granting of exemptions from customer identification requirements. In July 2003, the U.S. Treasury Department withdrew its advisory against the GOSVG.

Since July 2000, the GOSVG has passed substantial legislation, primarily the International Banks (Amendment) Act No. 7 of 2000 that deals with the authorization and regulation requirements for offshore banks as well as with the rules regarding the transfer of shares and beneficial interest. The GOSVG also enacted the International Banks (Amendment) Act of October 2000, which enables the Offshore Finance Inspector to have access to the name or title of an account of a customer and any other confidential information about the customer that is in the possession of a licensee. The GOSVG prepared a further amended International Banks Act with a view to improving licensing procedures and better regulating the offshore banking sector.

The GOSVG enacted the International Business Companies Amendment Act No. 26 of 2002, which became effective on May 27, 2002, to immobilize and register bearer shares. The GOSVG also revoked the Confidentiality Act and passed the Exchange of Information Act No. 29 of 2002 to authorize and facilitate the exchange of information, particularly among regulatory bodies. In April 2001, the GOSVG revoked its economic citizenship program, which provided the legal basis to sell SVG citizenship and passports, although no passports were reported to have been issued under the program.

SVG enacted the Proceeds of Crime and Money Laundering (Prevention) Act in December 2001 and the Proceeds of Crime (Money Laundering) Regulations in January 2002. Subsequent amendments further strengthened provisions of the Act and the Regulations. Among other measures, this Act criminalizes money laundering and imposes on financial institutions and regulated businesses a requirement to report suspicious transactions suspected of being related to money laundering or the proceeds of crime. The related regulations establish mandatory record keeping rules and limited customer identification/verification requirements.

The Financial Intelligence Unit Act No. 38 of 2001 established the Financial Intelligence Unit (FIU) that began operation in May 2002. The FIU Act, 2001 allows for the exchange of information with foreign FIUs. An amendment to the FIU Act permits the sharing of information even at the

investigative or intelligence stage. The FIU became a member of the Egmont Group in June 2003. By November 2003, the FIU had received 283 suspicious activity reports.

There were no money laundering convictions, but the GOSVG has frozen approximately \$1.5 million and confiscated approximately \$40,000. SVG officials also cooperated with a U.S. investigation of a major suspected money launderer in 2002. The GOSVG in 2003 reintroduced a customs declaration form to be completed and signed by incoming travelers. Incoming travelers are required to declare currency over approximately \$3,800.

The GOSVG enacted the United Nations Terrorism Measures Act No. 34, effective August 2, 2002. Sections 3 and 4 of the Act criminalize terrorist financing. The GOSVG is a party to the UN International Convention for the Suppression of the Financing of Terrorism and is deemed to be partially compliant. The GOSVG has not undertaken any specific initiatives focused on the misuse of charitable and nonprofit entities. The GOSVG circulates lists of terrorists and terrorist entities to all financial institutions in St. Vincent and the Grenadines. To date, no accounts associated with terrorists have been found in SVG.

The GOSVG is a member of the Caribbean Financial Action Task Force (CFATF), and underwent its Second Round mutual evaluation in November 2002. In addition, SVG is a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). SVG is a party to the 1988 UN Drug Convention and acceded to the Inter-American Convention Against Corruption in 2001. SVG signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. An updated extradition treaty and a Mutual Legal Assistance Treaty between the United States and SVG entered into force in September 1999.

The GOSVG should address all remaining concerns raised by the international community concerning its anti-money laundering regime, including in the areas of customer identification, physical presence, money remitters, outstanding bearer shares and money laundering prosecutions. The GOSVG should continue to provide training to its regulatory, law enforcement and FIU personnel on money laundering operations and investigations and strengthen the FIU's relationship with its foreign counterparts. The GOSVG also should ensure that it properly supervises the offshore sector.

Suriname

Suriname is not a regional financial center. Narcotics-related money laundering occurs primarily through unregulated private sector activities, specifically casinos, gold mining and car dealerships. Narcotics-related money laundering is closely linked to transnational criminal activity related to the transshipment of Colombian cocaine and is believed to occur through both the nonbanking financial system (i.e., money exchange businesses or cambios) and through a variety of other means including, but not limited to, the sale of gold purchased with illicit money and the manipulation of commercial and state controlled bank accounts. The money laundering proceeds are believed to be controlled by both local drug-trafficking organizations and organized crime.

Suriname's overall anti-money laundering regime remains weak. The Government of Suriname (GOS) is attempting to implement a package of anti-money laundering legislation passed in 2002 based on recommendations made by the Caribbean Financial Action Task Force (CFATF). This legislation addresses multiple issues including (a) criminalizing money laundering, (b) establishing a financial intelligence unit (FIU) to track and report on unusual and suspicious financial transactions, and (c) requiring financial service providers to store information on clients for seven years and to confirm the identities of clients, individual or corporate, before completing requested financial services. The legislation includes a due diligence section making individual bankers responsible if their institution is laundering money, and ensures the protection of bankers and others with respect to their cooperation

with law enforcement officials. The law, "Reporting of Unusual Transactions" was enacted in September 2002 and entered into force in March 2003. This law requires financial institutions, other intermediaries and natural legal persons who conduct financial services to report suspicious financial transactions to the FIU. In addition, there is an amendment to the criminal code allowing authorities to confiscate illegally obtained proceeds and assets obtained partly or completely through criminal offenses.

The Central Bank issued guidelines for the prevention of money laundering in 1996 that contain a definition of a suspicious transaction as any transaction that deviates from the usual account and customer activities and that are not "normal" daily banking business. These guidelines are not mandatory.

The FIU opened an office in early 2003 and is receiving extensive training. The FIU, which falls under the auspices of the Attorney General's office, is tasked with identifying, recording and reporting the identity of customers engaging in suspicious financial transactions. After an initial rough start, the head of the FIU resigned effective January 2004 after less than six months in office. No replacement has been announced.

Suriname's financial regime will be challenged in early 2004 by a planned currency change which will drop three zeros from the currency and change the name from the Surinamese Guilder to the Surinamese Dollar. Oversight of this transition will provide a significant test for the newly established FIU to prevent money launderers from exploiting the change in currency. The Central Bank, however, has anticipated this problem and will require that suspicious transactions be reported/investigated. Any currency conversions after an initial three-month grace period must be converted at the Central Bank with an explanation of why the currency was not converted earlier.

The GOS has not criminalized terrorist financing, however, GOS officials are working with the Caribbean Anti-Money Laundering Program to draft legislation requiring transparency in the financial sector that would contain specific provisions for terrorist financing.

The GOS has an agreement with the Netherlands on extradition and legal assistance with regard to criminal matters. Suriname also has bilateral treaties and cooperation agreements with the United States, on narcotics trafficking, and with Colombia, France and Netherlands Antilles on transnational organized crime. Suriname is a member of the CFATF and the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). Suriname is party to the 1988 UN Drug Convention and signed the Inter American Convention against Terrorism in June 2002.

Suriname should continue its efforts to fully implement its anti-money laundering legislation, particularly the establishment of the FIU, and train its personnel. The GOS should criminalize terrorist financing and become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Swaziland

Swaziland is a growing regional financial center. International narcotics trafficking continues to grow in Swaziland, increasing the threat of money laundering. Swaziland's proximity to South Africa, lack of effective counternarcotics legislation, limited enforcement resources, relatively open society, and developed economic infrastructure make it attractive for trafficking organizations and increase the risk for money laundering.

The Money Laundering Act of 2001 criminalizes money laundering for specified predicate offenses, including narcotics trafficking, kidnapping, counterfeiting, extortion, fraud, and arms-trafficking. The Act establishes a currency reporting requirement, requires banks to report suspicious transactions to

the Central Bank, and provides conditions when assets may be frozen and forfeited. It also requires banks to retain records for five years to improve the ability to trace suspicious transactions and patterns. The penalty for money laundering is six years imprisonment, a fine amounting to roughly \$3,500, or both. The Act also allows for providing assistance to foreign countries that have entered into mutual assistance treaties with the Government of Swaziland.

As of December 2003, the Central Bank received fewer than 10 reports of suspicious transactions. The police bear responsibility for investigating such cases, but no investigations have taken place. The police would also be responsible for seizing any assets related to money laundering, but no seizures have taken place under the Money Laundering Act of 2001. To assist the banking community with tracking suspicious transactions, the Central Bank distributed anti-money laundering guidelines to all banks in late 2002.

Swaziland is party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. Swaziland has signed, but not yet ratified, the UN International Convention against Transnational Organized Crime. Swaziland is also a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. In August 2002, Swaziland hosted the ESAAMLG plenary and Council of Ministers meeting. Swaziland served as President of ESAAMLG from August 2002 to August 2003.

Swaziland should criminalize terrorist financing. Swaziland should also establish a financial intelligence unit capable of sharing information with foreign law enforcement and regulatory officials.

Sweden

Sweden does not appear to have a significant money laundering problem. Swedish anti-money laundering legislation includes all serious crimes. Sweden's money laundering controls allow Sweden to fulfill the recommendations of the Hague Forfeiture Convention.

Swedish law obligates banks, credit market companies, securities businesses, exchange offices, remittance dealers, insurance brokers, life insurance companies and casinos to report suspicious activity to the police financial intelligence unit (FIU). The law also requires financial institutions, insurance companies, currency exchange houses, and money transfer companies to verify customer identification, inquire into a transaction's background, and verify identities for each transaction, particularly in the case of new customers and involving amounts above SEK 110,000 (\$12,300). Swedish law does not allow individual officers of obligated institutions to be penalized for noncompliance; however, the Swedish Supervisory Authority has the ability to sanction noncompliant institutions. The FIU is entitled to demand customer information from dealers in antiques, jewelry, and art; companies buying and selling new and used vehicles; and firms dealing with gambling and the sale of lottery tickets. Swedish law also provides for the seizure of assets derived from drug-related activity.

Sweden's FIU received 4,155 suspicious transaction reports in 2001, a 60 percent increase from 2000 due to the implementation of the European Union's Anti-Money Laundering Directive through Swedish law, which required bureaux de change to report suspicious activity. In 2002, the FIU received 8,008 suspicious transaction reports, and 10,000 reports in 2003.

Sweden ratified the International Convention for the Suppression of the Financing of Terrorism on June 6th 2002, and on July 1st 2002, a new act on penalties for financing serious crimes entered into force. According to the act, it is punishable to collect, provide or receive money or other funds with the intention that they should be used, or in the knowledge that they are to be used, in order to commit serious crimes that are classified as terrorism in international conventions. Attempts to commit such crimes are also punishable. Banks and financial institutions are obliged to observe and report to the police transactions that are suspected to comprise funds that will be used to finance serious crimes.

Freezing of assets based on UN Security Council Resolutions is carried out by implementation of EC law.

Sweden is in the process of implementing the second EU Directive on Money Laundering, which expands the reporting requirements to occupational groups such as lawyers, accountants, real estate agents, tax-advisers, and dealers in high value items. The proposal is out for public review, and the new law will come into effect by January 1, 2005.

Sweden has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision." Sweden is a member of the Financial Action Task Force and the Council of Europe. Its FIU is a member of the Egmont Group. Sweden is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. It is also a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

Sweden should continue to expand its anti-money laundering-antiterrorist financing regime. Sweden should adopt reporting requirements for the cross-border transportation of currency or monetary instruments. Sweden should ensure legislation is enacted to extend suspicious transaction reporting requirements to intermediaries, such as attorneys, accountants and financial advisors.

Switzerland

Switzerland is a major international financial center, with some 370 banks maintaining headquarters there. In addition, approximately 12,000 to 15,000 fiduciaries function as nonbank financial institutions. Narcotics-related money laundering proceeds are largely controlled by foreign drug-trafficking organizations. Authorities suspect that Switzerland is vulnerable at the layering and integration stages. Switzerland's central geographic location; relative political, social, and monetary stability; wide range and sophistication of available financial services; and long tradition of bank secrecy are all factors that make Switzerland a major international financial center. These same factors make Switzerland attractive to potential money launderers. However, Swiss authorities are aware of this and are sensitive to the size of the Swiss private banking industry relative to the size of the economy, and waive bank secrecy rules in the prosecution of money laundering and other criminal cases. An estimated \$2.9 trillion is represented by deposits in Swiss institutions, with foreigners accounting for over half of the input into the financial system; this amount is 12 times the GDP of the country.

Reporting indicates that criminals attempt to launder proceeds in Switzerland from a wide range of illegal activities conducted worldwide, particularly narcotics trafficking and corruption. Switzerland's extensive market in fine arts is also used to launder money. Although both Swiss and foreign individuals or entities conduct money laundering activities in Switzerland, narcotics-related money laundering operations are largely controlled by foreign narcotics-trafficking organizations, often from the Balkans or Eastern Europe. For example, some of the money generated by Albanian narcotics-trafficking rings in Switzerland goes to armed Albanian extremists in the Balkans.

Switzerland ranks fifth in the highly profitable art work trading market, and exported \$877 million worth of art work worldwide in 2003. Generating about \$200 billion a year in turnover, the market offers lucrative opportunities for organized crime to transfer stolen art or to use art to launder criminal funds. The U.S. is by far Switzerland's most important trading partner, and purchased \$442 million of "Swiss" works of art in 2003. The Swiss art market is especially attractive for unethical transactions, since art works, which may have been smuggled into Switzerland, can legally be re-exported as genuine Swiss art work after five years. Swiss officials, concerned about the possible abuse of the Swiss art dealer market, drafted new legislative changes to enlarge the scope of existing anti-money laundering legislation to include art dealers. Additionally, on June 17, 2003, the parliament adopted a

bill on the transfer of cultural goods, which regulates the return of looted cultural objects. The new legislation, which is expected to come into force by mid-2004, extends the timeframe from the current five years to meet the UN International Standards of 30 years as defined in the 1970 UNESCO Convention. It also will enable police forces to search bonded warehouses and art galleries.

Money laundering is a criminal offense. Switzerland has significant anti-money laundering legislation in place, making banks and other financial intermediaries subject to strict Know Your Customer and reporting requirements. Switzerland has also implemented legislation for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets.

The current money laundering laws and regulations have been extended to nonbank financial institutions. Consequently, all nonbank financial intermediaries are required to either join an accredited self-regulatory organization (SRO), or come under the direct supervision of the Money Laundering Control Authority (MLCA) of the Federal Finance Administration. The MLCA was formed in 1998 to oversee anti-money laundering laws in the nonbanking sector. The SROs must be independent of the management of the intermediaries they supervise and must enforce compliance with due diligence obligations. Noncompliance can result in a fine or a revoked license. About 7,000 fiduciaries operate in this previously unregulated arena. The MLCA is not afraid to take action against financial intermediaries: during the summer of 2002, the MLCA shut down three financial management companies, because they were operating illegally and failed to comply with anti-money laundering regulations. Reporting regulations on international money transactions, applicable to money transmitters in particular, have recently been tightened as well.

In January 2002, the Government Efficiency Bill took effect. Under this bill, the Chief Public Prosecutor became vested with the power to prosecute crimes provided by Article 340bis of the Swiss Penal Code; money laundering falls under these provisions. Formerly, the individual cantons were charged with investigating money laundering offenses on their own. Additional legislation, effective January 1, 2002, increased the effectiveness of the prosecution of organized crime, money laundering, corruption, and other white-collar crime, by increasing the personnel and financing of the criminal police section of the federal police office. The law confers on the federal police and Attorney General's office the authority to take over cases that have international dimensions, involve several cantons, or which deal with money laundering, organized crime, corruption, and white collar crime.

In December 2002, the new money laundering ordinances of the Swiss Federal Banking Commission were adopted; these became effective on July 1, 2003. These new regulations, aimed at the banking and securities industries, codify a risk-based approach to suspicious transaction and client identification, and install a global Know Your Customer (KYC) risk management program for all banks, including those with branches and subsidiaries abroad. In the case of higher-risk business relationships, additional investigation by the financial intermediary is required. The changes also require increased due diligence in the cases of politically exposed persons by ensuring that decisions to commence relationships with such persons be undertaken by the senior executive body of a firm. Legislation that aligns the Swiss supervisory arrangements with the Basel Committee's "Core Principles for Effective Banking Supervision" is contained in the Swiss Money Laundering Act.

The new ordinances also present new rules against terrorism financing, stating that instruments currently used to prevent money laundering are also applicable to the prevention of terrorism financing; if a financial intermediary investigates the background of an unusual or suspicious transaction, and linkages with a terrorist organization are revealed, the institution must report the matter to the Swiss financial intelligence unit (FIU) immediately. Additionally, the ordinance mandates computer-based transaction monitoring systems for all but the smallest financial intermediaries. Consistent with Financial Action Task Force (FATF) standards, all cross-border wire transfers must now contain details about the funds remitters. The provisions of the ordinance also address Swiss supervision of subsidiaries belonging to a consolidated group of financial intermediaries

(for which information channels must be established), and all provisions apply to correspondent banking relationships as well. Shell banks—banks with no physical presence at their place of incorporation—may not maintain any correspondent bank accounts.

In October 2003, the Swiss cabinet also mandated an interdepartmental working group led by the Ministry of Finance in order to comply with the new set of FATF Forty Recommendations adopted in June 2003. In December 2003, the MLCA effected a new money laundering ordinance which implements the new FATF Forty Recommendations. FATF is expected to review implementation by early 2005.

In July 2003, the government-sponsored Zimmerli Commission, charged by the Finance Ministry with examining reform of finance market regulators, presented 46 recommendations. Most notably, the Committee recommended merging the Federal Banking Commission and the Federal Office for Private Insurance, or the banking and insurance sectors, into a single, integrated financial market supervision body, possibly known as FINMA. These proposals are expected to be drafted into legislation and adopted by the Swiss parliament in 2006; the changes that would need to be made are extremely far-reaching.

Auditing firms, which in the past enjoyed preferential treatment compared to their clients, have also been put under scrutiny. The Swiss Ministry of Justice has drafted a bill on auditing firms oversight, which is expected to be introduced to parliament during 2004.

The Money Laundering Reporting Office Switzerland (MROS) is Switzerland's FIU. All financial intermediaries (banks, insurers, fund managers, currency exchange houses, securities brokers, etc.) are legally obliged to establish customer identity when forming a business relationship. They also must notify the MROS, or a government authorized supervisory body, if a transaction appears suspicious. If financial institutions determine that assets were derived from criminal activity, the assets must be reported to MROS and frozen within five days until a prosecutor decides whether to take further action. MROS's staff, particularly the nonbanking sector staff, increased in 2002, so the FIU staff, now eight, has doubled since its establishment in 1998. In June 2003, MROS released figures for the previous year: From 2002 into 2003, money laundering cases rose 56 percent over 2001 figures, with more than 650 reports of suspicious transactions (STRs) worth approximately \$500 million. For the first time, the majority of reports came from the nonbank sector, probably due to the stricter reporting regulations directed at nonbank financial intermediaries. However, while the percentage of STRs coming from banks has decreased, the number of STRs from the banks has actually continued to increase.

Switzerland's banking industry offers the same account services for both residents and nonresidents. These can be opened through various intermediaries who advertise their services. As part of Switzerland's international financial services, banks offer certain well-regulated offshore services, including permitting nonresidents to form offshore companies to conduct business, which can be used for tax reduction purposes.

The Swiss Commercial Law does not recognize any offshore mechanism per se and its provisions apply equally to residents and nonresidents. The stock company and the limited liability company are two standard forms of incorporation offered by Swiss Commercial Law. The financial intermediary is required to verify the identity of the beneficial owner of the stock company and must also be informed of any change regarding the beneficial owner. Bearer shares may be issued by stock companies but not by limited liability companies.

Swiss casino operators have joined counterparts from Greece, Austria, Finland, Spain, Portugal, and the United Kingdom to form a new Casino Operators' Association. Among the stated priorities for the group are addressing issues surrounding money laundering and how to stop it, and responsible gaming practices.

The European Union (EU) finance ministers issued a warning to Switzerland in 2002, saying that Switzerland's lack of action was hampering the global crackdown on money laundering and other financial crimes, and threatened sanctions if Switzerland did not change its banking secrecy laws. However, current Swiss law provides for no banking secrecy for suspected fraud, money laundering, or terrorist-related funds, despite Switzerland's steadfast position on maintaining banking secrecy in the face of tax evasion not related to other crimes.

The Government of Switzerland has made it a key foreign policy goal to correct the country's image as a haven for illicit banking services. The Swiss believe that their system of self-regulation, which incorporates a "culture of cooperation" between regulators and banks, equals or exceeds that of other countries. The primary interest of the Swiss system is to avert bad risks by countering them at the account-opening phase, where due diligence and KYC address the issues, rather than relying on an early-warning system keeping up with all filed transactions. The Convention on Due Diligence is very comprehensive, requiring the identification of the client and the beneficial owner, who needs to be a physical person. Because of the due diligence approach the Swiss have taken, there are fewer STRs filed than in other countries, but the ones that are filed lead to the opening of criminal investigations 80 percent of the time. In January 2003, Switzerland won a battle when the EU backed away from demands that Switzerland scrap banking secrecy. Despite the measures that Switzerland has taken, it is likely to endure more criticism from other countries for its continued banking secrecy laws and its refusal to look upon tax evasion as a crime.

The Oversight Commission of the Swiss Bankers Association fined Credit Suisse for inadequate due diligence in connection with a total of \$214 million deposited in the bank by former Nigerian dictator Sani Abacha. Swiss press reports put the fine at \$500,000 (SFr. 750,000 at the time), making it the largest fine ever imposed by the Commission. The recipient of the fine will be the International Red Cross Committee, a Swiss organization.

If financial institutions determine that assets were derived from criminal activity, the assets must be frozen immediately until a prosecutor decides on further action. Under Swiss law, suspect assets may be frozen for up to five days while a prosecutor investigates the suspicious activity. Switzerland cooperates with the United States to trace and seize assets, and has shared a large amount of funds seized with the U.S. Government (USG) and other governments. The Government of Switzerland has worked closely with the USG on numerous money laundering cases. The banking community cooperates with enforcement efforts. In addition, legislation permits "spontaneous transmittal"—allowing the Swiss investigating magistrate to signal to foreign law enforcement authorities the existence of evidence in Switzerland. The Swiss used this provision in 2001 to signal Peru that they had uncovered accounts linked to former Peruvian presidential advisor Vladimiro Montesinos. On March 31, 2003, the Swiss Federal Court rejected an appeal by Raul Salinas, brother of a former president of Mexico and main suspect in a major money laundering affair, to release millions of dollars blocked on 10 different Swiss bank accounts.

During 2002, the Swiss Federal Council presented a bill to the Nationalrat, Switzerland's lower house, that addressed a number of terrorism issues surrounding ratification of the UN terrorism conventions. This bill included an independent provision on terrorist financing that introduces criminal liability for legal persons involved in terrorism financing. The Swiss House was scheduled to consider it in the first half of 2003. The newly amended Swiss penal code makes terrorism financing a predicate offense for money laundering. Changes in the Criminal Code in 2003 also make terrorism financing a predicate offense in money laundering, and expand the scope of application to legal persons.

Since September 11, 2001, Swiss authorities have been alerting Swiss banks and nonbank financial intermediaries to check their records and accounts against lists of persons and entities with links to terrorism. The accounts of these individuals and entities are to be reported to the Ministry of Justice as suspicious transactions. Based on the "State Security" clause of the Swiss Constitution, the authorities

have ordered banks and other financial institutions to freeze assets of organizations and individuals designated by the UN 1267 Sanctions Committee. In the 2002 reporting period, MROS received reports of 15 cases possibly linked to the funding of terrorism. The total amount of money involved was \$1.03 million. All the reports involved individuals and institutions appearing on the U.S. Government's lists. The 15 reports were transmitted to the Swiss federal prosecutor in Berne.

Along with U.S. Government and UN lists, the Swiss Economic and Finance Ministries have drawn up their own list of approximately 44 individuals and entities connected with international terrorism or its financing. Swiss authorities have thus far blocked about 82 accounts totaling \$25 million from individuals or companies linked to Usama bin Ladin and al-Qaida under UN resolutions. The Swiss Federal Prosecutor also froze separately 41 accounts representing about \$25 million, on the grounds that they were related to terrorism financing, but the extent to which these funds overlap with the UN lists has yet to be determined. In January 2003, the Swiss Ministry of Justice handed over banking information to U.S. authorities, following a legal assistance request issued in April 2002. The request related to a bank transfer of \$1.4 million, which took place between June 2000 and September 2001, and was addressed to the Benevolence International Foundation, a Chicago-based Islamic foundation with alleged ties to al-Qaida and other terrorist groups. The transfer originated from a Swiss bank account whose account holder was a company located in the Virgin Islands. The firm had initially lodged a complaint against this decision to the supreme Swiss federal court but was turned down in November 2002.

Switzerland is a signatory of, but has not yet ratified, the UN Convention against Transnational Organized Crime. Switzerland has ratified the Council of Europe Convention on the Laundering, Search, Seizure, and Confiscation of Proceeds from Crime. In September 2003, Switzerland ratified the UN International Convention for the Suppression of the Financing of Terrorism, and in December 2003 signed the UN Convention Against Corruption. To date, Switzerland has not ratified the 1988 UN Drug Convention.

Swiss authorities cooperate with counterpart bodies from other countries. MROS cooperation with other FIUs has increased by more than 20 percent in 2003. Requests for cooperation with Liechtenstein, Switzerland's closest neighbor both culturally and geographically, have tripled. Switzerland has a Mutual Legal Assistance Treaty in place with the United States, and Swiss law allows authorities to furnish information to U.S. regulatory agencies, provided it is kept confidential and used for supervisory purposes. The U.S.-Swiss extradition treaty permits extradition for any unlawful act punishable by imprisonment in both countries. Switzerland is a member of the Financial Action Task Force and the Egmont Group. Switzerland is a member of the Basel Committee on Banking Supervision, which established the first international code of conduct for banks.

Switzerland should extend its anti-money laundering program to include dealers in high-end goods. Switzerland can also continue to improve on its anti-money laundering regime, as it has been doing, and address deficiencies that it finds, as well as continuing to work toward full implementation of its anti-money laundering/antiterrorist financing regime.

Syria

The U.S. Department of State had designated Syria as a State Sponsor of Terrorism. Given its extremely underdeveloped banking sector, Syria is not a likely center for money laundering via the formal financial sector. Since private banks were nationalized in the early 1960s, Syria's entire financial system has been owned and operated by the state, although in early 2004 a limited number of private banks received permission to begin operating in Syria. The existing public banks are inefficient and highly regulated, and focus almost exclusively on financing public enterprises. The Government of Syria (SARG) heavily restricts foreign currency flows out of the country, which contributes to the use of alternative systems of moving money or transferring value. Syrian businessmen also use banks

in neighboring Lebanon and Jordan to receive a full range of banking services. The private sector routinely conducts foreign currency transactions to finance imports, generally by using letters of credit from Lebanon and Europe. Due to foreign exchange controls, the private sector also has restricted access to foreign currency. Illicit proceeds from the narcotics trade may flow through Syria, but it is generally believed they are moved to Lebanon for laundering purposes. As a result, the primary money laundering vulnerability in Syria is not necessarily through financial institutions but via the use of alternative remittance systems such as hawala, trade-based money laundering, and currency smuggling. Such money laundering methodologies are often used to finance terrorism throughout the region and elsewhere. Although a positive development in terms of modernization of the financial sector, the opening of private banks in Syria makes the banking system increasingly vulnerable to money laundering until such time as the SARG implements measures to facilitate its oversight of financial transactions.

Due to distrust of public banks, currency restrictions, and displeasure with the official exchange rate, most Syrians prefer to utilize informal banking systems to transfer currency into Syria, sometimes by physically moving cash via Syrian bus and shipping companies with offices in the region. Relatives, friends and colleagues often provide a similar service using foreign bank accounts, particularly in Lebanon. For example, a Syrian businessman with excess Syrian pounds can pay for his expatriate cousin's new Damascus apartment in local currency, and the cousin then transfers a commensurate amount of hard currency to a designated overseas account. In instances where no relative or friend is available and/or the amount to be transferred is too high, a few money changers, well known to the business community and operating with tacit SARG approval, also provide a means of depositing hard currency in overseas accounts. These mechanisms are a form of hawala.

The government-controlled banking system in Syria consists of the Central Bank of Syria and five public banks, each specializing in one aspect of economic activity: the Commercial Bank of Syria, the Agricultural Cooperative Bank, the Industrial Bank, the Real Estate Bank, and the People's Credit Bank. These banks have in the past employed a rigid interest rate structure that discourages savings deposits, particularly during periods of inflation. Only the Commercial Bank of Syria has been permitted to provide commercial banking services until January 2004 when the first private banks opened. The Commercial Bank, as the sole legal trader of foreign currencies, also effectively has controlled all foreign trade and all foreign currency transactions. In addition to monopolizing the exchange of foreign currencies, the SARG maintains one of the last remaining fixed, multiple exchange rate systems in the world, employing three different rates depending on the nature of the transaction, although it is expected that the SARG may take steps toward eliminating the multiple exchange rate system in 2004. Until that is changed, however, this inefficient system also undoubtedly contributes to alternative methods of transferring value outside the state controlled banking system. There are reports that such transactions occur with the tacit approval, if not involvement, of SARG officials. A large percentage of Lebanon's banking services involve Syrian accounts.

In April 2001 Law No. 28 legalized private banking and Law No. 29 established rules on bank secrecy. The first private banks opened in January 2004, but the services they provide are limited under current governmental regulations. Clients may open savings and checking accounts, for example, but deposits to foreign currency accounts can be made by wire transfer only, and not by cash. Much still needs to be done to fundamentally restructure the banking sector, particularly in terms of either suspending or amending existing regulations that prohibit a newly-licensed private bank from operating fully. The SARG continues to work on detailed regulations that will govern the operation of private banks.

In September 2003, Syria passed Legislative Decree No. 59, creating an Anti-money Laundering Commission. While this is an important movement in principle toward addressing vulnerabilities in the banking sector, particularly the new vulnerabilities which can arise with the opening of private

banks, it is not yet clear what relationship the commission will have with financial institutions or whether the commission will hold effective investigative powers.

Syria is a party to the 1988 UN Drug Convention. Syria should become a party to the UN International Convention for the Suppression of the Financing of Terrorism, and should immediately stop all support of terrorist organizations.

As a first step in crafting a viable anti-money laundering program, Syria should approve comprehensive anti-money laundering and antiterrorism finance legislation that adheres to world standards. Syria should then take meaningful steps to enforce the law and follow-up rules and regulations governing the banking sector.

Taiwan

Taiwan's modern financial sector and its role as a hub for international trade make it attractive to money laundering. Its location astride international shipping lanes makes it vulnerable to transnational crimes such as narcotics trafficking and smuggling. The use of alternative remittance systems or "underground banking" is a money laundering vulnerability. There is a significant volume of informal financial activity through unregulated nonbank channels. According to suspicious activity reports (SARs) filed by financial institutions on Taiwan, the predicate crimes linked to SARs include: financial crimes, corruption, narcotics, and other general crimes, in that order.

Taiwan's anti-money laundering legislation is embodied in the Money Laundering Control Act (MLCA) of April 23, 1997. Its major provisions include a list of predicate offenses for money laundering, customer identification and record keeping requirements, disclosure of suspicious transactions, international cooperation, and the creation of a financial intelligence unit, the Money Laundering Prevention Center (MLPC).

The Legislative Yuan amended the MLCA in 2003, to expand the list of predicate crimes for money laundering, widen the range of institutions subject to suspicious transaction reporting, and mandate compulsory reporting of significant currency transactions of over New Taiwan (NT)\$1 million to the MLPC. As a result of the amendments, the list of institutions subject to reporting requirements was expanded to include casinos, automobile dealers, jewelers, boat and plane dealers, real estate brokers, credit card firms, insurance companies and securities dealers, as well as traditional financial institutions. In addition, two new articles were added to the MLCA, granting prosecutors and judges the power to freeze assets related to suspicious transactions, and giving law enforcement more powers related to asset forfeiture and the sharing of confiscated assets.

In terms of reporting requirements, financial institutions are required to identify, record, and report the identities of customers engaging in significant or suspicious transactions. Reports of suspicious transactions are required at the time of the transaction. Institutions are also required to maintain records necessary to reconstruct significant transactions for an adequate amount of time. Bank secrecy laws are overridden by anti-money laundering legislation, allowing the MLPC to access all relevant financial account information. Financial institutions are held responsible if they do not report suspicious transactions.

In 2003, the MLPC received 1,485 reports of possible money laundering activity, of which 1,057 cases were closed, 168 involved probable crimes, and 260 remain under review. The MLPC referred 76 cases to other departments of the Ministry of Justice Investigation Bureau (MJIB) for review, and referred 92 cases to the police.

Individuals are required to report currency transported into or out of Taiwan in excess of NT\$60,000 (approximately \$1,765), \$5,000, or \$5,000 worth of foreign currency. Starting in March 2004, over 6,000 Chinese renminbi (\$725) must also be reported. When foreign currency in excess of

NT\$500,000 (approximately \$14,700) is brought into or out of Taiwan, the bank customer is required to report the transfer to the Central Bank, though there is no requirement for Central Bank approval prior to the transaction. Prior approval is required, however, for exchanges between New Taiwan dollars and foreign exchange when the amount exceeds \$5 million for an individual resident and \$50 million for a corporate entity.

The authorities on Taiwan are actively involved in countering the financing of terrorism. As of December 2003, a new “Counter-Terrorism Action Law” (CTAL) was drafted and was under consideration by the legislature. The new law would explicitly designate the financing of terrorism as a major crime. Under the proposed CTAL, the National Police Administration, the MJIB and the Coast Guard would be able to seize terrorist assets even without a criminal case in Taiwan. Also, in emergency situations, law enforcement agencies would be able to freeze assets for three days without a court order. Assets and income obtained from terrorist-related crimes could also be permanently confiscated under the CTAL, unless the assets could be identified as belonging to victims of the crimes.

The Bureau of Monetary Affairs (BOMA) has circulated to all domestic and foreign financial institutions in Taiwan the names of individuals and entities included on the UN 1267 Sanctions Committee’s consolidated list. In accordance with UN Security Council Resolution 1373, the MLCA was amended to allow the freezing of accounts suspected of being linked to terrorism. No targeted assets have been identified to date. According to the MLPC, in 2003, financial institutions in Taiwan reported six possible cases of terrorist financing. However, in all six cases, the suspects were determined not to be terrorists.

Alternative remittance systems, or underground banks, are considered to be operating in violation of Banking Law Article 29. Authorities on Taiwan consider these entities to be unregulated financial institutions. Foreign labor employment brokers are authorized to use banks to remit income earned by foreign workers to their home countries. These remittances are not regulated or reported. Thus, money laundering regulations are not imposed on these foreign labor employment brokers. However, if the brokers accept money in Taiwan dollars for delivery overseas in another currency, they are violating Taiwan law. It is also illegal for small shops to accept money in Taiwan dollars and remit it overseas. Violators are subject to a maximum of three years in prison, and/or forfeiture of the remittance and/or a fine equal to the remittance amount. Authorities on Taiwan do not believe that charitable and nonprofit organizations in Taiwan are being used as conduits for the financing of terrorism.

A mutual legal assistance agreement between the American Institute in Taiwan (AIT) and the Taipei Economic and Cultural Representative Office in the United States (TECRO) entered into force in March 2002. It provides a basis for the law enforcement agencies of the territories represented by AIT and TECRO to cooperate in investigations and prosecutions for narcotics trafficking, money laundering (including the financing of terrorism), and other financial crimes.

Although Taiwan is not a UN member and cannot be a party to the 1988 UN Drug Convention, the authorities on Taiwan have passed and implemented laws in compliance with the goals and objectives of the Convention. Similarly, Taiwan cannot be a party to the UN International Convention for the Suppression of the Financing of Terrorism, as a nonmember of the United Nations, but it has agreed unilaterally to abide by its provisions. Taiwan is a founding member of the Asia/Pacific Group on Money Laundering (APG) and actively participates in the Group’s meetings. The MLPC is a member of the Egmont Group.

Over the past five years, Taiwan has created and implemented an anti-money laundering regime that comports with international standards. The MLCA amendments of 2003 address a number of vulnerabilities, especially in the area of asset forfeiture. The authorities on Taiwan should continue to strengthen the existing anti-money laundering regime as they implement the new measures. The

authorities on Taiwan should also enact legislation that would promulgate regulations regarding alternate remittance systems.

Tajikistan

Tajikistan is not an important financial center in the region and does not have a developed banking system. In many rural areas of the country, the use of a barter system is common.

The most significant financial crime in 2003 was a Ponzi scheme that defrauded many people out of thousands of dollars. The smuggling of consumer goods is a concern. In most cases, goods such as tobacco, alcohol, and fuel are not officially imported into Tajikistan. For example, a shipment intended for Kazakhstan transiting Tajikistan never reaches Kazakhstan. The same practice occurs with goods intended for Afghanistan. While there is certainly a black market for smuggled goods, there is little evidence that items are financed with narcotics money, with the exception of imported cars and luxury items. Drug traffickers can sell drugs outside the country, buy goods with the proceeds, import the goods into Tajikistan, and sell them. One recent money laundering case involved the purchase of Russian cars with the proceeds of narcotics. The cars were subsequently imported into Tajikistan and sold at prices lower than the Russian purchase price. Tajikistan is not an offshore center, but offshore zones are often used while concluding deals with foreign enterprises.

The Tajik Criminal Code of May 21, 1998 Legalization (laundering) of Illegally Obtained Income prohibits money laundering. This prohibition includes not only narcotics money laundering but also circumvention of other financial currency controls. However, under the law banks are not required to know, record, or report the identity of customers engaging in significant transactions unless criminal proceedings have been undertaken against a specific individual or organization. Financial institutions make no regular reports of transactions or other activity, and reporting officers have no special legal protections with respect to cooperating with law enforcement. Several laws and regulations have been adopted including Civil Code Article 284 that addresses the misuse of gold, precious metals and gems. The government has not addressed other forms of alternative remittance systems.

The Law on Banking Activity of May 23, 1998 addresses bank secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement authorities for domestic and offshore financial services companies. Tajikistan has cross-border currency reporting requirements. Travelers may depart with a maximum amount of \$2,000 but may enter with unlimited quantities. In 2003 there were no reported arrests or prosecutions for money laundering or terrorist financing.

Tajikistan does not currently have any asset-seizure mechanisms. Corruption and the undeveloped legal sector make such a program difficult. The Government passed Criminal Code, Art. 57 stating that asset forfeiture is possible but it also specified exceptions. A program is being developed to allow the Drug Control Agency to utilize this law as one means of achieving self-sustainability.

Terrorist finance is considered to be a "serious crime" under the 1998 money laundering statute. Tajikistan has not adopted laws or regulations that ensure the availability of adequate records in connection with narcotics, terrorism, terrorist financing or other investigations. Tajikistan signed the UN Convention Against Terrorism Financing, the CIS Agreement on the Legal Assistance and Cooperation on Civil, Family and Criminal Cases of January 22, 1993, and is a member of the CIS Antiterrorism Center. Tajik authorities have been cooperative with U.S. efforts to trace and halt terrorist-related funds.

Tajikistan is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Tajikistan should enact anti-money laundering and terrorist finance legislation that adheres to world standards.

Tanzania

Tanzania is not considered an important regional financial center, but is vulnerable to money laundering because of the weaknesses of its financial institutions and law enforcement capabilities. A weak financial sector and an under-trained, under-funded law enforcement apparatus make such crimes difficult to track and prosecute. Officials have noted that some real estate and used car businesses are used for money laundering purposes. Government officials have also cited narcotics trafficking and the emerging casino industry as areas of concern for money laundering. The prevalence of hawala and the threat of terrorist organizations on the unregulated island of Zanzibar make it an area of concern. Officials indicate that money laundering schemes in Zanzibar generally take the form of foreign investment in the tourist industry and bulk cash smuggling.

The Proceeds of Crime Act of 1991 criminalizes narcotics-related money laundering. However, the Act does not adequately define money laundering, and it has only been used to prosecute corruption cases. The law obliges financial institutions to maintain records of financial transactions exceeding 10,000 shillings (approximately \$109) for a period of 10 years. If the institution has reasonable grounds to believe that a transaction relates to money laundering, it may communicate this information to the police for investigation, although such reporting is not required. Financial institution employees are legally protected from liability stemming from reporting suspicious transactions.

In November 2002, Parliament approved the Prevention of Terrorism Act, which the President signed into law on December 14. The Act criminalizes terrorist financing. It also requires all financial institutions to inform the government each quarter of whether any of their assets or any transactions may be associated with a terrorist group, although the implementing regulations for this provision have not yet been drafted. Under the Act, the government may seize assets associated with terrorist groups.

The Government of Tanzania (GOT) became a party to the UN International Convention for the Suppression of the Financing of Terrorism in January 2003. Tanzania is a party to the 1988 UN Drug Convention and has signed the UN Convention against Transnational Organized Crime. Tanzania is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), which was founded in 1999. The GOT continues to play a leading role in the operation of this FATF-style regional body and has detailed personnel to the ESAAMLG Secretariat, located in donated office space in Dar es Salaam. Tanzania continues to host the ESAAMLG task force meetings held each March.

In line with Tanzania's commitment to supporting the ESAAMLG, Tanzania has created a multi-disciplinary committee on money laundering and a drafting committee that are preparing a review of the existing law and developing belated comprehensive money laundering legislation. The provisions included in this legislation should provide for the creation of a financial intelligence unit (FIU) that collects mandatory suspicious transaction reporting from financial institutions. This FIU should be empowered to share information with other FIUs and foreign law enforcement agencies.

Tanzania should continue to work through ESAAMLG to establish a FIU and develop a comprehensive anti-money laundering regime that comports with all international standards.

Thailand

Thailand is a major risk for money laundering. Smuggling of narcotics and contraband and evasion of customs duty are significant problems, although physical transit of heroin produced in Burma and Laos through Thailand has been reduced considerably in the past decade. Thailand is also a major production, transit, and distribution country for counterfeit goods. Drug traffickers use Thailand's banking system to hide and move their proceeds. The underground banking system is also widely in use as a money laundering method. Money is transported in bulk from the United States to other Asian

countries, and ultimately moved to Thailand. Gambling dens and underground lotteries account for a significant portion of Thailand's underground economy, and remain attractive mechanisms for money laundering. Thailand financial institutions and gem industry are also vulnerable to misuse by terrorist organizations and their supporters.

Thailand's anti-money laundering legislation, the Anti-Money Laundering Act (AMLA) B.E. 2542 (1999), criminalizes money laundering for the following seven predicate offenses: narcotics trafficking, trafficking in women or children for sexual purposes, fraud, financial institution fraud, public corruption, customs evasion, extortion, and blackmail. On August 11, 2003, Prime Minister Thaksin Shinawatra issued two Executive Decrees to enact measures related to terrorism and terrorist financing as permitted under the Thai Constitution. The two decrees amend section 135 of the penal code and criminalize both terrorism and terrorist financing and make terrorist related crimes the eighth predicate offense under the money laundering statute. In early 2004, the Thai cabinet approved amendments to AMLA to create an asset forfeiture fund, authorize asset sharing, and add the following additional predicate offenses: weapons smuggling, illegal gambling; government procurement fraud; crimes affecting natural resources and the environment; intellectual property rights infringement; and Money Exchange Control Act violations. Legislation is expected to be considered by the Parliament during 2004. Since October 27, 2000, there have been 68 convictions under the AMLA. Cases are proceeding for civil forfeiture against property involved in drug trafficking, prostitution, public fraud and embezzlement, customs evasion, and corruption offenses. The value of assets either forfeited or under seizure total 2,602,523,212.62 Baht (approx. \$65 million).

In addition to the passage of terrorist related legislation in 2003, the RTG issued instructions to all authorities to comply with UN Security Council Resolutions 1267, 1269, 1333, 1373, and 1390, including the freezing of funds or financial resources belonging to the Taliban and the al-Qaida network. To date, Thailand has not identified, frozen, and/or seized assets linked to individuals and entities included on the UN 1267 Sanctions Committee consolidated list. The only action taken regarding alternative remittance systems is the general provisions of the AMLA, that make it a crime to transfer, or receive a transfer, that represents the proceeds of a predicate criminal offense.

The AMLA requires customer identification, record keeping, and the reporting of large and suspicious transactions, and provides as well for the civil forfeiture of property involved in a money laundering offense. Financial institutions are also required to keep customer identification and specific transaction records for a period of five years from the date the account was closed, or from the date the transaction occurred, whichever is longer. Reporting individuals (banks and others) that cooperate with law enforcement entities are protected. Thailand does not have secrecy laws that prevent disclosure of client and ownership information of bank accounts to supervisors and law enforcement authorities. The AMLA gives the anti-money laundering office the authority to compel a financial institution to disclose such information.

The AMLA created the Anti-Money Laundering Office (AMLO), which became fully operational in 2001. AMLO is Thailand's financial intelligence unit (FIU). When first established, AMLO reported directly to the Prime Minister. In October 2002, a reorganization of the executive branch took place, and AMLO was designated as an independent agency under the Ministry of Justice. AMLO receives, analyzes, and processes suspicious and large transaction reports, as required by the AMLA. From January through September 2003, the AMLO received 636,129 currency transaction reports and 84,967 suspicious transaction reports. In addition, AMLO has the responsibility for investigating money laundering for civil forfeiture purposes and has additional responsibility for the custody, management, and disposal of seized and forfeited property. The AMLO is also tasked with providing training to the public and private sectors concerning the provisions of the AMLA. The law also creates the Transaction Committee, which operates within AMLO to review and approve disclosure requests to financial institutions and asset restraint/seizure requests. The AMLA also established the Money Laundering Control Board, which is comprised of ministerial level officials and agency heads and

serves as an advisory board that meets periodically to set national policy on money laundering issues and to propose the relevant ministerial regulations.

The anti-money laundering controls apply to financial institutions and the Bureau of Land. The Stock Exchange of Thailand (SET) requires securities dealers to have know-your-customer procedures; however, the SET does not do any anti-money laundering compliance checks during its reviews. Although insurance companies are covered under the definition in AMLA of a financial institution, there are no anti-money laundering regulations for the insurance industry. Currency exchange dealers are required to be licensed; however, there are no anti-money laundering regulations for exchange businesses.

The Bank of Thailand (BOT) regulates financial institutions in Thailand, but bank examiners are prohibited, except under limited circumstances, from examining the financial transactions of a private individual. This prohibition acts as an impediment to the BOT's auditing of a financial institution's compliance with the AMLA or BOT regulations. Besides this lack of power to conduct transactional testing, BOT does not currently examine its financial institutions for anti-money laundering compliance. However, as a result of discussions between BOT and AMLO, they have agreed to jointly conduct such examinations and expect to begin sometime in 2004.

Financial institutions (such as banks, finance companies, savings cooperatives, etc.), land registration offices, and persons who act as solicitors for investors are required to report significant cash, property, and suspicious transactions. Reporting requirements for most financial transactions (including purchases of securities and insurance) exceeding 2 million baht (approximately \$50,000), and property transactions exceeding 5 million baht (approximately \$125,000), have been in place since October 2000. However, in December 2002, a proposal was made to lower the threshold for reporting cash transactions to 500,000 baht (\$12,500). The proposal is not yet in effect. The various land offices are also required to report on any transaction involving property of 5 million Thai baht, or greater, or a cash payment of 2 million Thai baht, or greater, for the purchase of real property.

Licenses were first granted to Thai and foreign financial institutions to establish Bangkok International Banking Facilities (BIBFs), in March 1993. BIBFs may perform a number of financial and investment banking services but can only raise funds offshore (through deposits and borrowing) for lending in Thailand or offshore. The United Nations Drug Control Program and the World Bank listed BIBFs as potentially vulnerable to money laundering activities, because they serve as transit points for funds. Thailand's 44 BIBFs are now subject to AMLA.

The Royal Thai Government (RTG) has established the Department of Special Investigation (DSI), within the Ministry of Justice pursuant to the Special Investigations Act of 2004. The DSI and the Royal Thai Police (RTP) will conduct criminal investigations of money laundering and related predicate offenses, while the AMLO will handle civil asset forfeiture cases. The DSI will become operational following the promulgation of ministerial regulations, which is expected to occur in 2004. It is also anticipated that the DSI and the RTP will enter into a memorandum of understanding to delineate investigative responsibilities.

The U.S.-Thai Mutual Legal Assistance Treaty entered into force in 1993. Thailand also has mutual legal assistance agreements with the United Kingdom, Canada, China, France, and Norway. Numerous bilateral agreements are pending, as well as memoranda of understanding between the Anti-Money Laundering Office and financial intelligence units in other nations. In December 2000, Thailand signed, but has not yet ratified, the UN Convention against Transnational Organized Crime, and is studying its domestic laws to determine what implementing legislation is required. Thailand has signed the UN Convention against Corruption, the first legally binding international agreement aimed at combating corruption, in Merida, Mexico on December 9, 2003. Thailand is a party to the 1988 UN Vienna Convention. The RTG has signed, but not ratified, the UN International Convention for the Suppression of the Financing of Terrorism.

AMLO became a member of the Asia/Pacific Group on Money Laundering in April 2001 and the Egmont Group of financial intelligence units in June 2001. AMLO hosted the Pacific Rim Money Laundering and Financial Crimes Conference from March 24 through 26, 2003, in Bangkok.

The Royal Thai Government should continue to implement its anti-money laundering program, but until the RTG provides a viable mechanism for all of its financial institutions to be examined for compliance with the AMLA, Thailand's anti-money laundering regime will not comport with international standards. The RTG should require the SET to include anti-money laundering compliance checks during its reviews. The RTG should develop and implement anti-money laundering regulations for exchange businesses and should take additional measures to address alternative remittance systems to further strengthen its anti-money laundering regime against crime, particularly by expanding its predicate offenses to include a broader base of serious financial crimes, such as arms/weapons trafficking, alien smuggling, and environmental crimes, as well as making structuring a criminal offense.

Thailand continues to suffer problems with asset management and disposition, due in part to a lack of resources. This lack of resources could be addressed through the creation of an Asset Forfeiture Fund, which could make funds available for money laundering and asset forfeiture investigations. Thailand appears to recognize the utility in this concept as evidenced by the recent Cabinet approval to introduce legislation to amend AMLA.

During the past year, the RTG has instituted a practice of providing rewards to investigators up to 25 percent of the value of the asset forfeited. Such a practice raises ethical concerns, can distort the law enforcement motive when seizing property, can encourage overreaching and illegal seizures, and is a practice that should be revisited.

Thailand should become a party to the relevant UN multilateral conventions, including: International Convention for the Suppression of the Financing of Terrorism; Convention against Transnational Organized Crime; and Convention Against Corruption.

Togo

Togo's poor financial infrastructure makes it an unlikely venue for money laundering through its financial institutions. Its porous borders, however, make it a transshipment point in the regional and sub-regional trade in narcotics. Togo's 1998 drug law criminalizes narcotics-related money laundering and penalizes offenses with up to 20 years in prison. However, there have never been any arrests for money laundering. Financial institutions are required to monitor and report monetary transactions above a threshold appropriate to the local economic situation, and must maintain records of such transactions and supply them to government authorities on request. Financial institutions are legally protected in respect to their cooperation with law enforcement authorities. Due diligence legislation applies to bankers and other professionals, although no arrests have been made for violations of this law.

The Government of Togo (GOT) has the legal authority to seize assets associated with narcotics trafficking. In 2001, President Eyadema created the national Anti-Corruption Commission to combat corruption and money laundering.

Terrorist financing is a criminal offense in Togo. The GOT has circulated to Togolese financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. The GOT closely regulates charities and other nongovernmental organizations.

The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the countries in the West African Economic and Monetary Union (WAEMU): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal, and Togo, all of which use the French-backed CFA franc currency. All bank deposits over approximately \$7,700 made in BCEAO member countries must be reported to the BCEAO, along with customer identification information. In September 2002, the WAEMU Council of Ministers, which oversees the BCEAO, issued a directive requesting that each member country set up a national committee under their Minister of Finance to deal with financial information as it relates to money laundering. The BCEAO would be in charge of coordinating such committees. Each member country is now responsible for putting legislation in place to implement this directive, and the legislation is expected to be harmonized regionally.

The WAEMU Council of Ministers issued another directive in September 2002 requesting member countries to pass legislation requiring banks to freeze the accounts of any persons or organizations on the UN 1267 Sanctions Committee consolidated list.

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

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

Togo should criminalize money laundering for all serious crimes and should enforce existing laws and regulations.

Tonga

Tonga is an archipelago, located in the South Pacific, about two-thirds of the way from Hawaii to New Zealand. Tourism is the second largest source of hard currency earnings following remittances. Tonga is neither a financial center nor an offshore jurisdiction. An additional source of revenue is the registry of approximately 65 ships from 25 countries, including the United States. Tonga became a party to the UN International Convention for the Suppression of the Financing of Terrorism in December 2002.

In a report to the UN Counter-Terrorism Committee, Tonga reported that its Government Committee on Money Laundering and the Financing of Terrorism was working on proposed new legislation and amendments to bring its legislative framework into line with international best practices. Tonga should enact legislation that specifically criminalizes the financing of terrorism and should consider joining the Asia/Pacific Group on Money Laundering.

Trinidad and Tobago

Trinidad and Tobago has a well-developed and modern banking sector that makes it an increasingly significant regional financial center. Trinidad and Tobago (T&T) is not an offshore financial center. Narcotics proceeds are implicated in some money laundering, but this is not a known important source of financial crimes in T&T. Criminal proceeds laundered in T&T are derived primarily from domestic criminal activity and from the activity of nationals involved in crime abroad.

The Proceeds of Crime Act of 2000 (POCA) expands money laundering predicate offenses to include all serious crimes. The POCA requires financial institutions to proactively report suspicious transactions, and banks and financial institutions are required to maintain records necessary to

Money Laundering and Financial Crimes

reconstruct transactions for a number of years. Secrecy laws are limited to standard client confidentiality provisions. Failure to comply with POCA's record keeping and reporting requirements can result in a fine of 250,000 TT (approximately \$40,000) and imprisonment for two years for summary conviction, and a fine of 3,000,000 TT (approximately \$500,000) and seven years imprisonment for conviction on indictment. Upon summary conviction for money laundering, an offender can be liable for a fine of 25,000,000 TT (approximately \$4,000,000) and 25 years imprisonment. Furthermore, under the POCA, any officer who aids and abets the money laundering activities of an institution can be convicted of money laundering. The POCA also enables the courts to seize the proceeds of all serious crimes, although no profits or property have been seized under the Act.

The Central Bank has set anti-money laundering guidelines, including due diligence provisions that apply to all financial institutions subject to the 1993 Financial Institutions Act. These include banks, finance companies, leasing corporations, merchant banks, mortgage institutions, unit trusts, credit card businesses, financial services businesses and financial intermediaries. Credit unions and exchange houses are not subject to the guidelines.

Government of Trinidad and Tobago (GOTT) customs regulations require that any sum above approximately \$5,000 (in currency or monetary instruments) entering or leaving the country be declared. Cash above approximately \$10,000 may be seized, with judicial approval, pending determination of its legitimate source.

The GOTT is progressing operationally to establish a financial intelligence unit. In November 2003, as part of that goal, the GOTT Ministry of Finance inaugurated a new Criminal Investigation Division within the Bureau of Inland Revenue. The GOTT has an inter-ministerial counternarcotics/crime task force that investigates narcotics trafficking and related money laundering. Since January 1, 2003, there are five on-going money laundering investigations.

The GOTT has legislation in place that allows it to trace, freeze, and seize assets, including intangible assets such as bank accounts. Authorities may seize legitimate businesses if they are used to launder drug money. The GOTT does not have legislation that specifically authorizes the sharing of forfeited assets with other countries, but has done so in the past on a case-by-case basis through bilateral agreements.

Legislation specifically aimed to criminalize the financing of terrorism has been stalled in Parliament because the opposition party has blocked terrorist financing reform as part of its domestic political agenda. The GOTT is developing financial sector supervision regulations that acknowledge and monitor alternative remittance systems. The use of charitable or nonprofit entities has been reported whenever suspect by the banking system. The GOTT has circulated to its financial institutions the lists of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list as being linked to Usama Bin Ladin, al-Qaida, or the Taliban, along with the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 (on terrorist financing) and the relevant EU lists. There has not yet been any identified evidence of terrorist financing in T&T.

Trinidad and Tobago is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. The GOTT has not become a signatory to the UN International Convention for the Suppression of the Financing of Terrorism. T&T is also a member of the Caribbean Financial Action Task Force (CFATF), which is headquartered in Port of Spain. It underwent a second round CFATF mutual evaluation in 2002, and the report has been endorsed by CFATF's Council of Ministers. T&T is also a member of the OAS Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). In 1999, an MLAT with the United States entered into force. In 2000, the United States and GOTT signed a joint

statement on law enforcement cooperation, which pledges in part to expand cooperation on the detection and prosecution of money laundering and related criminal activities.

The GOTT should pass antiterrorist financing legislation that will provide the authority to identify, freeze and seize terrorist assets. The GOTT should also continue to implement its anti-money laundering program and its efforts to improve its ability to investigate money laundering.

Tunisia

Tunisia is not considered an important regional financial center due in large part to the very strict control exercised by the Central Bank over all aspects of financial transactions and the general nonconvertibility of the Tunisian dinar. There is no discernible money laundering activity reported to be occurring in Tunisia through formal financial institutions.

Although there is no specific anti-money laundering law in Tunisia, Law No. 92-52 (of May 18, 1992) against narcotics trafficking includes provisions that could contribute to combat money laundering. Under Articles 2 and 30 of this law anyone aiding in narcotic operations or transfers of proceeds in connection with these operations, including financial institutions, can be punished. On December 9, 2003 the Tunisian Parliament passed Law No. 94/2003 criminalizing support and financing to individuals, organizations or activities related to terrorism.

The Tunisian penal code allows for the sequestering, confiscating, or seizure of assets and property in certain situations including narcotics trafficking and terrorist activities. The definition of “assets” is quite broad and could cover any number of financial or physical assets. Financial assets are traced by the Central Bank and the Economic Enforcement Agency, each of which has broad powers for investigating and seizing financial assets. Tunisia has no legal provisions for sharing seized criminal assets with other governments.

Financial institutions are required to gather full identifying information for personal and business accounts. In addition, all supporting documentation must be maintained for 10 years. Only certain categories of individuals and businesses are allowed to open foreign currency or convertible dinar accounts and all of these accounts are monitored by the Central Bank. Because there is no law against money laundering in general, there is no obligation for a financial institution to report suspicious activities or provisions for holding bankers responsible if their institution is used for money laundering. However, the prevailing practice is for institutions to verbally report any unusual activity to the Central Bank, who will notify the investigative Economic Enforcement Agency. There are no “secret” or numbered accounts in Tunisia.

Offshore financial institutions are held to the same regulatory standards as onshore institutions. Offshore institutions undergo the same due diligence process as onshore banks and are licensed only after the Central Bank investigates their reference and recommends that the Ministry of Finance approve their application. Tunisian law also makes provisions for “moral integrity” checks of major shareholders, directors, and officers of financial institutions at any time doubts may arise. Anonymous directors are not allowed. Tunisia currently hosts 12 offshore banks, approximately 1,200 offshore companies and approximately 300 offshore trading companies. There are no offshore casinos or Internet gaming sites. Bearer financial instruments or shares are prohibited (Act No. 35 of 2000.)

Although the Tunisian government maintains that there are no alternative fund transfer systems such as hawala since all fund transfers must go through the banks or National Post Office, it is precisely due to these restrictions and currency exchange controls there are underground methods of moving money or transferring value in and out of the country. While a gray market in consumer goods does exist in the country, there is no evidence that this trade is funded by illicit proceeds. Residents are generally prohibited from holding or exporting foreign currency except in certain cases (travel or business needs, etc.) Nonresidents entering Tunisia with foreign currency or other instruments are required to declare

the total amount if they wish to re-export a portion (not exceeding 1,000 dinar or approximately \$840) or deposit any of the money in a Tunisian bank. Nonresidents do not need to declare currency exports of under 1,000 dinar. In December 2002, the legislature discussed tightening gold import regulations in light of an emerging parallel gold market. Customs may at any time require declarations for gold or securities.

Tunisia is a party to the 1988 UN Drug Convention. It has signed and ratified the UN Convention against Transnational Organized Crime. The Central Bank has adhered to all requests from the UN 1267 Sanctions Committee. To date no terrorist assets have been identified in Tunisia. Tunisia is party to the UN International Convention for the Suppression of Financing of Terrorism. Tunisia has varying bilateral agreements on “criminal matters” with 29 countries and is party to 12 international agreements on counterterrorism.

Tunisia should pass a comprehensive anti-money laundering law that adheres to world standards as the first step in developing a viable anti-money laundering program.

Turkey

Turkey is an important regional financial center, particularly for Central Asia and the Caucasus, as well as for the Middle East and Eastern Europe. Turkey is not an offshore financial center and does not have secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement officials. It continues to be a major transit route for Southwest Asian opiates moving to Europe. However, local narcotics-trafficking organizations are reportedly responsible for only a small portion of the total of funds laundered in Turkey. A substantial percentage of money laundering that takes place in Turkey appears to involve tax evasion, and informed observers estimate that as much as 50 percent of the economy is unregistered. There is no significant black market for smuggled goods in Turkey.

Money laundering takes place in both banks and nonbank financial institutions. Traditional money laundering methods in Turkey involve the cross-border smuggling of currency; bank transfers into and out of the country; and the purchase of high value items such as real estate, gold, and luxury automobiles. It is believed that Turkish-based traffickers transfer money to pay narcotics suppliers in Pakistan and Afghanistan, primarily through Istanbul exchange houses. The exchanges then wire transfer the funds through Turkish banks to accounts in Dubai and other locations in the United Arab Emirates. The money is then paid, often through alternative remittance systems, to the Pakistani and Afghan traffickers.

Turkey criminalized money laundering in 1996 for a wide range of predicate offenses, including narcotics-related crimes, smuggling of arms and antiquities, terrorism, counterfeiting, and trafficking in human organs and in women. The Council of Ministers subsequently passed a set of regulations that mandate the filing of suspicious transaction reports (STRs), and require customer identification and the maintenance of records for five years. These regulations apply to banks and a wide range of nonbank financial institutions, including insurance firms and jewelry dealers. However, the number of STRs being filed is quite low, even taking into consideration the fact that the Turkish economy is cash-based. A possible reason for this is the lack of safe harbor protection for bankers and other filers of STRs. Turkish officials indicated in August 2002 that the Government of Turkey (GOT) has drafted a bill that will provide such protection, but it has not yet been enacted. Turkey also has in place a system for identifying, tracing, freezing, and seizing narcotics-related assets, although Turkish law allows for only criminal forfeiture.

In July 2001, the Ministry of Finance issued a circular of banking regulations requiring all banks, including the Central Bank, securities companies, and post office banks, to record tax identity information for all customers opening new accounts, applying for checkbooks, or cashing checks. The

circular also requires exchange offices to sign contracts with their clients. Additionally, noninterest-utilizing entities such as Islamic financial institutions are required to record tax identity information for all transactions.

The Ministry of Finance also issued a circular mandating that a tax identity number be used in all financial transactions as of September 1, 2001. The circular applies to all Turkish banks and to branches of foreign banks operating in Turkey, as well as other financial entities. The new requirements are intended to increase the government's ability to track suspicious financial transactions.

Since the financial crisis of 2000, the GOT has taken over 19 of Turkey's 81 banks and has significantly tightened oversight of the banking system through an independent regulatory authority, the Banking Regulatory and Supervisory Agency (BRSA), which conducts anti-money laundering compliance reviews at banks under authority delegated from the Financial Crimes Investigation Board (MASAK). However, BRSA's reputation was hurt recently by its failure to detect a major bank fraud involving Imar Bank. There is also some concern about the current government's commitment to BRSA's continued independence.

The 1996 anti-money laundering law established MASAK, which is part of the Ministry of Finance. MASAK, which became operational in 1997, receives, analyzes, and refers STRs for investigation. MASAK serves as Turkey's financial intelligence unit (FIU). MASAK has a pivotal role between the financial community, on the one hand, and Turkish law enforcement, investigators, and judiciary, on the other. Since its inception, MASAK has pursued more than 500 money laundering cases. Of those, 59 have been prosecuted, with only two cases resulting in convictions as of December 2003. Part of this is due to the fact that Turkey's police, prosecutors, judges, and investigators still need substantial training in dealing with financial crimes and because of a lack of coordination between the courts that prosecute the predicate offenses and the courts that prosecute money laundering cases. Most of the cases involve nonnarcotics criminal actions or tax evasion; roughly 30 percent are narcotics related.

MASAK itself is not yet functioning at the optimal level of efficiency. It requires additional legal authority, continuity of senior management, training, and computers. Training and equipment needs are being addressed by a European Union accession project, which is expected to commence by mid-2004. In 2003 MASAK prepared an amendment to the seminal 1996 law, that MASAK hopes Parliament will ratify in early 2004. The new law will broaden the definition of money laundering and expand the list of predicate offenses. It will also increase MASAK's authority and expand its ability to cooperate with other GOT agencies. After passage of the proposed legislation, MASAK expects to conduct compliance reviews of banks itself instead of relying on the BRSA. The GOT is also drafting legislation that will enable MASAK to conduct money laundering investigations into bank owners who misuse their banks' capital, to investigate the proceeds of bribery and corruption, and to investigate fraudulent bankruptcy cases. If all these changes are implemented, Turkey's anti-money laundering law will include all predicate offenses listed by the Financial Action Task Force (FATF).

Turkey cooperates closely with the United States and its neighbors in the Southeast Europe Cooperation Initiative (SECI). Turkey and the United States have an MLAT and cooperate closely on narcotics and money laundering investigations. Following the election of a new government in Turkey in November 2002, many of the key officials responsible for counternarcotics and anti-money laundering programs (including the head of MASAK) were replaced in 2003. Recently, the timeliness of MASAK's response to requests made through the assistance mechanisms of the Egmont Group has been declining.

Turkey has traditionally taken a strong stance against terrorism. In February 2002, MASAK issued General Communiqué No. 3 that detailed a new type of STR to be filed by financial institutions in cases of terrorist financing. The GOT complies with UNSCR 1373 through the distribution to interested GOT agencies (but not financial institutions) of ministerial decrees. Financial institutions

receive the lists through the Turkish Bankers Association. The GOT has the authority to identify and freeze the assets of terrorist individuals and groups designated by the UN 1267 Sanctions Committee, and it froze such assets in several cases during 2002. However, the process can be cumbersome and is not particularly effective; in 2003, a joint FBI-Royal Canadian Mounted Police investigation on terrorist financing was hampered by the lack of a specific law criminalizing the financing of terrorism. The proposed legislation described above should ameliorate the situation. In the interim, there are various laws with provisions that can be used to punish the financing of terrorism. In particular, Article 169 of the Turkish Penal Code prohibits assistance in any form to a criminal organization or to any organization which acts to influence public services, media, proceedings of bids, concessions, and licenses, or to gain votes, by using or threatening violence. To commit crimes by implicitly or explicitly intimidating and cowering people is illegal under the provisions of the Law No. 4422 on the Prevention of Benefit-Oriented Criminal Organizations.

Turkey is a member of the FATF. MASAK is an active member of the Egmont Group. Turkey is a party to the 1988 UN Drug Convention and in December 2003 ratified the UN Convention against Transnational Organized Crime. Additionally, in April 2003 Turkey ratified the Council of Europe (COE) Civil Law on Corruption. In May 2002, Turkey became a party to the UN International Convention for the Suppression of Terrorist Bombings. Turkey also became a party to the UN International Convention for Suppression of the Financing of Terrorism on June 28, 2002. Turkey has signed, but not yet ratified, the COE Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime.

Turkey has declared its commitment to fight money laundering and terrorist financing. However, it needs to strengthen its legislative basis for this by swiftly enacting the draft laws to strengthen MASAK's powers and to criminalize terrorist financing. It should also obtain training for its prosecutors, judges, and investigators and improve the coordination between the courts in order to enable them to obtain more convictions for money laundering. The GOT should enact its safe harbor bill to protect the filers of STRs, which may result in increased filings. Tax evasion remains a severe problem in Turkey and is directly linked to money laundering. Turkey's 2001 initiative on tax identity numbers should enhance its ability to prosecute tax evaders. Turkey should also regulate and investigate alternative remittance networks to thwart misuse by terrorist organizations or their supporters.

Turkmenistan

Turkmenistan has only a few international banks and a small, underdeveloped domestic financial sector. Turkmenistan's economy is primarily cash-based. Due to the presence of narcotics-trafficking and organized criminal groups, the country is susceptible to money laundering. There is some concern that several of the country's foreign-owned hotels and casinos could be vulnerable to financial fraud and used for money laundering. In addition, the national currency, the manat, has a black market exchange rate that is four times the official rate. These rates create conditions that are favorable to money laundering. Corruption in Turkmenistan is also a source of concern due to the low salaries and broad general powers of Turkmen law enforcement officials. In 2003, the Government of Turkmenistan did not report any suspected cases of money laundering.

Article 242 of the Criminal Code imposes liability for the laundering of criminal proceeds. Financial and other transactions using criminal proceeds are punishable by a fine or up to two years imprisonment. Presidential Resolution 0210/02-2 of 1995 gives the Central Bank authority over all international financial transactions. Under this resolution, any entity making an electronic transfer of funds to an account abroad must provide documentation that establishes the source of the funds. Turkmenistan's tax inspectorate has responsibility for uncovering irregularities that might be

indicative of financial crimes and money laundering. The tax inspectorate works in coordination with Turkmen law enforcement. Turkmenistan is a party to the 1988 UN Drug Convention.

Turkmenistan is urged to sign the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism. Turkmenistan should pass anti-money laundering and terrorist finance legislation that adheres to world standards.

Turks and Caicos

The Turks and Caicos Islands (TCI) is a Caribbean overseas territory of the United Kingdom (UK). TCI is comprised of two island groups and forms the southeastern end of the Bahamas archipelago. The U.S. dollar is the currency in use. TCI has a significant offshore center, particularly with regard to insurance and international business companies (IBCs). Its location has made it a transshipment point for narcotics-traffickers. The TCI is vulnerable to money laundering because of a large offshore financial services sector as well as because of bank and corporate secrecy laws and Internet gaming activities. There was no updated information to add in 2004.

The TCI's offshore sector has eight banks (five of which also deal with onshore clientele), approximately 2,500 insurance companies, 1,000 trusts, and 13,000 "exempt companies" that are IBCs, including those formed by the Enron Corporation. The Financial Services Commission (FSC) licenses and supervises banks, trusts, insurance companies, and company managers; it also licenses IBCs and acts as the Company Registry for the TCI. The Financial Services Commission employs a staff of 14 and conducts limited on-site inspections. The FSC became a statutory body under the Financial Services Commission Ordinance 2001 and became operational in March 2002, and now reports directly to the Governor.

The offshore sector offers "shelf company" IBCs, and all IBCs are permitted to issue bearer shares; however, the Companies (Amendment) Ordinance 2001 requires that bearer shares be immobilized by depositing them, along with information on the share owners, with a defined custodian. This applies to all shares issued after enactment and allows for a phase-in period for existing bearer shares of two years. Trust legislation allows establishment of asset protection trusts inoculating assets from civil adjudication by foreign governments; however, the Superintendent of Trustees has investigative powers and may assist overseas regulators.

The 1998 Proceeds of Crime Ordinance criminalizes money laundering related to all crimes and establishes extensive asset forfeiture provisions and "safe harbor" protection for good faith compliance with reporting requirements. The Law also establishes a Money Laundering Reporting Authority (MLRA), chaired by the Attorney General, to receive, analyze, and disseminate financial disclosures such as suspicious activity reports (SARs). Its members also include the following individuals or their designees: Collector of Customs, the Superintendent of the FSC, the Commissioner of Police, and the Superintendent of the Criminal Investigation Department. The MLRA is authorized to disclose information it receives to domestic law enforcement and foreign governments.

The Proceeds of Crime (Money Laundering) Regulations came into force January 14, 2000. The Money Laundering Regulations place additional requirements on the financial sector such as identification of customers, retention of records for a minimum of five years, training staff on money laundering prevention and detection, and development of internal procedures in order to ensure proper reporting of suspicious transactions. The Money Laundering Regulations apply to banking, insurance, trustees, and mutual funds. Although the customer identification requirements only apply to accounts opened after the Regulations came into force, TCI officials have indicated that banks would be required to conduct due diligence on previously existing accounts by December 2005.

In 1999, the FSC, acting as the secretary for the MLRA, issued nonstatutory Guidance Notes to the financial sector, in order to help educate the industry regarding money laundering and the TCI's anti-

money laundering requirements. Additionally, it provided practical guidance on recognizing suspicious transactions. The Guidance Notes instruct institutions to send SARs to either the Royal Turks & Caicos Police Force or the FSC. Officials forward all SARs to the Financial Crimes Unit (FCU) of the Royal Turks and Caicos Islands Police Force, which analyzes and investigates financial disclosures. The FCU also acts as TCI's financial intelligence unit (FIU).

As with the other United Kingdom Caribbean overseas territories, the Turks and Caicos underwent an evaluation of its financial regulations in 2000, co-sponsored by the local and British governments. The report noted several deficiencies and the government has moved to address most of them. The report noted the need for improved supervision, which the government acknowledged. An Amendment to the Banking Ordinance was introduced in February 2002 to remedy deficiencies outlined in the report relating to notification of the changes of beneficial owners, and increased access of bank records to the FSC, but the Ordinance has not yet been enacted. No legislation has yet been introduced to remedy the deficiencies noted in the report with respect to the Superintendent's lack of access to the client files of Company Service and Trust providers, nor is there legislation that clarifies how the Internet gaming sector is to be supervised with respect to anti-money laundering compliance.

The TCI cooperates with foreign governments—in particular, the United States and Canada—on law enforcement issues including narcotics trafficking and money laundering. The FCU also shares information with other law enforcement and regulatory authorities inside and outside of the TCI. The Overseas Regulatory Authority (Assistance) Ordinance 2001, allows the TCI to further assist foreign regulatory agencies. This assistance includes search and seizure powers and the power to compel the production of documents.

The TCI is a member of the Caribbean Financial Action Task Force, and is subject to the 1988 UN Drug Convention. The Mutual Legal Assistance Treaty between the United States and the United Kingdom concerning the Cayman Islands was extended to the TCI in November 1990.

The Turks and Caicos have put in place a comprehensive system to combat money laundering with the relevant legislative framework and an established FIU. The FSC has made steady progress in developing its regulatory capability and has some experienced senior staff. However, the current regulatory structure is not fully in accordance with international standards. The TCI should criminalize the financing of terrorists and terrorism, and enhance its on-site supervision program. TCI should expand efforts to cooperate with foreign law enforcement and administrative authorities. TCI should provide adequate resources and authorities to provide supervisory oversight of its offshore sector in order to further ensure criminal or terrorist organizations do not abuse the TCI's financial sector.

Uganda

Uganda is not a regional money laundering center. Ugandan law enforcement agencies suspect that Uganda's bank and nonbank financial sectors are used to launder money, but thus far have been unable to prove their suspicions because of the country's inadequate legal framework. Foreign exchange bureaus and alternative remittance systems are widely used in Uganda and are essentially unregulated.

In 2001, Uganda criminalized narcotics-related money laundering. The Bank of Uganda issued "Know Your Customer" guidelines; however, the bank does not have the authority to penalize noncompliance. In December 2003, the Ministry of Finance submitted to parliament a comprehensive anti-money laundering bill developed based on FATF's Forty Recommendations on Money Laundering. This legislation would criminalize money laundering for all serious crimes.

Uganda is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) and served as chairman of ESAAMLG in 2003. Uganda is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the United Nations Convention against Transnational Organized Crime.

Uganda criminalized terrorist financing in the Anti-Terrorism Act of June 2002. Uganda is a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Uganda should enact comprehensive anti-money laundering legislation and construct a viable anti-money laundering regime capable of thwarting terrorist financing.

Ukraine

Although Ukraine has adopted, enacted, and implemented comprehensive anti-money laundering legislation over the past year, high level and widespread corruption, organized crime, smuggling, and tax evasion continue to plague Ukraine's economy. Transparency International has rated Ukraine 2.4—unchanged from 2002—on a scale where 10 means “highly clean.” Money laundering in Ukraine is not primarily related to proceeds from narcotics trafficking. Instead, proceeds originate in criminal activities such as smuggling of goods or trafficking in humans, and large-scale corruption by government official and others. Ukraine's former Prime Minister, Pavlo Lazarenko, is currently out on bail awaiting trial in San Francisco on charges that he laundered over \$114 million, which he allegedly obtained illegally while serving as Prime Minister. Ukraine has provided assistance to the United States in connection with this prosecution. Retail outlets that sell luxury goods and other businesses (including casinos and some restaurants) in Kiev and elsewhere are suspected of being fronts for money laundering and/or tax evasion.

When the Financial Action Task Force (FATF), in September 2001, placed Ukraine on the list of noncooperative countries and territories in the fight against money laundering (NCCT), its report noted that Ukraine lacked (1) a complete set of anti-money laundering laws; (2) an efficient mandatory system for reporting suspicious transactions to a financial intelligence unit (FIU); (3) adequate customer identification requirements; and (4) adequate resources at present to combat money laundering. Following the FATF action, the United States Treasury Department issued an advisory to all U.S. financial institutions instructing them to “give enhanced scrutiny” to all transactions involving Ukraine. FATF gave Ukraine until October 2002 to enact comprehensive, effective anti-money laundering legislation, or it would face the possibility of countermeasures from the FATF member countries.

At its September 2002 plenum, FATF extended its original October 2002 deadline until December 15, 2002. On November 28, 2002, President Kuchma signed into law Ukrainian Law No. 249-IV, an anti-money laundering package “On Prevention and Counteraction to the Legalization (Laundering) of the Proceeds from Crime.” On December 20, 2002, the FATF determined that Ukraine's AML statute did not meet international standards and announced that FATF members would impose countermeasures on Ukraine. Under Section 311 of the USA PATRIOT Act, the United States designated Ukraine as a jurisdiction of primary money laundering concern on December 20, 2002. In response to the imminent threat of countermeasures, Ukraine passed further comprehensive legislative amendments in December 2002 and February 2003, in accordance with FATF demands. Immediately upon passage of the February amendments, the FATF withdrew its call for members to invoke countermeasures and the U.S. followed suit on April 17, 2003 by revoking Ukraine's designation under Section 311 of the USA PATRIOT Act as a jurisdiction of primary money laundering concern.

By passing comprehensive anti-money laundering (AML) legislation, Ukraine was not only able to avoid the countermeasures threatened by the FATF, but to initiate the process of NCCT de-listing. At the FATF plenary in September 2003, Ukraine was invited to submit an implementation plan, and upon review by the FATF Europe Review Group (ERG), an on-site visit to assess Ukraine's progress in developing its anti-money laundering regime has been scheduled for January 19-23, 2004. The results of the on-site visit by the FATF evaluation team will be reported to the FATF ERG prior to the Paris plenary on February 25, 2004. The ERG will give its recommendation as to whether or not the NCCT designation should be lifted and a decision will be taken by the general plenary at that time.

As a member of the Council of Europe, Ukraine has undergone two mutual evaluations by that group's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), in May 2000 and September 2003. Although Ukraine criminalized drug money laundering in 1995, the initial 2000 mutual evaluation report was highly critical of Ukraine. The 2003 evaluation presented quite a different finding, as evaluators noted that a number of the previously noted deficiencies had been remedied, especially with regard to passage of a basic anti-money laundering law in November 2002.

Two subsequent sets of amendments adopted in December 2002 and February 2003 have further helped bring Ukraine into compliance with internationally-recognized standards, as set forth by the FATF, the Vienna and Strasbourg conventions, the European Union (EU) directives on prevention of use of the financial system for money laundering purposes, and the Basel principles applicable to banks. Effective September 1, 2001, the Government of Ukraine (GOU) criminalized nondrug money laundering in the Criminal Code of Ukraine. Subsequent amendments adopted in January 2003 include willful blindness provisions and also expand the scope of predicate crimes for money laundering to include any action that is punishable under the criminal code by imprisonment of three years or more, excluding certain specified actions. Provisions in the criminal code also address drug-related money laundering offenses and provide for the confiscation of proceeds generated by criminal activities.

The GOU enacted the "Act on Banks and Banking Activities" (Act) of January 2001, which imposes anti-money laundering measures upon banking institutions. The Act prohibits banks from opening accounts for anonymous persons, requires the reporting of large transactions and suspicious transactions to state authorities, and provides for the lifting of bank secrecy pursuant to an order of a court, prosecutor, or specific state body. Further amendments in February 2003 require banks to establish and implement bank compliance programs, conduct due diligence to identify beneficial account owners prior to opening an account or conducting certain transactions, and maintain records on suspicious transactions and the people carrying them out, for a period of five years. Cross-border transportation of cash sums exceeding \$1000 must be declared by travelers.

In August 2001, "The Law on Financial Services and State Regulation of the Market of Financial Services" was signed. The law establishes regulatory controls over nonbank financial institutions that manage insurance, pension accounts, financial loans, or "any other financial services involving savings and money from individuals." Specifically, the law defines financial "institutions" and "services," imposes record keeping requirements on covered entities, and identifies the responsibilities of regulatory agencies. The law created the State Commission on Regulation of Financial Services Markets, which, with the National Bank of Ukraine and the State Commission on Securities and the Stock Exchange, has the primary responsibility for regulating financial services markets. Amendments introduced in February 2003 set forth additional requirements similar to those prescribed for banks for all nonbanking financial institutions.

The AML legislation calls for customer identification, reporting of suspicious and unusual transactions to the State Department of Financial Monitoring, and five years of record keeping. It also mandates the establishment of anti-money laundering procedures in first-line financial institutions such as banks; stock, securities, and commodity brokers; and insurance companies, among other entities. Subsequent amendments to Articles 5, 6, and 8, respectively, mandate establishment of bank compliance programs and appointment of bank compliance officers who may be subject to criminal liability for noncompliance. They also mandate that financial institutions identify beneficial owners of accounts, and that employees of entities of initial financial monitoring unconditionally report transactions suspected for money laundering or terrorism finance. The AML legislation includes a "safe harbor" provision that protects reporting institutions from liability for cooperating with law enforcement agencies.

Significantly, amendments to Article 11 of the Law reduce the monetary threshold beyond which transactions and operations are subject to compulsory financial monitoring, from Ukrainian hryvnias (UAH) 300,000 (approximately \$57,750) for cashless payments and UAH 100,000 (approximately \$19,250) for payments in cash to one single amount for both, UAH 80,000 (approximately \$15,400). The compulsory transaction-reporting threshold stands only if the transaction also meets one or more suspicious activity indicators as set forth in the law. Any transaction that is suspected of being connected to terrorist activity is to be reported to the appropriate authorities immediately.

On December 10, 2001, the Ukrainian Presidential Decree “Concerning the Establishment of a Financial Monitoring Department” mandated the creation of the State Department of Financial Monitoring (FMD) by January 1, 2002, to function as Ukraine’s FIU. Under the terms of this decree, the FMD is an independent authority administratively subordinated to the Ministry of Finance and is the sole agency authorized to receive and analyze financial information from first line financial institutions. Ukraine’s basic AML law establishes a two-tiered system of financial monitoring and combating of criminal proceeds, including terrorist financing provisions. It also identifies the participants: entities of initial financial monitoring, or those legal entities that carry out financial transactions; and entities of state financial monitoring, or those regulating entities charged with regulation and supervision of activities of the service providers. The overall regulatory authority in the system is vested in the FMD, which became operational on June 12, 2003, in accordance with Article 4 of the AML law.

The FMD is an administrative agency with no investigative or arrest authority. It is authorized to collect and analyze suspicious transactions, including those related to terrorism financing, and to transfer financial intelligence information to competent law enforcement authorities for investigation. FMD also has authority to conclude interagency agreements, and can exchange intelligence on financial transactions with a money laundering or terrorist financing nexus with other FIUs. As of October 21, 2003, memoranda of understanding were concluded between the FMD and the financial intelligence units of the Russian Federation, the Slovak Republic, Estonia, Spain, and the Kingdom of Belgium.

To date, the FMD has received 209,025 suspicious transaction reports (STRs), the bulk of which have been reported by banks. Approximately ten percent of these have been identified by the FIU for “active research” and 3,211 separate materials have been sent to competent law enforcement agencies. From June 12, 2003, the date the FMD became operational, through December 2003, FMD has referred 11 criminal cases to the General Prosecutor’s Office, two cases to the State Tax Administration, three cases to the Ministry for Internal Relations, and two cases to the Security Service.

Regarding criminal prosecution of anti-money laundering cases, 25 cases were brought before the courts during the last five months of 2001, for which three convictions were obtained. In 2002, 287 criminal AML cases were brought before the courts and 77 convictions were obtained. For the first nine months of 2003, 128 criminal AML cases were brought before the courts, resulting in 40 convictions.

Ukraine is in the initial stages of drafting a law that may permit asset forfeiture. Ukraine has yet to establish a system and a legal basis for freezing and seizing assets derived from serious crimes.

In response to earlier criticisms by the FATF regarding lack of coordination and information-sharing among agencies, the Cabinet of Ministers issued Decree No. 1896 on December 10, 2003, establishing a Unified State Informational System of Prevention and Counteraction of Money Laundering and Terrorism Financing, which will allow for integration of disparate state databases and foster better interagency cooperation.

Amendments to criminalize terrorism finance and to vest the Security Service of Ukraine with authority to investigate terrorism finance have been proposed. The GOU has cooperated with USG efforts to track and freeze the financial assets of terrorists and terrorist organizations. The National Bank of Ukraine (NBU), State Tax Administration, Ministry of Finance, and State Security Service (SBU) are fully aware of U.S. Executive Order (E.O.) 13224 and subsequent updates and addenda to the lists of terrorists and terrorist organizations. All agencies have tracked data that was provided, and have exchanged information. The NBU has issued orders to banks to freeze accounts of individuals or organizations listed in the E.O. and later lists.

The GOU has also taken appropriate steps to implement UN Security Council resolutions relevant to fighting terrorism. The Cabinet of Ministers, on December 22, 1999, issued a resolution ordering agencies and banks to freeze Taliban funds as specified in UNSCR 1267. A Cabinet of Ministers resolution instructed the NBU to order all banks to comply with UNSCR 1333. In response to these measures, the NBU sent letters to regional departments and commercial banks to execute all applicable provisions of UNSCRs 1267 and 1333.

The FMD acknowledges the existence and use of alternative remittance systems such as hawala. FMD personnel have attended seminars and exchanged information about such systems. The FMD and security agencies monitor charitable organizations and other nonprofit entities that might be used to finance terrorism.

The FMD is a viable candidate for joining the Egmont Group of FIUs in 2004, having been successfully vetted by the Egmont Legal Working Group at the June 2003 plenary. The U.S.-Ukraine Treaty on Mutual Legal Assistance in Criminal Matters was signed in 1998 and entered into force in February 2001. A bilateral Convention for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with respect to Taxes on Income and Capital, which provides for the exchange of information in administrative, civil and criminal matters, is also in force.

Ukraine has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Ukraine is a party to the 1988 UN Drug Convention as well as the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, which came into force with respect to Ukraine in January 1998. In January 2002, the European Convention on the Suppression of Terrorism was signed. Ukraine ratified the UN International Convention for the Suppression of the Financing of Terrorism in September 2002. Ukraine also became a signatory to the UN Convention Against Corruption, which has not yet entered into force, on December 11, 2003.

Ukraine has demonstrated considerable political will to combat money laundering by strengthening, clarifying, and implementing its newly adopted laws. As evidenced by the strides made by its FIU, the NBU, and other actors in the financial and legal sectors, Ukraine has clearly shown its ability to implement a comprehensive anti-money laundering regime. The GOU should criminalize the financing and support of terrorists and terrorism. The GOU should adopt an asset forfeiture regime. The GOU should continue to enhance and implement its newly adopted anti-money laundering regime and to work towards NCCT de-listing and accession of its FIU to the Egmont Group of FIUs in 2004.

United Arab Emirates

The United Arab Emirates (UAE), which remains a cash-based society, is considered an important regional financial center for the Gulf region. The financial sector is modern and outward looking. Dubai, in particular, is a major banking center. About 50 million people are projected to pass through Dubai's airport by the year 2010. The UAE's robust economic development and liberal business environment have attracted a massive influx of people and capital. Approximately 80 percent of the UAE population is comprised of nonnationals. Because of the UAE's role as the primary transportation and trading hub for the Gulf states, East Africa, and South Asia, and with expanding

trade ties with the countries of the former Soviet Union, the UAE has the potential to be a major center for money laundering. That potential is exacerbated by the large number of resident expatriates from these areas, many of whom are engaged in legitimate trade with their homelands.

Following the September 11 terrorist attacks in the United States, and revelations that terrorists had moved funds through the UAE, the Emirates' authorities acted swiftly to address potential vulnerabilities and, in close concert with the United States, to freeze the funds of groups with terrorist links, including the Al-Barakat organization, which was headquartered in Dubai. Both federal and emirate-level officials have gone on record as recognizing the threat money laundering activities in the UAE pose to the nation's security and have taken significant steps in 2003 to better monitor cash flows through the UAE financial system.

While the laundering of narcotics funds may take place in the UAE, given the country's close proximity to Afghanistan—where 70 percent of the world's opium is produced—the potential exploitation of the UAE financial system by foreign terrorists and terrorist financing groups is the primary concern.

In January 2002, the President of the United Arab Emirates promulgated Law No. 4 criminalizing all forms of money laundering activities. The law calls for stringent reporting requirements for wire transfers exceeding \$545 and currency importation/exportation limits set roughly at \$11,700. The law imposes stiff criminal penalties (up to seven years in prison and a fine of up to 300,000 dirhams (\$81,700), as well as seizure of assets if found guilty) for money laundering and also provides safe harbor provisions for those who report such crimes. Banks and other financial institutions supervised by the Central Bank (exchange houses, investment companies, and brokerages) are required to follow strict "know your customer" guidelines; all financial transactions over \$54,000, regardless of their nature, must be reported to the Central Bank. Financial institutions also are required to maintain records on transactions for five years.

The Central Bank (CB) announced that it received 633 suspicious transaction reports from August 2001 to August 2003, of which 497 were from banks, 49 from money changers, and 87 from customs departments. Thirteen accounts have been frozen as a result of these STRs.

Money laundering may take place within the formal banking system, including the numerous money exchange houses, but is believed to be largely confined to the informal and largely undocumented "hawala" remittance system. The fact that hawala is an undocumented and nontransparent system, and is highly resilient in response to enforcement and regulatory efforts, makes it difficult to control and an attractive mechanism for terrorist and criminal exploitation. The UAE has begun to make progress in publicly accepting its vulnerability and involvement vis-à-vis hawala. New regulations to improve oversight of the hawala system were implemented in 2002. There is no accurate estimate of the number of UAE-based hawala brokers.

The CB now supervises 61 hawala brokers, which—like other financial institutions in the UAE—are now required to submit sheets containing names and addresses of transferors and beneficiaries to the CB and to complete suspicious transaction reports. The new attention on hawala is encouraging more people to use regulated exchange houses in the UAE. Traders in Dubai's Central Souk (Market) said hawala exchange rates are now only 3 percent cheaper than formal exchange houses, persuading many to use the formal, and more secure, banking network.

The UAE Government (UAEG) also has admitted the need to better regulate "near-cash" items such as gold, jewelry, and gemstones, especially in the burgeoning markets in Dubai. The UAE acceded to the Kimberley Process (KP) in November 2002 and began certifying rough diamonds exported from the UAE on January 1, 2003. The Dubai Metals and Commodities Center (DMCC) is the quasi-governmental organization charged with issuing KP certificates in the UAE, and employs four individuals full-time to administer the KP program. Prior to January 1, 2003, the DMCC circulated a

sample UAE certificate to all KP member states and embarked on a public relations campaign to educate the estimated 50 diamond traders operating in Dubai concerning the new KP requirements.

UAE customs officials may delay or even confiscate diamonds entering the UAE from a KP member country without the proper KP certificate.

The UAE hosted an International Conference on Hawala in May 2002, which was attended by over 300 delegates including government officials, executives of supervisory institutions, banking experts, and law enforcement officials from 58 countries. The conference concluded with the issuance of “The Abu Dhabi Declaration on Hawala,” which calls for the establishment of a sound mechanism to regulate hawala. The CB intends to sponsor a follow-up conference on hawala in April 2004 to assess the effectiveness of hawala registration and documentation requirements that went into effect in November 2002.

The supervision of the UAE banking and financial sector falls under the authority of the CB. The CB issues instructions and recommendations as deemed appropriate and is permitted to take any necessary measure to ensure the integrity of the UAE’s financial system. The CB issues licenses to financial institutions under its supervision and may impose administrative sanctions for compliance violations.

UAE anti-money laundering measures can be found in a series of rules and regulations issued by the CB, and thus are generally applicable to those financial entities that fall under its supervision. There are a number of circulars issued by the CB requiring customer identification and providing for a basic suspicious transaction-reporting obligation. When suspicious activity is reported from a financial institution, the Central Bank is able to freeze suspect funds, make appropriate inquiries, and coordinate with law enforcement officials.

In July 2000, the UAE established the National Anti-Money Laundering Committee, under the Chairmanship of the Central Bank’s Governor, with representatives from the Ministries of Interior, Justice, Finance, and Economy, the National Customs Board, the Secretary General of the Municipalities, the Federation of the Chambers of Commerce, and five major banks and money exchange houses (as observers). It has overall responsibility for coordinating anti-money laundering policy.

Following a review of current practices by the Committee, in November 2000 the CB issued Circular 24/2000, which consolidates and expands anti-money laundering requirements for the financial sector. The circular, which is applicable to all banks, money exchanges, finance companies, and other financial institutions operating in the UAE, provides the procedures to be followed for the identification of natural and juridical persons, the types of documents to be presented, and rules on what customer records must be maintained on file at the institution. Other provisions of Circular 24/2000 call for customer records to be maintained for a minimum of five years, and further require that they be periodically updated as long as the account is open.

With implementation of Law 4/2002 came the establishment of the Anti-Money Laundering and Suspicious Case Unit (AMLSCU), which is located within the CB and acts as the financial Intelligence unit (FIU). Financial institutions under the supervision of the CB are required to report suspicious transactions to the AMLSCU, which is charged with examining them and coordinating the release of information with law enforcement and judicial authorities. It has the authority to request information from foreign regulatory authorities in carrying out its preliminary investigation of suspicious transaction reports. Officials indicate that exchanges with foreign financial intelligence units are possible, provided the exchanges are conducted on a basis of reciprocity. The AMLSCU, which is a member of the Egmont Group, is exploring areas of information sharing with other financial intelligence units. AMLSCU has provided information relating to investigations carried out by international authorities. The Central Bank conducted 58 workshops on money laundering and terrorist finance for banks and other financial institutions in 2003.

The National Anti-Money Laundering Committee issued a Cautionary Notice in the local press to make the general public aware of the possibilities through which terrorist financing could be transacted, and has urged avoidance of such possibilities. UAE has extended full support and cooperation to the UN and U.S. authorities in their efforts to track the accounts of terrorists. Under UNSCR 1267/1390, UAE has frozen accounts of certain organizations and individuals with amounts equal to approximately \$3 million. In addition, a number of money laundering cases involving foreign nationals have been referred to courts. Some cases ended in convictions.

The UAE authorities have arrested two individuals on suspicion of money laundering. This is the first time that the UAE has arrested suspected money launderers since the legislation went into effect; however, the UAEG has frozen financial assets under the law. Likewise, 23 other suspected money laundering cases have been referred to the public prosecutor's office for further review.

The CB has circulated to all financial institutions under its supervision the lists of individuals and entities suspected of terrorism and terrorist financing, included in UN Security Council resolutions. To date, the Central Bank has frozen a total of \$3.13 million in 18 bank accounts in the UAE since 9/11. Additionally, the AMLSCU has provided international organizations and its counterpart FIUs data on 172 cases related to terrorist financing.

In 2002, the UAEG worked in partnership with the United States to block terrorist financing, and froze the assets of more than 150 named terrorist entities—including significant assets in the UAE belonging to the Al-Barakat terrorist financing group.

The UAEG monitors registered charities in the country and requires them to keep records of donations and beneficiaries. The Ministry of Labor and Social Affairs regulates charities and charitable organizations in the UAE. The UAEG is much more sensitive post-9/11 to the oversight of charities and accounting of transfers abroad. In 2002, the UAEG mandated that all licensed charities interested in transferring funds overseas must do so via one of three umbrella organizations: the Red Crescent Authority, the Zayed Charitable Foundation, or the Muhammad Bin Rashid Charitable Trust. These three quasi-governmental bodies are properly managed, and in a position to ensure that overseas financial transfers go to legitimate parties. As an additional step, the UAEG has contacted the governments in numerous aid receiving countries to compile a list of recognized, acceptable recipients for UAE charitable assistance.

The UAE is noted for its growing free trade zones (FTZs). There are well over a hundred multinational companies located in the FTZs with thousands of individual trading companies. The FTZs permit 100 percent foreign ownership, no import duties, full repatriation of capital and profits, no taxation, and easily obtainable licenses. Companies located in the free trade zones are treated as being offshore or outside the UAE for legal purposes. There is little Customs scrutiny of goods going into and out of the free trade zones. The UAE is not an offshore financial center; nonresidents are not permitted to open bank accounts here and offshore banking is prohibited. The UAE is a party to the 1988 UN Drug Convention, and it has entered into a series of bilateral agreements on mutual legal assistance. The UAE is a member of the Gulf Cooperation Council, which is a member of the Financial Action Task Force (FATF). The UAE has been generally receptive to U.S. Government overtures to cooperate on money laundering issues, and has welcomed money laundering-related training and visits by U.S. officials.

The United States and the UAE continue to share information on exchanging records in connection with terrorist financing and other money laundering cases on an ad hoc basis. A Mutual Legal Assistance Treaty (MLAT), which will codify that cooperation, is in the process of being negotiated.

The UAE Government has begun constructing a far-reaching anti-money laundering program. The UAE government has sought to crack down on potential vulnerabilities in the financial markets and is cooperating in the international effort to prevent money laundering, particularly by terrorists.

However, there remain areas requiring further action. Law enforcement and customs officials should begin to take the initiative to recognize money laundering activity and proactively develop cases without waiting for referrals from the AMLSCU. UAE officials should give greater scrutiny to trade based money laundering in all of its forms. The Central Bank should be more diligent in its efforts to encourage hawala dealers to participate in the registration program. The AMLSCU should take a more active role in participating in international anti-money laundering gatherings and increasing its ties with other FIUs.

United Kingdom

The United Kingdom (UK) plays a leading role in European and world finance and remains attractive to money launderers because of the size, sophistication, and reputation of its financial markets. Although drugs are still a major source of illegal proceeds for money laundering, the proceeds of other offenses, such as financial fraud and the smuggling of people and goods, have become increasingly important. The past few years have witnessed the movement of cash placement away from High Street banks and mainstream financial institutions. Criminals continue to use bureaux de change, cash smuggling into and out of the UK, gatekeepers (including solicitors and accountants), and the purchase of high-value assets as disguises for illegally obtained money.

The UK has implemented the provisions of the European Union's two Directives on the prevention of the use of the financial system for the purpose of money laundering and the Financial Action Task Force (FATF) Forty Recommendations on Money Laundering. Narcotics-related money laundering has been a criminal offense in the UK since 1986. The laundering of proceeds from other serious crimes is criminalized by subsequent legislation. Banks and nonbank financial institutions in the UK must report suspicious transactions.

In November 2001, money laundering regulations were extended to money service bureaus (e.g., bureaux de change, money transmission companies). As of January 1, 2004, more sectors are subject to formal suspicious transaction reporting (STR) requirements, including attorneys, solicitors, accountants, real estate agents, and dealers in high-value goods such as cars and jewelry. Sectors of the betting and gaming industry that are not currently regulated are being encouraged to establish their own codes of practice, including a requirement to disclose suspicious transactions.

On July 24, 2002, the Proceeds of Crime Act 2002 was enacted, and it went into force on January 1, 2003. The final regulations will take effect on March 1, 2004. It creates, for the regulated sector, a new imprisonable offense of failing to disclose suspicious transactions in respect to all crime, not just narcotics- or terrorism-related crimes, as was the case previously. Along with the Act came an expansion of investigative powers relative to large movements of cash in the United Kingdom. In light of this, Her Majesty's (HM) Customs has increased its national priorities to include investigating the movement of cash through money exchange houses, and identifying unlicensed money remitters. A total of \$28.5 million in cash seizures was made under the new act in 2003.

The UK's banking sector provides accounts to residents and nonresidents, who can open accounts through private banking activities and various intermediaries that often advertise on the Internet and also offer various offshore services. Private banking constitutes a significant portion of the British banking industry. Both resident and nonresident accounts are subject to the same reporting and record keeping requirements. Individuals typically open nonresident accounts for a tax advantage or for investment purposes.

Bank supervision falls under the Financial Services Authority (FSA). The FSA's primary responsibilities are in areas relating to the safety and soundness of the institutions in its jurisdiction. The FSA also plays an important part in the fight against money laundering through its continued involvement in the authorization of banks, and investigations of money laundering activities involving

banks. The FSA administers a civil-fines regime and has prosecutorial powers. The FSA has the power to make regulatory rules with respect to money laundering, and to enforce those rules with a range of disciplinary measures (including fines) if the institutions fail to comply.

In December 2003, the FSA fined Abbey National, the UK's sixth largest bank, 2.3 million British pounds (approximately \$4.2 million), for "extremely serious failings" in its anti-money laundering procedures during the period 2001-2003. According to the FSA, Abbey National was cited for failure to report suspicious banking transactions in a timely manner, as well as failure to carry out proper identity checks on new customers.

STRs are filed with the Financial Intelligence Division (FID), formerly the Economic Crime Bureau, of the National Criminal Intelligence Service (NCIS). The NCIS serves as the UK's financial intelligence unit (FIU). The FID analyzes reports, develops intelligence, and passes information to police forces and HM Customs and Excise for investigation. In 2001, the FID received approximately 32,000 STRs, and 65,000 STRs in 2002. The FID estimates it will receive roughly 100,000 STRs in 2003.

The Proceeds of Crime Act 2002 enhances the efficiency of the forfeiture process and increases the recovered amount of illegally obtained assets. The Act consolidates existing laws on forfeiture and money laundering into a single piece of legislation, and, perhaps most importantly, creates a civil asset forfeiture system for the proceeds of unlawful conduct. It also creates the Assets Recovery Agency (ARA), to enhance the financial investigators' power to request information from any bank about whether it holds an account for a particular person. The Act provides for confiscation orders related to people who benefit from criminal conduct, and for restraint orders to prohibit dealing with property. It also allows for the recovery of property that is, or represents, property obtained through unlawful conduct, or that is intended to be used in unlawful conduct. Furthermore, the Act shifts the burden of proof to the holder of the assets (for example, to prove that the assets were acquired through lawful means). In the absence of such proof, assets may be forfeit, even without a criminal conviction. The Act gives standing to overseas requests and orders concerning property believed to be the proceeds of criminal conduct. The Act also provides the ARA with a national standard for training investigators, and gives greater powers of seizure at a lower standard of proof. Officials at the ARA reported that a total of \$28.5 million (16.2 million British pounds) in cash seizures had been made under the Act as of December 2003.

The Terrorism (United Nations Measures) Order 2001 makes it an offense for any individual, without a license from the Treasury, to make any funds for financial or related services available, directly or indirectly, to, or for the benefit of, a person who commits, attempts to commit, facilitates, or participates in the commission of acts of terrorism. The Order also makes it an offense for a bank or building society to fail to disclose to the Treasury a suspicion that a customer or entity, with whom the institution has had dealings since October 10, 2001, is attempting to participate in acts of terrorism. The Anti-Terrorism, Crime, and Security Act 2001 provides for the freezing of assets.

As a direct result of the events of September 11, 2001, the FID established a separate Terrorist Finance Team (TFT) to maximize the effect of reports from the regulated sector. The TFT chairs a law enforcement group to provide outreach to the financial industry concerning requirements and typologies. The operational unit that responds to the work and intelligence development of the TFT has seen a threefold increase in staffing levels directly due to the workload. The Metropolitan Police responded to the growing emphasis on terrorist financing by expanding the focus and strength of its specialist financial unit dedicated to this area of investigations. This unit is now called the National Terrorist Financing Investigative Unit (NTFIU).

In 2003, the UK issued 21 terrorist asset freeze orders on 72 individuals and 16 organizations. Two of the orders implemented the European Union's September 2003 decision to freeze all funds, other financial assets, and economic resources of Hamas. On November 19, 2002, Chancellor Gordon

Brown ordered financial institutions in the UK to freeze funds belonging to the Benevolence International Foundation (BIF). BIF's Chief Executive, Enaam Arnaout, a Syrian-born U.S. citizen, was indicted in the United States for running a racketeering enterprise, conspiracy to launder money, money laundering, wire and mail fraud, and providing material support to organizations, including Usama Bin Ladin's terror network.

The UK cooperates with foreign law enforcement agencies investigating narcotics-related financial crimes. The UK is a party to the 1988 UN Drug Convention. The UK ratified the UN International Convention for the Suppression of the Financing of Terrorism on March 7, 2001. In December 2000, the UK signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. The UK is a member of the FATF and the European Union. The NCIS is an active member of the Egmont Group and has information sharing arrangements in place with the FIUs of the United States, Belgium, France, and Australia. The Mutual Legal Assistance Treaty (MLAT) between the UK and the United States has been in force since 1996. The United States and UK recently negotiated an asset sharing agreement that is awaiting signature by the appropriate parties. The UK also has an MLAT with the Bahamas. Additionally, there is an MOU between the U.S. Customs Service and HM Customs and Excise.

The UK should continue the strong enforcement of its comprehensive anti-money laundering/counterterrorist financing program and its active participation in international organizations to combat the domestic and global threat of money laundering and the support and financing of terrorists and their organizations.

Uruguay

In the past, Uruguay's strict bank secrecy laws, liberal currency exchange regulations, and overall economic stability made it vulnerable to money laundering, although its extent and exact nature were unknown. In 2002, however, banking scandals and mismanagement, along with massive withdrawals of Argentine deposits led to a near collapse of the Uruguayan banking system, and an end to Uruguay's role as a regional financial center. The near collapse likely explains the diminished attractiveness of Uruguayan financial institutions to money launderers in the region.

Over the last five years, the Government of Uruguay (GOU) has instituted several legislative and regulatory reforms in connection with the further consolidation of its anti-money laundering program. In May 2001, it enacted Law 17,343, which extended the predicate offenses for money laundering beyond narcotics trafficking and corruption to include terrorism, smuggling (above the threshold of \$20,000); illegal trafficking in weapons, explosives and ammunition; trafficking in human organs, tissues or medications; trafficking in human beings; extortion; kidnapping; bribery; trafficking in nuclear and toxic substances; and illegal trafficking in animals or antiques. The courts have the power to seize and later confiscate property, products or financial instruments linked to money laundering activities. In December 2003, the Uruguayan Chamber of Representatives approved a bill designed to limit bank secrecy and confidentiality. The bill is specifically intended to increase credit transparency by eliminating bank secrecy for information pertaining to personal loans, financial credits, mortgages, or similar obligations. The bill does not, however, lift bank secrecy for law enforcement investigations regarding money laundering or terrorist finance.

Several government bodies seek to combat money laundering. The President's Vice-Minister of the Presidency heads the National Drug Board, which is the senior authority directing anti-money laundering policy. The Center for Training on Money Laundering serves as a forum for discussion and advice on policy as well as allowing private sector input. In 2000, the Financial Information and Analysis Unit (UIAF), was created within the Superintendence of Financial Intermediation Institutions that has the responsibility of coordinating all anti-money laundering efforts. The UIAF is Uruguay's Financial Intelligence Unit (FIU). It receives, analyzes, and remits to judicial authorities suspicious

transaction reports for possible investigation. Central Bank Circular 1722 enables the UIAF to respond to requests from foreign analogs.

The Ministry of Finance and Economics, the Ministry of the Interior (via the police force), and the Ministry of Defense (via the Naval Prefecture) also participate in anti-money laundering efforts. The private sector has also developed self-regulatory measures against money laundering such as the Codes of Conduct approved by the Association of Banks and the Chamber of Financial Entities (in 1997), the Association of Exchange Houses (2001), and the Securities Market (2002).

Money laundering is considered a crime separate from underlying crimes such as narcotics trafficking, administrative corruption, terrorism or smuggling, which are formally listed in the legal statutes. The court can confiscate or preventively impound assets; proceeds or instruments used or intended to be used in money laundering crimes. Real estate ownership is registered in the name of the titleholder. However, ownership of a specific property cannot not be traced unless the “pardon”—the identification number of the property in the registry—is known. This system makes tracking money laundering in this important sector extremely difficult, particularly in the partially foreign-owned tourist industry around Punta del Este.

Safeguarding the financial sector from money laundering activities is a priority for the GOU. A series of Central Bank regulations require banks (including offshore), currency exchange houses, and stockbrokers to implement anti-money laundering policies, including the recording in internal databases transactions over \$10,000, and the reporting of suspicious transactions to the UIAF. In addition, the insurance and reinsurance sector, stock market, and currency exchange houses must know and thoroughly identify their customers, and report suspicious financial transactions to UIAF. The insurance sectors are further required to maintain a registry of “relevant” transactions, such as payments of insurance premiums of \$10,000 or more, while stock and investment fund administrators must maintain a registry of individuals and entities exchanging currency or other valuables in amount greater than \$10,000. There are twelve offshore banks and six offshore mutual fund companies.

The offshore banks are subject to the same laws and regulations as local banks, and are required to be licensed by the GOU—a process involving background checks on license applicants. There are no records of the number of Uruguayan offshore firms or shell companies, although, a large number are believed to exist. Offshore trusts are not allowed. Bearer shares may not be used in banks and institutions under the authority of the Central Bank, and any share transactions must be authorized by the Central Bank.

Uruguay has been a member of the Financial Action task force for South America (GAFISUD) since its inception in December 2000 and served as its President in 2003. GAFISUD Mutual evaluation report stated that Uruguay’s anti-money laundering regime meets the FATF 40 recommendations. The report also recognized Uruguay’s efforts to train public and private sector players in money laundering-related issues. While Uruguay’s past role as a financial center put it at risk of becoming a money laundering center, the mutual evaluation team did not find any major money laundering criminal activity producing economic profits. The report included several suggestions to expand the scope of Uruguayan money laundering legislation as it relates to gambling, real estate, certain professions (primarily in the legal and financial services sectors), and the smuggling of cash and securities. It also suggested the Government of Uruguay

Uruguay remains active in international anti-money laundering efforts. In addition to its membership in GAFISUD, Uruguay is also a member of the OAS Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering. The USG and the GOU are parties to an extradition treaty and a mutual legal assistance treaty that entered into force in 1984 and 1994, respectively. It is a party to the 1988 UN Drug Convention. Uruguay has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and became a party to the UN International Convention for the Suppression of the Financing of Terrorism on January 8, 2004. In

addition, for 2004 Uruguay holds the presidency of the Interamerican Committee against Terrorism (CICTE).

The GOU should take steps necessary to bring it into compliance with the FATF Special Eight Recommendations on Terrorist Financing including the criminalizing of terrorist financing. The GOU should enact legislation that requires the identification and registration of real estate—a sector particularly vulnerable to money laundering. Effective implementation and enforcement of anti-money laundering measures must remain a priority for the GOU in order to eliminate the potential for money laundering and terrorist financing activities throughout its financial sector. Uruguay should become a party to the UN Convention against Transnational Organized Crime.

Uzbekistan

Uzbekistan is not considered an important regional financial center and does not have a developed financial system. Reportedly, Uzbek citizens and residents attempt to avoid using the official banking system for transactions, except when required by law. There is little trust in current financial controls and fear that the Government of Uzbekistan (GOU) may seize one's assets. In Uzbekistan, the majority of the population holds savings in the form of cash stored at home. There is a significant black market for smuggled goods in Uzbekistan. Contraband and narcotics smuggling generates illicit funds that are not laundered through the official banking system. Since the GOU imposed a restrictive trade and import regime in mid-2002, the smuggling of consumer goods increased dramatically. Many Uzbek citizens make a living by shuttle-trading goods from neighboring countries, Iran, the Middle East, India, Korea, Europe, and the United States. The basically un-reported and un-monitored trade is very susceptible to trade-based money laundering. According to the GOU, nonbank financial crimes, such as the over invoicing for procurements, have increased substantially. It is thought that narcotic traffickers also exchange their proceeds on the black market, allowing small-scale business people access to drug dollars. As in neighboring countries, narcotics can also act as a commodity, and they are frequently bartered or traded for desired goods. Illicit proceeds are often carried across Uzbekistan's borders for deposit in other countries' banking systems, such as in Kazakhstan, Russia, or the United Arab Emirates. The proceeds of narcotics trafficking are controlled by local and regional drug-trafficking organizations.

Though Uzbekistan has formally removed currency exchange controls, in practice, obtaining currency conversion for a moderate to large sum of money remains difficult. This system inadvertently encourages the use of alternate remittance systems. Cash proceeds of crime denominated in the local currency, the soum, can easily be converted into other currencies on the black market. Residents and nonresidents may bring the equivalent of \$10,000 into the country tax-free. Amounts in excess of this limit are assessed a one percent duty. Nonresidents may take out as much currency as they brought into the country. However, residents are limited to the equivalent of \$1,500. Nonetheless, foreign currency is readily available to criminals, via the thriving black market.

There appears to be little money laundering through formal financial institutions in Uzbekistan in large part due to the extremely high degree of supervision and control exercised by the Central Bank of Uzbekistan, the Ministry of Finance, and the state-owned and controlled banks. The GOU has anti-money laundering legislation. Though not legislatively mandated, banks are required to know, record and report the identity of customers engaging in significant transactions, including the recording of large currency transactions at thresholds appropriate to Uzbekistan's economic situation. The Central Bank unofficially requires commercial banks to report on private transfers to foreign banks that exceed \$10,000. Institutions must report suspicious transactions immediately, via phone call and follow up memorandum to the Central Bank of Uzbekistan. Depending on the type of transaction, banks are required to maintain records for time deposits for a minimum of three years, generally not an adequate period to reconstruct suspect transactions. Money laundering controls are not applied to nonbanking

financial institutions such as exchange houses, stock brokerages, casinos, insurance companies or professional intermediaries such as lawyers and accountants.

In September 2003, Uzbekistan enacted a bank secrecy law that prevents the disclosure of client and ownership information to bank supervisors and law enforcement authorities for domestic and offshore financial services companies. Private bank information can be disclosed to prosecution and investigative authorities, provided there is a criminal investigation underway. The information can be provided to the courts on the basis of a written request in relation to cases currently under consideration. Protected banking information can also be disclosed to tax authorities in cases involving the taxation of a bank's client.

Article 41 of the Law on Narcotic Drugs and Psychotropic substances (1999) stipulates that any institution may be closed for performing a financial transaction for the purpose of legalizing (laundering) proceeds derived from illicit traffic in narcotic drugs and psychotropic substances. Article 243 of the Criminal Code imposes penalties for the legalization of proceeds derived from criminal activity, i.e. five to ten years of imprisonment. This article also defines the act of money laundering. It includes transfer, conversion, exchange, as well as concealing of origin, true nature, source, location, disposition, movement and rights with respect to the assets derived from criminal activity as punishable acts.

In accordance with Uzbekistan's Code of Criminal Procedure, investigation of money laundering offenses falls under the jurisdiction of the Ministry of Internal Affairs. The Department of Investigation of Economic Crimes within the Ministry conducts investigations of all types of economic offenses. There are also specialized structures within the National Security Service and the Department on Combating Economic Crimes and Corruption in the Office of the Prosecutor-General, which are also authorized to conduct investigation of, inter alia, money laundering offenses.

Uzbekistan has established systems for identifying, tracing, freezing, seizing, and forfeiting proceeds of narcotics and other money laundering related crimes. Since 2000, at least 200 million soum in assets have been seized. At that time, a special fund was established that directs the assets derived from the sale of confiscated proceeds and instruments of drug related offenses. The fund supports entities of the National Security Service, the Ministry of Interior, the State Customs Committee, and the Border Guard Committee, all of which are directly involved in combating illicit drug trafficking. A total of 42 million soum (approximately \$35-40,000) has been distributed by this fund since it was established.

Article 155 of Uzbekistan's criminal code and Law Number 167 "On Fighting Terrorism" of 15 December 2000 criminalizes terrorist financing. These laws were designed to provide for the security of individuals, society, and the state from terrorism; protection of territorial integrity and state sovereignty; preserving civil peace; and preventing ethnic strife. The National Security Service (NSS), the Ministry of Internal Affairs (MVD) the Committee on the Protection of State Borders, the State Customs Committee, the Ministry of Defense and the Ministry for Emergency Situations are designated as responsible for implementing the antiterrorist legislation. The law names the NSS as the coordinator for government agencies fighting terrorism.

The GOU has the authority to identify, freeze, and seize terrorist assets. The banking community, which is entirely state controlled and, with few exceptions, state-owned, generally cooperates with efforts to trace funds and seize accounts. Uzbekistan has circulated to its financial institutions the list of individuals and entities that have been included on the UN 1267 sanction list.

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

Uzbekistan should continue to refine its anti-money laundering and terrorist financing legislation to world standards. Uzbekistan should establish a suspicious activity reporting system from bank and nonbank financial institutions and a Financial Intelligence Unit (FIU) to analyze the reports and disseminate them for investigation. Uzbekistan authorities need to do more to combat smuggling and trade based money laundering.

Vanuatu

Vanuatu's offshore sector is vulnerable to money laundering, as it has historically maintained strict secrecy provisions that have the effect of preventing law enforcement agencies from identifying the beneficial owners of offshore entities registered in the sector. Due to allegations of money laundering, a few United States-based banks announced in December 1999 that they would no longer process U.S. dollar transactions to or from Vanuatu. The Government of Vanuatu (GOV) responded to these concerns by introducing reforms designed to strengthen domestic and offshore financial regulation.

Vanuatu's financial sector includes five licensed banks (that carry on domestic and offshore business) and 60 credit unions, regulated by the Reserve Bank of Vanuatu. The Financial Services Commission (FSC) regulates the offshore sector that includes 55 banks and approximately 2,500 "international companies" (i.e., international business companies or IBCs), as well as offshore trusts and captive insurance companies. IBCs may be registered using bearer shares, shielding the identity and assets of beneficial owners of these entities. Secrecy provisions protect all information regarding IBCs and provide penal sanctions for unauthorized disclosure of information. These secrecy provisions, along with the ease and low cost of incorporation, make IBCs ideal mechanisms for money laundering and other financial crimes.

As of January 1, 2003, the Reserve Bank of Vanuatu has regulated Vanuatu's 55 offshore banks, formerly regulated by the FSC. This requirement was one of many recommendations of the 2002 International Monetary Fund Module II Assessment Report (IMFR) that found Vanuatu's onshore and offshore sectors to be "noncompliant" with many international standards.

The Financial Transaction Reporting Act (FTRA) of 2000 established Vanuatu's Financial Intelligence Unit (FIU) within the State Law Office. The FIU receives suspicious transaction reports (STRs) filed by banks and distributes them to the Public Prosecutor's Office, the Reserve Bank of Vanuatu, the Vanuatu Police Force, the Vanuatu Financial Services Commission, and law enforcement agencies or supervisory bodies outside Vanuatu. The FIU also issues guidelines to, and provides training programs for, financial institutions regarding record keeping for transactions and reporting obligations. The Act also regulates how such information can be shared with law enforcement agencies investigating financial crimes. Financial institutions within Vanuatu must establish and maintain internal procedures to combat financial crime. Every financial institution is required to keep records of all transactions. Five key pieces of information are required to be kept for every financial transaction: the nature of the transaction, the amount of the transaction, the currency in which it was denominated, the date the transaction was conducted, and the parties to the transaction.

The IMFR noted several weaknesses in Vanuatu's anti-money laundering regime. Consequently, the government of Vanuatu (GOV) has prepared a policy paper currently being considered by the Council of Ministers for tabling by the parliament in mid-2004. The amendments to the FTRA would require mandatory customer identification requirements, broaden the range of covered institutions required to file STRs to include auditors, trust companies, company service providers and provide safe harbor for both individuals and institutions required to file STRs. The proposed amendments would override any extant banking and or other secrecy provisions and clarify the FIU's investigative powers.

Regulatory agencies in Vanuatu have instituted stricter procedures for issuance of offshore banking licenses, and continue to review the status of previously issued licenses. All financial institutions, both

domestic and offshore, are required to report suspicious transactions and to maintain records of all transactions for six years, including the identities of the parties involved.

The Serious Offenses (Confiscation of Proceeds) Act 1989 criminalized the laundering of proceeds from all serious crimes and provided for seizure of criminal assets and confiscation after a conviction. The new Proceeds of Crime Act (2002) retains the criminalization of the laundering of proceeds from all serious crimes, criminalizes the financing of terrorism and, includes full forfeiture and restraining, monitoring and production powers regarding assets.

Vanuatu passed the Mutual Assistance in Criminal Matters Act in December 2002 for the purpose of facilitating the provision of international assistance in criminal matters for the taking of evidence, search and seizure proceedings, forfeiture or confiscation of property, and restraint of dealings in property that may be subject to forfeiture or seizure. The Attorney General possesses the authority to grant requests for assistance, and may require government agencies to assist in the collection of information pursuant to the request. The Extradition Act of 2002 includes money laundering within the scope of extraditable offenses.

The amended International Banking Act has now placed Vanuatu's international and offshore banks under the supervision of the Reserve Bank of Vanuatu. Section 5(5) of the Act states that if existing licensees wish to carry on international banking business after December 31, 2003, the licensee should have submitted an application to the Reserve Bank of Vanuatu under section 6 of the Act for a license to carry on international banking business. If an unregistered licensee continues to conduct international banking business after December 31, 2003, it will be in contravention of section 4 of the Act, and, if found guilty, the licensee will be subject to a fine and/or imprisonment in the case of an individual. Under section 19 of the Act, the Reserve Bank can conduct investigations where it suspects that an unlicensed person/entity is carrying on international banking business. One of the most significant requirements of the amended legislation is the banning of "shell" banks. As of January 1, 2004, all offshore banks registered in Vanuatu must have a physical presence in Vanuatu, and management, directors and employees must be in residence. At the September 2003 APG Plenary, Vanuatu noted its intention to draft new legislation regarding trust companies and company service providers. The new legislation will cover disclosure of information with other regulatory authorities, capital and solvency requirements and fit and proper requirements. Additionally, Vanuatu is drafting legislation to comply for compliance with standards set by the International Associations of Insurance Supervisors.

The E-Business Act No. 25 of 2000 and the Interactive Gaming Act No. 16 of 2000 regulate e-commerce. Section 5 of the E-Business legislation permits the establishment of a Vanuatu-based website where business can be conducted without residency, directors, shareholders, or a registered office. Reportedly, the E-Business Act requires online operations to maintain stringent customer identification and record keeping requirements, as well as reporting suspicious transactions. The Financial Transaction Reporting Act of 2000 applies to e-commerce or businesses by defining any company listed under the Vanuatu Interactive Gaming Act 2000 as a financial institution.

In April 2002, the Organization for Economic Cooperation and Development (OECD) launched an initiative to address harmful tax practices worldwide. Vanuatu was one of seven countries listed as an "uncooperative tax haven". In January 2004, the OECD revealed that it has removed Vanuatu from its list of "uncooperative tax havens," following Vanuatu's earlier announcement that it will implement measures under the Harmful Tax Initiative. The OECD stated in a news release that it welcomes the commitment that Vanuatu has made to improve the transparency of its tax and regulatory systems and to establish, by December 2005, effective exchange of information for tax matters with OECD countries. This move by OECD has made Vanuatu the first country to secure removal from the list of uncooperative tax havens.

Vanuatu is a member of the Asia/Pacific Group on Money Laundering, the Offshore Group of Banking Supervisors, the Commonwealth Secretariat, and the Pacific Island Forum. The Financial Intelligence Unit became a member of the Egmont Group in June 2002. Vanuatu should immobilize bearer shares, require complete identification of the beneficial ownership of IBCs, and implement all provisions of its newly enacted Proceeds of Crime Act, and enact all necessary legislation for its onshore and offshore financial sectors that would bring both sectors into compliance with international standards. Vanuatu should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism, the Convention against Transnational Organized Crime and the 1988 UN Drug Convention

Venezuela

Venezuela is not a regional financial center, nor does it have an offshore financial sector. The relatively small but modern banking sector, which consists of 52 banks, primarily serves the domestic market. Venezuela's proximity to drug producing countries, weaknesses in its anti-money laundering system, and corruption, continue to make Venezuela particularly vulnerable to money laundering. The main source of money laundering in Venezuela stems from proceeds generated by Colombia's cocaine and heroin trafficking organizations. Reportedly, some money is laundered through the real estate market in its Margarita Island free trade zone.

The 1993 Organic Drug Law provides the only legal mechanism for the investigation and prosecution of money laundering crimes. Under this law, a direct connection between the illegal drugs and the proceeds must be proven to establish a money laundering offense. The Government of Venezuela (GOV) freezes assets of individuals charged in international drug trade or money laundering cases directly related to narcotics trafficking. If a conviction is obtained, the frozen assets are turned over to the Ministry of Finance for use in drug demand reduction programs. After the introduction of a new Code of Criminal Procedure in 1999, responsibility for initiating these actions shifted from judges to prosecutors. Due to prosecutors' unfamiliarity with the accusatory judicial system, as well as their having to assume the burden of tens of thousands of backlogged cases, the number of cases resulting in seizure of trafficker assets has decreased.

To expand the predicate offenses for money laundering beyond activities involving the illicit drug trade, the GOV introduced the Organic Law against Organized Crime bill in 2002. Under this bill, money laundering is made a separate, autonomous offense, with no drug nexus required, and those who cannot establish the legitimacy of possessed or transferred funds, and who have awareness of the illegitimate origins of those funds, would be guilty of money laundering. The bill broadens assets forfeiture and sharing provisions, adds conspiracy as a criminal offense, strengthens due diligence requirements, establishes a fully autonomous financial intelligence unit (FIU), and provides law enforcement with stronger investigative powers by authorizing the use of modern investigative techniques such as the use of undercover agents. Although 97 of its 150 articles were approved in 2002, not a single additional article was passed in 2003. The bill remains in its final reading at the National Assembly. If the Organized Crime bill is ultimately enacted, the GOV would meet the requirements of the 1998 Vienna Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime, all of which the GOV has ratified.

Under Resolution 333-97 of 1997, entitled "Standards for the Prevention, Control, and Prosecution of Money Laundering," the Superintendence of Banks and Other Financial Institutions (SUDEBAN) has implemented controls to prevent and investigate money laundering. These include stricter customer identification requirements and the reporting of currency transactions and suspicious activity. These controls apply to all banks (commercial, investment, mortgage, private), savings and loan institutions, currency exchange houses, money remitters, money market funds, capitalization companies, and

frontier foreign currency dealers. The institutions are also required to file reports with Venezuela's FIU, the Unidad Nacional de Inteligencia Financiera (UNIF), created under the SUDEBAN in July 1997.

The UNIF receives suspicious activity reports (SARs) and reports of currency transactions exceeding 4.5 million bolívares (approximately \$2,800) from institutions regulated by SUDEBAN, the Office of the Insurance Examiner, the National Securities and Exchange Commission, the Bureau of Registration and Notaries, the Central Bank of Venezuela, and the Bank Deposits and Protection Guarantee Fund. Some institutions regulated by SUDEBAN, such as tax collection entities and public service payroll agencies, are exempt from the reporting requirement. SUDEBAN also allows certain customers of financial institutions—those who demonstrate “habituality” in the types and amounts of transactions they conduct—to be excluded from currency transaction reports filed with the UNIF. In addition to filing SARs and currency transaction reports, the UNIF also receives reports on the transfer of foreign currency exceeding \$10,000, the sale and purchase of foreign currency exceeding \$10,000, and summaries of cash transactions by states, exceeding 4.5 million bolívares. The Venezuelan Association of Currency Exchange Houses (AVCC), which counts all but one of the country's money exchange companies among its membership, voluntarily complies with the same reporting standards as those required of banks, including the reporting of suspicious transactions. Each currency exchange house in the country has and employs systems to electronically transmit transaction reports to SUDEBAN.

The UNIF analyzes SARs and other reports, and refers those deemed appropriate for further investigation to the Public Ministry (the Office of the Attorney General). The Public Ministry subsequently opens and oversees the criminal investigation. The Venezuelan Constitution guarantees the right to bank privacy and confidentiality, but in cases under investigation by the UNIF, SUDEBAN or the Public Ministry, or by order of the Judge of Control, bank secrecy may be waived. Comprehensive financial and law enforcement information is available to the UNIF.

Lacking the legal basis to employ modern investigative techniques, with appropriate legal safeguards, Venezuelan law enforcement authorities find it difficult if not impossible to investigate and prosecute sophisticated criminal organizations and complex crimes such as money laundering. No law enforcement offices have dedicated specific resources to investigating and prosecuting money laundering. There is no special prosecutorial unit for the prosecution of money laundering cases under the Public Ministry, which is the only entity legally capable of initiating money laundering investigations. Currently only the drug prosecutors conduct money laundering investigations. There are only 20 drug prosecutors for all of Venezuela, most of whom lack the technical financial experience to successfully prosecute money laundering investigations, and there are no financial analysts or forensic accountants dedicated to assisting them with the preparation of their cases. Indeed, there have only been three money laundering convictions in Venezuela since 1993, and all of them were narcotics related.

Current Venezuelan law does not specifically mention crimes of terrorism. The Organized Crime Bill would rectify this by defining terrorist activities and establishing punishments of up to 20 years in prison. The Bill's expanded definition of money laundering would also make it possible to prosecute those engaged in terrorism financing and to freeze and seize their assets.

The UNIF has been a member of the Egmont Group since 1999 and has signed bilateral information exchange agreements with counterparts worldwide. Venezuela participates in the Organization of American States Inter-American Commission on Drug Abuse Control (OAS/CICAD) Experts Group to Control Money Laundering, is a member of the Caribbean Financial Action Task Force (CFATF), and the Multilateral Working Group against the Black Market Peso Exchange System and as of July 2003, became a member of GAFISUD, the South American Financial Task Force.

Venezuela is a party to the 1988 UN Drug Convention and ratified the UN Convention against Transnational Organized Crime, which entered into force on September 29, 2003. On September 23, 2003, the GOV ratified the UN International Convention for the Suppression of the Financing of Terrorism. The GOV has signed the UN Convention Against Corruption.

The GOV continues to share money laundering information with U.S. law enforcement authorities under the 1990 antidrug money laundering agreement. The information shared has supported U.S. domestic operations, resulting in the seizure of significant amounts of money and several arrests in the United States.

The GOV should enact measures including the criminalization of terrorist financing as well as institute measures to expedite the freezing of terrorist assets. The GOV should enact the Organic Law Against Organized Crime to provide law enforcement and judicial authorities the much-needed tools for the effective investigation and prosecution of money laundering derived from all serious crimes.

Vietnam

Vietnam is not an important regional financial center. The Vietnamese banking sector is underdeveloped and the Government of Vietnam (GVN) controls the flow of all U.S. dollars in official channels. The nature of the banking system makes it unlikely that major money laundering or terrorist financing is currently occurring in financial institutions. The “drug economy” exists in Vietnam’s informal financial system. Vietnam has a large “shadow economy” in which U.S. dollars and gold are the preferred currency. Due to the limited size of Vietnam’s banking system and currency exchange controls, even legitimate businesses carry on transactions in this “shadow economy”. In addition, Vietnamese regularly transfer money through gold shops and other informal mechanisms to remit or receive funds from overseas. Officially, expatriate remittances account for \$2.5 billion U.S. dollars and unofficially the number may be more than double that amount. It is believed that a percentage of transactions in the formal and alternative remittance systems result from narcotics proceeds.

Although Vietnam does not yet have a separate law on money laundering or terrorist financing; it is currently working on anti-money laundering legislation, that is being circulated among ministries and agencies for their comment and input. In addition, Article 251 of the Amended Penal Code criminalizes money laundering. The Counter-narcotics Law, which took effect June 1, 2001, makes two narrow references to money laundering in relation to drug offenses: it prohibits the “legalizing” (i.e. laundering) of monies and/or property acquired by committing drug offenses (article 3.5); and it gives the Ministry of Public Security’s specialized counternarcotics agency the authority to require disclosure of financial and banking records when there is a suspected violation of the law. The implementing regulations have not yet been promulgated. The State Bank of Vietnam, which has the lead on countering terrorist financing, can also request the disclosure of information when it believes that a transaction might fall within this category. Furthermore, the State Bank requires banks to report suspicious transactions of any kind.

International financial institutions and other donors have been working with the Government of Vietnam on draft banking legislation. The GVN is also working with international agencies to increase its banking supervision capabilities.

The Government of Vietnam is a party to the UN International Convention for the Suppression of the Financing of Terrorism. The GVN has signed the UN Convention against Transnational Organized Crime. The GVN should pass separate terrorist financing legislation if it is not included in the current anti-money laundering draft legislation that is expected to cover all serious crimes. The GVN should also establish cross border currency controls and regulate the use of gold as an alternative remittance system.

Yemen

The Yemeni financial system is not yet well developed. Thus, the extent of money laundering is not known. The prevalence of hawala makes Yemen vulnerable to money laundering. The banking sector is relatively small with 17 commercial banks, including three Islamic banks. The Central Bank of Yemen (CBY) supervises the country's banks. Local banks account for approximately 62 percent of the total banking activities, while foreign banks cover the other 38 percent.

Yemen's parliament passed a comprehensive anti-money laundering legislation in April 2003. The legislation criminalizes money laundering for a wide range of crimes, including narcotics offenses, kidnapping, embezzlement, bribery, fraud, tax evasion, illegal arms trading, and money theft, and imposes penalties of three to five years of imprisonment. There is no specific legislation relating to counterterrorist financing in Yemen. But terrorism is covered in various pieces of legislation that treat terrorism and its financing as serious crimes.

The April 2003 law requires banks, financial institutions, and precious commodity dealers to verify the identity of persons and entities that desire to open accounts or deal with them, to keep records of transactions for up to ten years, and to report suspicious transactions. In addition, the law requires that reports be submitted to an information-gathering unit within the CBY. The unit acts as the financial intelligence unit (FIU), which in turn will report to the Anti-Money Laundering Committee (AMLC). The AMLC is composed of representatives from the Ministries of Finance, Justice, Interior, and Industry and Commerce, the CBY, and the board of banks, and is authorized to issue regulations and guidelines and provide training workshops related to combating money laundering efforts.

Several training workshops on the new legislation have been conducted by the CBY in 2003. The law grants the AMLC the right to exchange information with foreign entities. The head of the committee can ask local judicial authorities to enforce foreign court verdicts based on reciprocity. Also, the law permits the extradition of non-Yemeni criminals in accordance with international treaties or bilateral agreements.

Prior to passage of the anti-money laundering law, in April 2002, the CBY issued Circular 22008, informing banks and financial institutions that they must verify the legality of all proceeds deposited in or passing through the Yemeni banking system. The circular stipulates that financial institutions must positively identify the place of residence of all persons and businesses that establish relationships with them. The circular also requires that banks verify the identity of persons or entities that wish to transfer more than \$10,000 through banks at which they have no accounts. The same provision applies to beneficiaries of such transfers. Banks must also take every precaution when transactions appear suspicious, and report such activities to the CBY. The circular was distributed to the banks along with a copy of the Basel Committee's "Customer Due Diligence for Banks," concerning "Know Your Customer" procedures.

In 2003, DHS/ICE agents in New York conducted an investigation of a company suspected to be involved in the smuggling and distribution of pseudoephedrine. The investigation disclosed employees at the business were sending a large number of negotiable checks to Sana, Yemen. Analysis of the documents seized as a result of search warrants and bank records revealed that the suspects had also wire transferred money to an individual with suspected ties to the al-Qaida organization. ICE agents also initiated an investigation pursuant to an outbound seizure of suspected hawala generated funds seized en-route to Yemen, concealed in jars of honey. The investigation disclosed that the courier, and the reputed owner/broker of the funds, was actively involved in a hawala network.

In response to UNSCR 1267/1390/1452 and Yemen's Council of Ministers' directives, CBY issued a number of circulars to all banks operating in Yemen, directing them to freeze accounts of 144 persons, companies, and organizations, and to report any finding to CBY. As a result, one account was immediately frozen with a balance equal to \$33. In September 2003, the CBY issued Circular No.

75304 containing a consolidated list of all persons and entities belonging to al-Qaida (182) and the Taliban (153).

A law was passed in 2001 governing charitable organizations. This law entrusted the Ministry of Pensions and Social Affairs with overseeing their activities. The law also imposes penalties of fines and/or imprisonment on any society or its members convicted of carrying out activities or spending funds for other than the stated purpose for which the society in question was established.

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

Yemen is making progress in enforcing its domestic anti-money laundering program. The passage of the anti-money laundering legislation represents a significant first step in meeting international standards. However, development of the FIU and international cooperation with criminal investigations are only getting started. The CBY is still organizing its enforcement mechanism. Its effectiveness will demonstrate the authorities' commitment to ending money laundering. Yemen should also examine the prevalence of alternative remittance systems such as hawala and trade-based money laundering. As a next step, Yemen should also enact specific legislation with respect to terrorist financing and forfeiture of the assets of those suspected of terrorism. Yemen should become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Zambia

Zambia is not a major financial center. Reports indicate, however, that proceeds of narcotics transactions and money derived from public corruption are major sources of laundered money. Law enforcement officials also indicate that bulk cash smuggling is a concern.

The Prevention of Money Laundering Bill Act of 2001 makes money laundering a criminal offense, stiffens penalties for financial crimes, requires financial institutions to report suspicious transactions to regulators and retain transaction records for a period of ten years, allows seizure of assets related to money laundering, and increases the investigative and prosecutorial powers of the Drug Enforcement Commission (DEC). It also establishes an Anti-Money Laundering Authority that is chaired by the attorney general and includes the heads of Zambia's principal law enforcement agencies, Revenue Authority, and Central Bank. The DEC has the responsibility for investigating money laundering offenses. When regulatory agencies have reason to suspect money laundering, they must report this to the DEC, which acts as the enforcement arm of the anti-money laundering authority, and make relevant records available to investigators. The law authorizes investigators to seize property when they have reasonable grounds to believe that it is derived from money laundering. Following a conviction under the anti-money laundering law, the court may order the forfeiture to the state of property seized during an investigation. In 2003, three officers of a commercial bank were tried and convicted for money laundering offenses. The penalty for money laundering is imprisonment for a term not exceeding ten years and/or a fine.

The anti-money laundering law does not contain specific provisions on the financing of terrorism; the Government of Zambia (GOZ) does have the authority to order financial institutions to freeze assets, but this can be difficult if there is no evidence of a domestic crime. Zambia lacks comprehensive and reliable mechanisms for freezing the assets of terrorist organizations.

In 2003 an anti-money laundering unit was established under the DEC. The main purpose of the unit is to lead efforts within the GOZ to counter money laundering and enforce the Prevention of Money Laundering Act.

In August 2003, the Republic of Zambia signed the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) memorandum of understanding. Zambia is not a signatory to the UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Transnational Organized Crime. Zambia is a party to the 1988 UN Drug Convention.

Zambia should expand its anti-money laundering unit into a fully operational financial intelligence unit (FIU) that is recognized by international standards. Zambia 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. Zambia should also criminalize terrorist financing.

Zimbabwe

Zimbabwe is not a regional financial center and is not considered to be at significant risk for money laundering.

Zimbabwe's Anti-Money Laundering Act criminalizes narcotics-related money laundering. In December 2003, the Government of Zimbabwe submitted the Anti-Money Laundering and Proceeds of Crime Bill to Parliament. The bill is expected to pass in 2004. The bill would apply to all forms of money laundering and would require banks to maintain records sufficient to reconstruct individual transactions for at least six years. The bill would also mandate a prison sentence of up to five years for a money laundering conviction. The pending legislation would also address terrorist financing and the tracking and seizing of assets. In the context of the Government's history of using the legal system selectively and aggressively to target political opponents, the legislation as drafted could raise significant human rights concerns.

Zimbabwe is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the United Nations Convention against Transnational Organized Crime.

Zimbabwe should enact a comprehensive anti-money laundering regime (with appropriate due process protections) that criminalizes terrorist financing and money laundering for all serious crimes. Zimbabwe recently joined the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), the FATF-style regional body, in August 2003 and should sign the ESAAMLG Memorandum of Understanding. Zimbabwe should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism.