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. Currently, St. Lucia has four offshore banks, 1,884 international business companies, 43 international trusts, 17 international insurance companies, two money remitters, three mutual fund administrators, nine registered agents and three registered trustees (service providers) and a total of 30 domestic financial institutions. St. Lucia has a free trade zone. The Government of St. Lucia (GOSL) also is considering the establishment of gaming enterprises.

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 transactions for seven years. In September 2003, legislation was adopted that extends anti-money laundering compliance requirements to credit unions, money remitters and pawnbrokers, as well as strengthens criminal penalties for money laundering. Many of the 1993 Proceeds of Crime Act provisions are superseded by the 1999 Money Laundering (Prevention) Act (ML Prevention Act), which criminalizes the laundering of proceeds with respect to 15 prescribed offenses, including narcotics trafficking, corruption, fraud, terrorism, gambling and robbery. The ML Prevention Act mandates suspicious transaction reporting requirements and imposes record keeping requirements. In addition, the ML 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. It also requires an institution to take reasonable measures to identify the underlying beneficial owner when an agent, trustee or nominee operates an account. These obligations apply to domestic and offshore financial institutions, including credit unions, trust companies, and insurance companies. In April 2000, the Financial Services Supervision Unit issued detailed guidance notes, entitled "Minimum Due Diligence Checks, to be conducted by Registered Agents and Trustees."

Pursuant to the ML Prevention Act, the Money Laundering (Prevention) Authority (the 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 transaction 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 ML Prevention Act imposes a duty on the Authority to cooperate with competent foreign authorities. Assistance includes the provision of documents, testimony, conduct 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, to issue guidelines to financial institutions, and to instruct a financial institution to facilitate an investigation by the Authority.

In 1999, the GOSL also enacted a comprehensive inventory of offshore legislation, consisting of the International Business Companies (IBC) Act, the Registered Agent and Trustee Licensing Act, the International Trusts Act, the International Insurance Act, the Mutual Funds Act and the International Banks Act. An IBC may be incorporated under the IBC Act. Only a person licensed under the Registered Agent and Trustee Licensing Act as a licensee may apply to the Registrar of IBCs to incorporate and register a company as an IBC. The registration process involves submission of the memorandum and articles of the company by the registered agent, payment of the prescribed fee and the Registrar's determination of compliance with the requirements of the IBC Act. IBCs can be registered online through the GOSL's web page. IBCs intending to engage in banking, insurance or mutual 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 functions of the Authority have been transferred to the new FIU. The FIU is able to compel the production of information necessary to investigate possible offenses under the 1993 Proceeds of Crime Act and the ML 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) has trained St. Lucia's FIU personnel. In September 2003, legislation was adopted merging the Authority with the FIU. In 2005, the FIU received 85 suspicious transaction reports. There has been no money laundering convictions to date in St. Lucia. However, there is a money laundering case pending.

The GOSL established the Committee on Financial Services in 2001. The Committee, which meets monthly, is designed to safeguard St. Lucia's financial services sector. The Committee is composed of the Minister of Finance, the Attorney General, the Solicitor General, the Director of Public Prosecutions, the Director of Financial Services, the Registrar of Business Companies, the Commissioner of Police, the Deputy Permanent Secretary of the Ministry of Commerce, the police officer in charge of the Special Branch, the Comptroller of Inland Revenue and others. The GOSL announced in 2003 its intention to form an integrated regulatory unit to supervise the onshore and offshore financial institutions the GOSL currently regulates. The Eastern Caribbean Central Bank regulates St. Lucia's domestic banking sector. Counter-terrorism and counterterrorist financing legislation is pending before the St. Lucia Parliament. 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 Round 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 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. St. Lucia also has a Tax Information Exchange Agreement with the United States. The GOSL has been cooperative with the USG in financial crime investigations. St. Lucia is a party to the 1988 UN Drug Convention and, on September 26, 2001, signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. The GOSL has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of St. Lucia should become a party to the UN International Convention for the Suppression of the Financing of Terrorism and adopt counterterrorism financing legislation. St. Lucia should continue to enhance and implement its money laundering legislation and programs, including adopting civil forfeiture legislation.

St. Vincent and the Grenadines

St. Vincent and the Grenadines remains vulnerable to money laundering, other financial crimes, and the facilitation of terrorist financing, as a result of the rapid expansion and inadequate regulation of its offshore sector. The offshore sector includes six offshore banks, 6,632 international business corporations, 14 offshore insurance companies, 29 mutual funds, 33 registered agents, and 114 international trusts. No physical presence is required for offshore financial institutions and businesses. Nominee directors are not mandatory except where an international business corporation is formed to

carry on banking business. Bearer shares are permitted for international business corporations but not for banks. The domestic sector comprises of two commercial banks, a development bank, two savings and loan banks, a building society, 13 insurance companies, 10 credit unions, and two money remitters. There are no free trade zones in St. Vincent and the Grenadines (SVG) nor have any Internet gaming licenses been issued.

The Eastern Caribbean Central Bank (ECCB) supervises SVG's four 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 St. Vincent and the Grenadines (GOSVG) gave the ECCB increasing authority to review and make recommendations regarding approval of offshore bank license applications, and to directly supervise the offshore banks in cooperation with the GOSVG's International Financial Services Authority (IFSA). The agreement includes provisions for joint on-site inspections to evaluate the financial soundness and anti-money laundering programs of offshore banks. The IFSA alone continues to supervise and regulate the other offshore sector entities; however, its staff exercises only rudimentary controls over these institutions. The GOSVG has strengthened the structure and staffing of the IFSA by appointing five new members to the IFSA board. This brings the total to 12 staffers to regulate offshore insurance and mutual funds.

In June 2003, the Financial Action Task Force (FATF) recognized that the GOSVG, through enactment and implementation of appropriate legal reforms, had sufficiently addressed deficiencies identified by the FATF in 2000, and removed it from the list of Non-Cooperative Countries or Territories (NCCT). With SVG's removal from the NCCT list, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) lifted its advisory, which had instructed all U.S. financial institutions to "give enhanced scrutiny" to all transactions involving St. Vincent and the Grenadines. The FATF encouraged the GOSVG to consider tightening provisions relating to the granting of exemptions from customer identification requirements.

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 a customer account and any other confidential information about the customer that is in the possession of a licensee. The GOSVG prepared a further amendment to the International Banks Act with a view to improving licensing procedures and better regulating the offshore banking sector.

The GOSVG 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 strengthen provisions of the Act and the Regulations. Among other measures, the Act criminalizes money laundering and imposes on financial institutions and regulated businesses a requirement to report suspicious transactions likely to be related to money laundering or the proceeds of crime. The related regulations establish mandatory record keeping rules and limited customer identification/verification requirements. Financial institutions are required to maintain all records relating to transactions for a minimum of seven years. Reporting is required for all suspicious activities despite the transaction amount. Customers are required to complete a source of funds declaration for a cash transaction over $10,000 ECD ($3,703). However, it is not mandatory to report other transactions exceeding $10,000 ECD.

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

citizenship and passports, although there were no reports of passports having been issued under the program.

The Financial Intelligence Unit Act No. 38 of 2001 (FIU Act) establishes the Financial Intelligence Unit (FIU) that began operation in May 2002. The FIU Act allows for the exchange of information with foreign FIUs. An amendment to the FIU Act permits the sharing of information even at the investigative or intelligence stage. The FIU has a staff of 14 and became a member of the Egmont Group in June 2003. As of November 2005, the FIU had received 104 suspicious activity reports for the year and almost 500 since its inception. In November 2004, the FIU began an anti-money laundering /counterterrorist finance training initiative at the financial institutions.

There have been no money laundering convictions; however, there were five money laundering cases pending in 2005. In 2005 the GOSVG froze approximately 500,254 ECD ($185,279) and seized $396,232 ECD ($146,753). In 2003, the GOSVG reintroduced a customs declaration form to be completed by incoming travelers. Incoming travelers are required to declare currency over approximately $3,703.

The GOSVG is a member of the Caribbean Financial Action Task Force, and underwent its Second Round mutual evaluation in November 2002. In addition, the GOSVG is a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). The GOSVG is a party to the 1988 UN Drug Convention and acceded to the Inter-American Convention against Corruption in 2001. The GOSVG signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. 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 with its requirements. 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 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 SVG. To date, no accounts associated with terrorists have been found.

An updated extradition treaty and a Mutual Legal Assistance Treaty between the United States and the GOSVG entered into force in September 1999. The FIU executes the Mutual Legal Assistance Treaty requests.

The Government of St. Vincent and the Grenadines should address all remaining concerns raised by the international community in regard to its anti-money laundering regime. These include the areas of customer identification, money remitters, outstanding bearer shares, and money laundering prosecutions. St. Vincent and the Grenadines should continue to provide training to its regulatory, law enforcement, and Financial Intelligence Unit personnel in money laundering operations and investigations. The GOSVG should also ensure that it properly supervises the offshore sector. St. Vincent and the Grenadines should pass counterterrorist financing legislation that will provide the authority to identify, freeze and seize terrorist assets. In addition, the GOSVG should pass civil forfeiture legislation and consider the utility of special investigative techniques.

Swaziland

Swaziland is a growing regional financial center. International narcotics trafficking, primarily in marijuana, continues to grow in Swaziland. The country'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.

Although the Money Laundering Act of 2001 (Act) criminalizes money laundering for specified predicate offenses, including narcotics trafficking, kidnapping, counterfeiting, extortion, fraud, and

arms trafficking, it does not adequately address processes and procedures for the police to follow when money laundering is suspected. As a result, the Central Bank of Swaziland and the Ministry of Finance have assisted in drafting amendments to the Act for review by the Cabinet. The penalty for money laundering is six years imprisonment, a fine amounting to roughly $3,500, or both. The Act establishes a currency reporting requirement, requires banks to report suspicious transactions to the Central Bank, and provides conditions when assets may be frozen and forfeited. The Act also requires banks to retain records for five years, to improve the ability to trace suspicious transactions and patterns.

On November 16, 2004, the Central Bank of Swaziland and the Bankers Association of Swaziland issued a general statement on anti-money laundering regarding the importance of positive identification in banking. The statement says that Swaziland's financial institutions will not conduct transactions with any customers failing to furnish proof of their identity and that service shall not be provided when there is any reason to suspect that money laundering may be involved. As of June 30, 2005, all existing customers of Swaziland's financial institutions must present current information to establish their actual identity.

To assist the banking community with tracking suspicious transactions, the Central Bank distributed anti-money laundering guidelines to all banks. As of November 2005, the Central Bank received an estimated 75 reports of suspicious transactions. The police bear responsibility for investigating such cases, but no investigations have taken place. The police also would be responsible for seizing any assets related to money laundering, but no seizures have taken place under the Act.

Members of the Royal Swaziland Police Service (RSPS) have noted that they lack the ability to understand and monitor small businesses. The RSPS has little liaison or cooperation with those ministries of the Government of the Kingdom of Swaziland (GKOS) involved with regulating businesses and business owners. Their expressed concerns in this arena include a perceived escalation in the number of foreign business owners throughout Swaziland. While the RSPS is becoming aware that businesses, such as used car lots, cellular and electronic shops, and sundries stores, are commonly used throughout the world as fronts and/or laundering mechanisms, the RSPS lacks the inter-departmental infrastructure and agreements to address this growing concern. The small business sector in Swaziland has been traditionally overlooked as a very real potential money laundering and support element for drug traffickers and terrorist groups. More inter-departmental and inter-ministerial cooperation is needed in order to properly assess and address this vulnerability.

The Act allows for providing assistance to foreign countries that have entered into mutual assistance treaties with the GKOS. An amendment to the Act will allow for Swaziland to comply with regional agreements and international conventions.

Swaziland is party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The GKOS has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Swaziland is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body.

The Government of the Kingdom of the Swaziland (GKOS) should criminalize terrorist financing. Swaziland should also establish an anti-money laundering regime consistent with international standards, including a financial intelligence unit capable of sharing information with foreign law enforcement and regulatory officials. The Kingdom of the Swaziland should provide the appropriate resources and training to its law enforcement personnel to allow them to adequately perform their duties.

Switzerland

Switzerland is a major international financial center, with some 338 banks and a large number of non-bank financial intermediaries. Authorities suspect that Switzerland is vulnerable at the layering and

integration stages of the money laundering process. Switzerland's central geographic location, relative political, social, and monetary stability, wide range and sophistication of available financial services, and long tradition of bank secrecy are all factors that make Switzerland a major international financial center. These same factors also make Switzerland attractive to potential money launderers. However, Swiss authorities are aware of this and are sensitive to the size of the Swiss banking industry relative to the size of the economy. Total assets and liabilities in Swiss banking institutions were over 2.4 trillion Swiss francs ($1.8 trillion) in 2004, with foreigners accounting for over half of this figure. By comparison, Switzerland's GDP in 2004 was approximately $250 billion.

Reporting indicates that criminals attempt to launder proceeds in Switzerland from a wide range of illegal activities conducted worldwide, particularly financial crimes, narcotics trafficking, arms trafficking, organized crime, and corruption. Although both Swiss and foreign individuals or entities conduct money laundering activities in Switzerland, narcotics-related money laundering operations are largely controlled by foreign narcotics trafficking organizations, often from the Balkans or Eastern Europe. Some of the money generated by Albanian narcotics trafficking rings in Switzerland has been funneled to armed Albanian extremists in the Balkans.

Swiss bank accounts also frequently figure in investigations of fraud and corruption of government officials and leaders, most often from foreign countries. Recent examples of public figures that have been the subject of money laundering allegations or investigations include a former Kyrgyzstan President, a former Russian Minister of Atomic Energy, and the son of the Nigerian dictator Sani Abacha. The former Swiss Ambassador to Luxembourg was sentenced to three and a half years in jail for money laundering and other crimes in June 2005.

Money laundering is a criminal offense in Switzerland. Swiss law, however, does not recognize certain types of criminal offenses as predicate offenses for money laundering, including illegal trafficking in migrants, counterfeiting and pirating of products, smuggling, insider trading, and market manipulation. The adoption of anti-money laundering (AML) regulations planned for 2007 will make these crimes predicate offenses.

Switzerland has significant AML 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. Legislation that aligns the Swiss supervisory arrangements with the Basel Committee's "Core Principles for Effective Banking Supervision" is contained in the Swiss Money Laundering Act.

Swiss money laundering laws and regulations apply to both banks and non-bank financial institutions. The Federal Banking Commission, the Federal Office of Private Insurance, and the Swiss Federal Gaming Board serve as primary oversight authorities for a number of financial intermediaries, including banks, securities dealers, insurance institutions, and casinos. Other financial intermediaries are required to either come under the direct supervision of the Money Laundering Control Authority (MLCA) of the Federal Finance Department or join an accredited self-regulatory organization (SRO). The SROs are non-governmental self-regulating organizations authorized by the Swiss government to oversee implementation of AML measures by their members. 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 6,000 financial intermediaries are associated with SROs; the majority of these are financial management companies.

The Swiss Federal Banking Commission's AML regulations were revised in 2002 and became effective in 2003. These regulations, aimed at the banking and securities industries, codify a risk-based approach to suspicious transaction and client identification and install a global know-your-customer risk management program for all banks, including those with branches and subsidiaries abroad. In the case of higher-risk business relationships, additional investigation by the financial intermediary is required. The regulations require increased due diligence in the cases of politically exposed persons by

ensuring that decisions to commence relationships with such persons be undertaken by at least one member of the senior executive body of a firm. All provisions apply to correspondent banking relationships as well. Swiss banks may not maintain business relationships with shell banks (banks with no physical presence at their place of incorporation), but there is no requirement that banks ensure that foreign clients do not authorize shell banks to access their accounts in Swiss banks.

The 2002 Banking Commission regulations mandate that all cross-border wire transfers must contain identifying details about the funds' remitters, though banks and other covered entities may omit such information for "legitimate reasons." The Swiss Federal Banking Commission has said that there are no plans at the moment to follow EU regulations aimed at registering names, addresses, and account numbers of everyone making even small money transfers between EU member states.

In July 2003, the government-sponsored Zimmerli Commission, tasked by the Department of Finance with examining reform of finance market regulators, presented 46 recommendations. Among the most far-reaching of these was the recommendation to merge the Federal Banking Commission and the Federal Office for Private Insurance—the institutions supervising the banking and insurance sectors—into a single, integrated financial market supervision body, to be called FINMA. In November 2004, the Cabinet instructed the Department of Finance to draft a parliamentary bill providing for the establishment of FINMA. Under the Cabinet's proposal, MLCA would also be included within the FINMA. The draft bill is scheduled for submission to Parliament by early 2006.

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. Pursuant to an agreement signed by the EU and Switzerland in 2004, EU residents have tax withheld on interest payments from savings accounts. This measure, enacted in concert with the EU's Savings Directive (2003/48/EC), was implemented on July 1, 2005, and may reduce the use of Swiss bank accounts by EU residents.

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

Switzerland has duty free zones. The customs authorities supervise the admission into and the removal of goods from customs warehouses. Warehoused goods may only undergo manipulations necessary for their maintenance, such as repacking, splitting, sorting, mixing, sampling and removal of the external packaging. Any further manipulation is subject to authorization. Goods may not be manufactured in the duty free zones. Swiss law has full force in the duty free zones; for example, export laws on strategic goods, war material, and medicinal products, as well as laws relating to anti-money laundering prohibitions, all apply. In view of the fact that customs authorities may and frequently do enter any customs warehouse area they choose, they believe they would be aware of the nature of any "value added" activity taking place in duty free zones.

Switzerland ranks fifth in the highly profitable artwork trading market, exporting $686 million worth of artwork worldwide in 2004. The Swiss market offers lucrative opportunities for organized crime to transfer stolen art or to use art to launder criminal funds. The United States is by far Switzerland's most important trading partner in this area, having purchased $253 million worth of "Swiss" works of art in 2004. The 2003 Cultural Property Transfer Act, implemented in 2005, codifies in Swiss law elements of the 1970 United Nations Educational, Scientific, and Cultural Organization (UNESCO) Convention. This measure increases from five to thirty years the time period during which stolen

pieces of art may be confiscated from those who purchased them in good faith. The law also allows police forces to search bonded warehouses and art galleries.

The Money Laundering Reporting Office Switzerland (MROS) is Switzerland's financial intelligence unit (FIU), charged with receiving and processing suspicious transaction reports (STRs). MROS does not have any investigative powers of its own nor can it obtain additional information from reporting entities after receiving a STR. In 2004, the number of STRs received by MROS fell by five percent over 2003, with 821 reports involving approximately $586 million. As in 2002 and 2003, the majority of reports came from money transmitters where funds transfers are conducted quickly and the rapid-turnover does not allow the financial intermediary the same ability as a bank or a fiduciary to gather background information on a transaction, thus arousing greater suspicion.

At the same time, the number of STRs provided by banks in 2004 increased relative to 2003, both in absolute numbers (from 302 to 340) and in terms of the percentage of all STRs (from 35 percent to 41 percent). Banks increasingly reported attempts at money laundering by prospective clients prior to the establishment of a banking relationship, which has resulted in a government plan to make the reporting of attempted money laundering mandatory for all financial intermediaries.

Under the 2002 Efficiency Bill, the Swiss Attorney General is vested with the power to prosecute crimes addressed by Article 340bis of the Swiss Penal Code, which also covers money laundering offenses. In the past, the individual cantons (administrative components of the Swiss Confederation) were charged with investigating money laundering offenses. Additional legislation, effective January 1, 2002, increased the effectiveness of the prosecution of organized crime, money laundering, corruption, and other white-collar crime, by increasing the personnel and financing of the criminal police section of the federal police office. The law confers on the federal police and Attorney General's office the authority to take over cases that have international dimensions, involve several cantons, or which deal with money laundering, organized crime, corruption, and white collar crime.

If financial institutions determine that assets were derived from criminal activity, the assets must be frozen immediately until a prosecutor decides on further action. 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.

Swiss legislation permits "spontaneous transmittal," a process allowing the Swiss investigating magistrate to signal to foreign law enforcement authorities the existence of evidence in Switzerland. The Swiss used this provision in 2001 to signal Peru that they had uncovered accounts linked to former Peruvian presidential advisor Vladimiro Montesinos.

Revisions to the Swiss Penal Code regarding terrorist financing, adopted by the Swiss Parliament in March 2003, entered into force on October 1, 2003. Article 260quinquies of the Penal Code provides for a maximum sentence of five years' imprisonment for terrorist financing. Article 100quater of the Penal Code, also added in 2003, extends criminal liability for terrorist financing to include companies. The FATF's 2005 mutual evaluation of Switzerland found it "largely compliant" with FATF Special Recommendation II regarding the criminalization of terrorist financing; however, it noted that the Swiss Penal Code criminalizes the financing of an act of criminal violence, not the financing of an individual, independent of a particular act.

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

have ordered banks and other financial institutions to freeze the assets of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list.

Along with the U.S. and UN lists, the Swiss Economic and Finance Ministries have drawn up their own list of approximately 44 individuals and entities connected with international terrorism or its financing. Swiss authorities have thus far blocked about 82 accounts totaling $25 million from individuals or companies linked to Usama Bin Ladin and al-Qaida under relevant UN resolutions. The Swiss Attorney General also separately froze 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 consolidated list has yet to be determined.

In the 2004 reporting period, MROS received reports of eleven cases possibly linked to the funding of terrorism, up from five reports in 2003. The total amount of money involved was $683,100. Four of the eleven reports involved Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224. All eleven reports were forwarded to law enforcement agencies.

Switzerland has ratified the Council of Europe's Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and is a party to the UN International Convention for the Suppression of the Financing of Terrorism. Switzerland has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Switzerland ratified the 1988 UN Drug Convention on September 14, 2005.

Swiss authorities cooperate with counterpart bodies from other countries. Requests from FinCEN, the U.S. FIU, accounted for eight percent of requests received by MROS from foreign FIUs. Switzerland has a mutual legal assistance treaty in place with the United States, and Swiss law allows authorities to furnish information to U.S. regulatory agencies, provided it is kept confidential and used for supervisory purposes. Switzerland is a member of the Financial Action Task Force (FATF) and the Basel Committee on Banking Supervision, and its FIU is a member of the Egmont Group.

The FATF conducted a mutual evaluation of Switzerland's anti-money laundering (AML) and counterterrorist financing (CTF) regime in 2005. The FATF concluded that Switzerland was at least partially compliant in most areas. However, the evaluators found Switzerland to be non-compliant with respect to correspondent banking, beneficial ownership of legal persons, and cash couriers.

The Government of Switzerland hopes 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 know-your-customer procedures address the issues, rather than relying on an early-warning system on all filed transactions. The Swiss Government believes that because of the due diligence approach the Swiss have taken, there are fewer STRs filed than in some other countries. At the same time, 75 percent of the STRs that are filed lead to the opening of criminal investigations.

While generally positive, Switzerland's recent FATF mutual evaluation report nonetheless identified weaknesses in the Swiss anti-money laundering and counterterrorist financing regime, including problems with correspondent banking, identification of beneficial owners, and the cross-border transportation of currency. The Government of Switzerland should continue to improve on its regime while simultaneously working toward full implementation of existing laws and regulations. It should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Syria

Syria, a designated State Sponsor of terrorism, is not an important regional or offshore financial center, due primarily to its still under-developed private banking sector and the fact that the Syrian Pound (SYP) is not a fully convertible currency. However, there remain significant AML/CFT vulnerabilities in Syria's financial and non-bank financial sectors that have not been addressed by necessary legislation or other government action. In addition, Syria's black market hawaladars are unregulated, and the country's borders remain porous. Most of the money laundering threat is believed to be of domestic origin and to involve Syria's political and business elite, whose corruption and extra-legal activities represent the biggest obstacle to Syria fully choking off money laundering and terrorist financing activities.

Syria's free trade zones also may provide an easy entry or transit point for the proceeds of criminal activities. There are seven free zones in Syria, serviced mostly by subsidiaries of Lebanese banks, including BLOM Bank, BEMO (Banque Europeenne Pour le Moyen-Orient Sal), and BBAC (Bank of Beirut and Arab Countries). The volume of goods entering the free zones is estimated to be in the billions of dollars, since all automobiles and automotive parts enter the zones free of customs tariffs before being imported into Syria. There also is a significant amount of trade that transits Syria through the zones, gaining Syrian value added before being shipped to foreign markets. While all industries and financial institutions located in the free zones must be registered with the General Organization for Free Zones, which is located in the Ministry of Economy and Trade, the Syrian General Directorate of Customs does not have strong procedures to check country of origin certification or the resources to adequately monitor goods that enter Syria through the zones. There are indications that Syrians have used the free zones to import goods into Syria in violation of USG sanctions under the Syrian Accountability and Lebanese Sovereignty Act.

The banking sector is dominated by the Commercial Bank of Syria (CBS), which holds almost 90 percent of all deposits and controls most of the country's foreign currency reserves. With the liberalization of the sector and competition from the private banks, the CBS is preparing to provide a range of retail services and more competitive interest rates. However, the CBS and the country's four other specialized public banks- the Agricultural Cooperative Bank, the Industrial Bank, the Real Estate Bank, and the People's Credit Bank- still primarily focus on financing Syria's public enterprises. In May 2004, the U.S. Department of the Treasury designated the CBS, along with its subsidiary, the Syrian Lebanese Commercial Bank, as a financial institution of "primary money laundering concern," pursuant to Section 311 of the USA PATRIOT Act, due to a reasonable belief that the CBS has been used by terrorists or persons associated with terrorist organizations and as a conduit for the laundering of proceeds generated from the illicit sale of Iraqi oil. This designation remains in place due to continued concerns that the CBS may still be exploited by criminal enterprises. However, the final rulemaking on the implementation of the special measure against the CBS has not been issued.

Syria began taking steps to develop a private banking sector in April 2001, with Law No. 28, which legalized private banking, and Law No. 29, which established rules on bank secrecy. Bank of Syria and Overseas, a subsidiary of Lebanon's BLOM Bank, was the first private bank to open in Syria in January 2004, followed quickly by Banque BEMO Saudi Fransi and the International Bank for Trade and Finance. Bank Audi became the fourth private bank in Syria, opening a Damascus branch in October 2005. The sector's total capitalization is small, approximately $300 million, and while the banks report steady growth in their deposit accounts and are playing an increasing role in providing the business sector with foreign currency to finance imports, unnecessary regulations that do not allow banks to make money on their liquidity hamper the sector's continued development.

Recent legislation provides the Central Bank of Syria with new authority to oversee the banking sector and investigate financial crimes. The SARG passed Decree 59 in September 2003 to criminalize money laundering and create an Anti-Money Laundering Commission, which was established in May

2004. In response to international pressure to improve its AML/CFT regulations, the SARG passed Decree 33 in May 2005, which strengthens the Commission and lays the foundation for a functioning FIU. The Decree finalized the Commission's composition to include the Governor of the Central Bank, a Supreme Court Judge, the Deputy Minister of Finance, the Deputy Governor for Banking Affairs, the SARG's Legal Advisor, and will include the Chairman of the Syrian Financial Market once the Market is operational.

Under Decree 33, all banks and non-financial institutions are required to file Suspicious Activity Reports (SARs) with the Commission-which is acting as the FIU-for all transactions over $10,000, as well as all suspicious transactions regardless of amount. The chairmen of Syria's private banks report that they employ internationally recognized "know your customer" (KYC) procedures to screen transactions and employ their own investigators to check suspicious accounts. In September 2005, the Commission informed banks that they must use KYC procedures to follow up on their customers every three years and maintain records on closed accounts for five years. Non-bank financial institutions are also to file SARs with the Commission, but many of them are still unfamiliar with the requirements of the law. The Syrian Chamber of Commerce has organized workshops for its membership about the law, but it will take some time for the information to penetrate the market.

Once a SAR has been filed, the Commission has the authority to conduct an investigation, waive bank secrecy on specific accounts in order to gather additional information, share information with the police and judicial authorities, and direct the police to carry out a criminal investigation. In addition, Decree 33 empowers the Governor of the Central Bank, who is the chairman of the Commission, to share information and sign Memoranda of Understanding (MOUs) with foreign FIUs. In November 2005, the Prime Minister announced that the Commission had completed an internal reorganization, creating four specialized units to: oversee financial investigations; share information with other SARG entities including customs, police and the judiciary; produce AML/CFT guidelines and verify their implementation; and develop a financial crimes database.

Decree 33 provides the Commission with a relatively broad definition of what constitutes a crime of money laundering, but one that does not fully meet international standards. The definition includes acts that attempt to conceal the proceeds of criminal activities, the act of knowingly helping a criminal launder funds, and the possession of money or property that resulted from the laundering of criminal proceeds. In addition, the law specifically lists thirteen crimes that are covered under the AML legislation, including narcotics offenses, fraud, and the theft of material for weapons of mass destruction. However, it is unclear whether terrorist financing is a predicate offense for money laundering or otherwise punishable under Decree 33.

While a SAR is under investigation, the Commission can freeze accounts of suspected money launderers for a non-renewable period of up to eighteen days. However, the Syrian judicial system moves slowly and there are some concerns that this period is too short to hinder criminal activities. The law also stipulates the sanctions for convicted money launderers, including a three to six-year jail sentence and a fine that is equal to or double the amount of money laundered. Further, the law allows the SARG to confiscate both the money and assets of the convicted money launderer. The Commission circulates among its private and public banks the names of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanction Committee's consolidated list, and it has taken action to freeze the assets of designated individuals.

Despite the legislative powers of the Commission, only 100 suspicious transactions were reported in 2005, including SARs from the police who identified suspected money laundering activities in the course of other investigations. There have been no arrests or convictions in 2005. Since money laundering legislation is new, most judges are not yet familiar with the evidentiary requirements of the law. The Commission has estimated that it will take at least a year before Syria's judicial system is fully capable of prosecuting money laundering cases. The Commission further reported that it has not

conducted investigations into any of the SARs filed over the past year, and that its ongoing investigations are into the financial activities of individuals who already were charged and imprisoned for financial crimes before Decree 33 went into effect. The Commission itself is hampered by human resource constraints. It has a staff of six, and hopes to expand to fifteen by the end of 2006. Most of the staff has not received much training in AML/CFT detection, although the European Commission has expressed a willingness to establish a training center in the Central Bank.

Although Decree 33 provides the Central Bank with a foundation to combat money laundering, most Syrians still do not maintain bank accounts. Very few Syrians use checks or credit cards, and the use of ATM machines is relatively new. The Syrian economy is primarily cash-based, and Syrians use moneychangers, some of whom also act as hawaladars, for many financial transactions. It is illegal for persons to participate in the informal financial sector, but it remains significant. Estimates of the volume of business conducted in the black market by Syrian moneychangers range between $15-70 million a day. Due to the lack of hard data on this sector, the SARG admits that it does not have visibility into the amount of money that currently is in circulation. The SARG has begun issuing new regulations to entice people to use the banking sector, including offering high interest Certificates of Deposit and allowing Syrians to access more foreign currency from banks when they are traveling abroad. In addition, the SARG has advertised a deadline of mid-January 2006 by which it hopes to pass a Moneychangers Law to regulate the sector. Once the Moneychangers Law is passed, the Commission will have the authority to monitor the sector under Decree 33. Until the SARG passes sufficient legislation and enforcement mechanisms, the hawaladars in Syria's black market remain a source of concern for money laundering and terrorist financing.

The SARG also has not updated its laws regarding charitable organizations to include strong AML/CFT language. While the SARG decided at the end of 2004 to restrict charitable organizations to only distributing non-financial assistance, the current laws do not require organizations to submit detailed financial information or information on their donors. However, the Commission has stated its intention to cooperate with the Ministry of Social Affairs to deal with this issue.

While the SARG maintains strict controls on the amount of money that individuals can take with them out of the country, there is a high incidence of cash smuggling across the Lebanese and Jordanian borders. Most of the smuggling involves the SYP, as there are strong markets for Syrian currency among expatriate workers and tourists in Lebanon, Jordan and the Gulf countries, although some of the smuggling may involve the proceeds of narcotics and other criminal activity as previously reported. In addition to cash smuggling, there also is a high rate of commodity smuggling out of Syria, particularly of diesel fuel, caused by individuals buying diesel domestically at the low subsidized rate and selling it for much higher prices in neighboring countries. There are reports that some smuggling is occurring with the knowledge of or perhaps even under the authority of the Syrian security services.

The General Directorate of Customs lacks the necessary staff and financial resources to effectively handle the problem of smuggling, and it currently lacks the means to share information among border posts or other government agencies. Customs recently announced that it plans to develop a special office to combat AML/CFT in coordination with the Ministry of Finance and Syria's security services, and plans to place cameras at all border posts and link them with a unified database. Customs currently lacks the infrastructure to effectively monitor or control even the legitimate movement of currency across its borders. Tourists are not required to declare the amount of money they are bringing into Syria, for instance. In order to combat corruption among customs officers, the General Directorate of Customs announced in December 2005 that it plans to ban all cash transactions at the borders, including the payment of customs duties, and will replace cash transactions with a system that utilizes pre-paid cards. However, most of the plans to unify and streamline customs procedures are far from being realized and depend upon technical and financial support from foreign donors.

Syria is one of the fourteen founding members of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body. In 2006, it is scheduled for a mutual evaluation by its peers in MENAFATF. In 2005, Syria hosted a team from the Egmont Group regarding the creation of its FIU. Syria has stated its intention to join the Egmont Group in the near future. In addition, Syria will host a legal team from FATF in early 2006, which will assess its progress in enforcing AML/CFT statutes. Syria is a party to the 1988 UN Drug Convention. In April 2005, it became a party to the International Convention on the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime.

While Syria has made strides throughout 2005 in developing AML/CFT regulations that govern its formal financial sector, non-bank financial institutions and the unregulated black market remain very vulnerable to money laundering and terrorist financiers. In addition, the General Directorate of Customs, the Central Bank and the judicial system in particular lack the resources to effectively implement AML/CFT legislation. Although the SARG has stated its intention to create the technical foundation through which different government agencies can share information about financial crimes, this does not exist to date. Syria should ratify the UN Convention against Transnational Organized Crime. It should criminalize terrorist financing or clarify that Decree 33 already does so. In addition, there are concerns that the SARG lacks the political will to punish terrorist financing or to classify what it sees as legitimate resistance groups as terrorist organizations. Further, corruption at the highest levels of government and business may be the biggest obstacle to developing a comprehensive and effective AML/CFT regime.

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. In 2005, the number of drug-related cases investigated, and the amount of illegal drugs seized has risen markedly. The use of alternative remittance systems or "underground banking" is a money laundering vulnerability. There is a significant volume of informal financial activity through unregulated non-bank channels. Most illegal or unregulated financial activities are related to tax evasion, fraud, or intellectual- property violations. According to suspicious activity reports (SARs) filed by financial institutions on Taiwan, the predicate crimes commonly linked to SARs include financial crimes, corruption, narcotics, and other general crimes.

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 (parliament) amended the MLCA in 2003 to expand the list of predicate crimes for money laundering, widen the range of institutions subject to suspicious transaction reporting, and mandate compulsory reporting to the MLPC of significant currency transactions of over New Taiwan Dollars (TDW)1 million (approximately $30,000). Between August 2003, when the amended MLCA came into force, and May 31, 2004, the MLPC received over one million such reports on currency transactions-with 99 percent of them reported electronically. Also as a result of the 2003 MLCA amendments, the list of institutions subject to reporting requirements was expanded, to include casinos, automobile dealers, jewelers, boat and plane dealers, real estate brokers, credit cooperatives, consulting companies, insurance companies, and securities dealers, as well as traditional financial institutions.

Taiwan also set up a single financial regulator, the Financial Supervisory Commission (FSC) on July 1, 2004. The FSC consolidates the functions of regulatory monitoring for the banking, securities, futures and insurance industries, and also conducts financial examinations across these sectors. In mid-December 2005, the Financial Supervisory Commission (FSC) began an incentive program for the public to provide information on financial crimes. The reward for information on a financial case with fines of TDW 10 million (approximately $300,000) or at least a one-year sentence is up to TDW 500,000 (approximately $15,000). The reward for information on a case with a fine of between TDW 2-10 million (approximately $60,000-$300,000) or less than a one-year sentence is up to TDW 200,000 (approximately $6,000).

Two new articles added to the 2003 amendments to the MLCA granted prosecutors and judges the power to freeze assets related to suspicious transactions and gave law enforcement more powers related to asset forfeiture and the sharing of confiscated assets. In terms of reporting requirements, financial institutions are required to identify, record, and report the identities of customers engaging in significant or suspicious transactions. There is no threshold amount specified for filing suspicious transaction reports. The time limit for reporting cash transactions of over TDW 1 million (approximately $39,000) is within five business days. Banks are barred from informing customers that a suspicious transaction report has been filed. Reports of suspicious transactions must be submitted to the MLPC within 10 business days after the transaction took place.

Institutions are also required to maintain records necessary to reconstruct significant transactions, for an adequate amount of time. Bank secrecy laws are overridden by anti-money laundering legislation, allowing the MPLC to access all relevant financial account information. Financial institutions are held responsible if they do not report suspicious transactions. In May 2004, the Ministry of Finance issued instructions requiring banks to demand two types of identification and to keep copies when bank accounts are opened upon request for a third party, in order to prove the true identity of the account holder. Individual bankers can be fined TDW 200,000-1 million ($7,800-$39,000) for not following the MLPA.

All foreign financial institutions and offshore banking units follow the same regulations as domestic financial entities. Offshore banks, international businesses, and shell companies must comply with the disclosure regulations from the Central Bank, Bureau of Monetary Affairs (CB), and MLPC. These supervisory agencies conduct background checks on applicants for banking and business licenses. Offshore casinos and Internet gambling sites are illegal.

On January 5, 2006, the Offshore Business Unit (OBU) Amendment was ratified to allow expansion of OBU operations to the same scope as Domestic Business Units (DBU). This was done to assist China-based Taiwan businesspeople in financing their offshore business operations. DBUs engaging in cross-strait financial business must follow the regulations of the "Act Governing Relations between Peoples of the Taiwan Area and the Mainland Area" and "Regulations Governing Approval of Banks to Engage in Financial Activities between the Taiwan Area and the Mainland Area." The Competent Authority, as referred to in these Regulations, is the Ministry of Finance.

Taiwan prosecuted 947 cases involving financial crimes from January to October 2005. Among these cases, 871 involved unregistered trading in stock markets, credit-card theft, currency counterfeiting, or fraud. Among the other money laundering cases, six were corruption-related and two were drug-related. In addition, the number of drug-related investigations jumped markedly in 2005, from 64,497 in January-November 2004 to 81,058 in January-November 2005. Among these 81,058 drug cases, 80,858 investigations were completed, 27,152 subjects were indicted, and 21,206 subjects were cleared. From January-October 2005, the volume of seized drugs totaled 12,728 kilograms, about 66.3 percent higher than that seized in the same period of 2004.

Individuals are required to report currency transported into or out of Taiwan in excess of TDW 60,000 (approximately $1,850). Starting in March 2004, transactions over 6,000 Chinese renminbi ($725)

must also be reported. When foreign currency in excess of TDW 500,000 (approximately $15,400) is brought into or out of Taiwan, the bank customer is required to report the transfer to the Central Bank, though there is no requirement for Central Bank approval prior to the transaction. Prior approval is required, however, for exchanges between New Taiwan dollars and foreign exchange when the amount exceeds $5 million for an individual resident and $50 million for a corporate entity. Effective September 2003, the Directorate General of Customs assumed responsibility for providing the MLPC on a monthly basis with electronic records of travelers entering and exiting the country carrying any single foreign currency amounting to TDW 1.5 million (approximately $58,500).

The authorities on Taiwan are actively involved in countering the financing of terrorism. In 2003, a new "Counter-Terrorism Action Law" (CTAL) was drafted, although as of December 2005 it was still under review by the Legislative Yuan. The new law would explicitly designate the financing of terrorism as a major crime. Under the proposed CTAL, the National Police Administration, the MJIB, and the Coast Guard would be able to seize terrorist assets even without a criminal case in Taiwan. Also, in emergency situations, law enforcement agencies would be able to freeze assets for three days without a court order.

Assets and income obtained from terrorist-related crimes could also be permanently confiscated under the proposed CTAL, unless the assets could be identified as belonging to victims of the crimes. Taiwan officials currently have the authority to freeze and/or seize terrorist-related financial assets under the MLCA promulgated in 1996 and amended in February 2003 to cover terrorist finance activities. Under the Act, the prosecutor in a criminal case can initiate freezing assets, or without criminal charges, the freezing/seizure can be done in response to a request made under a treaty or international agreement.

The Bureau of Monetary Affairs (BOMA) has circulated to all domestic and foreign financial institutions in Taiwan the names of individuals and entities included on the UN 1267 Sanctions Committee's consolidated list. Taiwan and the United States have established procedures to exchange records concerning suspicious terrorist financial activities. After receiving financial terrorist lists from the American Institute in Taiwan, BOMA conveys the list to relevant financial institutions. Banks are required to file a report on cash remittances if the remitter/remittee is on a terrorist list. Although as noted above Taiwan does not have the authority to confiscate the assets, the MLCA was amended to allow the freezing of accounts suspected of being linked to terrorism.

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

Authorities in Taiwan do not believe that charitable and nonprofit organizations in Taiwan are being used as conduits for the financing of terrorism, and there are currently no plans to investigate such entities further for terrorist financing. Such organizations are required to register with the government.

All of Taiwan's five free trade zones, including Taipei Free Trade Zone, Taichung Free Trade Zone, Keelung Free Trade Zone, Kaohsiung Free Trade Zone, and Taoyuan Air Cargo Free Trade Zone have opened since 2004. According to the Center for Economic Deregulation and Innovation (CEDI) under the Council for Economic Planning & Development, by the end of 2005 there were seven shipping and logistics companies listed in the Kaohsiung Free Trade Zone, four in Taichung Free Trade Zone, five

in Keelung Free Trade Zone, one in Taipei Free Trade Zone, and 49 manufacturers and enterprises in Taoyuan Air Cargo Free Trade Zone.

According to Taiwan's Banking Law and Securities Trading Law, in order for a financial institution to conduct foreign currency operations, Taiwan's Central Bank must first grant approval. The financial institution must then submit an application to port authorities to establish an offshore banking unit (OBU) in the free-trade zone. No financial entity has yet applied to establish such an OBU in any of the five free trade zones.

Taiwan has established drug-related asset seizure and forfeiture regulations that state that according to treaties or agreements, Taiwan's Ministry of Justice shall share seized assets with foreign official agencies, private institutions or international parties that provide Taiwan with assistance in investigations or enforcement. Assets of drug traffickers, including instruments of crime and intangible property, can be seized along with legitimate businesses used to launder money. The injured parties can be compensated with seized assets. The Ministry of Justice distributes other seized assets to the prosecutor's office, police or other anti-money laundering agencies. The law does not allow for civil forfeiture. A mutual legal assistance agreement between the American Institute in Taiwan (AIT) and the Taipei Economic and Cultural Representative Office in the United States (TECRO) entered into force in March 2002. It provides a basis for the law enforcement agencies of the people represented by AIT and TECRO to cooperate in investigations and prosecutions for narcotics trafficking, money laundering (including the financing of terrorism), and other financial crimes.

Although Taiwan is not a UN member and cannot be a party to the 1988 UN Drug Convention, the authorities in Taiwan have passed and implemented laws in compliance with the goals and objectives of the Convention. Similarly, Taiwan cannot be a party to the UN International Convention for the Suppression of the Financing of Terrorism, as a nonmember of the United Nations, but it has agreed unilaterally to abide by its provisions. Taiwan is a founding member of the Asia/Pacific Group on Money Laundering (APG) and in 2005, was elected to the APG steering committee. The MLPC is a member of the Egmont Group of Financial Intelligence Units. The Investigation Bureau of the Ministry of Justice expanded information exchanges with various countries/jurisdictions from 17 jurisdictions in 2004 to 20 in 2005.

Over the past five years, Taiwan has created and implemented an anti-money laundering regime that comports with international standards. The MLCA amendments of 2003 address a number of vulnerabilities, especially in the area of asset forfeiture. The authorities on Taiwan should continue to strengthen the existing anti-money laundering regime as they implement the new measures. Taiwan should endeavor to pass the proposed Counter-Terrorism Action Law to better address terrorist financing issues. The authorities on Taiwan should also enact legislation that would promulgate regulations regarding alternate remittance systems.

Tanzania

Tanzania is not considered an important regional financial center, but it 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 money laundering difficult to track and prosecute. Officials suspect that some real estate and used car businesses are used for money laundering purposes. Government officials have also cited the emerging casino industry as an area of concern for money laundering. Money laundering is even more likely to occur in the informal non-bank financial sector, as the formal sector is still relatively undeveloped. Front companies used to launder funds include hawaladars and bureaux de change, especially on the island of Zanzibar, where fewer federal regulations apply. Officials indicate that money laundering schemes in Zanzibar generally take the form of foreign investment in the tourist industry and bulk cash

smuggling. The most likely sources of illicit funds include Asia and the Middle East, and to a lesser extent Europe. Such transactions rarely include significant amounts of U.S. currency.

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 100,000 shillings (approximately $109) for a period of 10 years.

Current law does not include banker negligence laws. 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. The Central Bank, the Bank of Tanzania (BOT), has issued regulations requiring financial institutions to file suspicious transaction reports (STRs), but this requirement is not being enforced, and no mechanism currently exists for receiving and analyzing the STRs.

The 2002 Prevention of Terrorism Act criminalizes terrorist financing. It also requires all financial institutions to inform the government each quarter as to whether any of their assets or 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 BOT circulates to Tanzanian financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanction Committee's consolidated list, but to date no assets have been frozen under this provision. The Government of Tanzania (GOT) did take action in 2004 against one charitable organization on the list by closing its offices and deporting its foreign directors. However, it is not clear whether Tanzania has the investigative capacity to identify and seize related assets. Tanzania has cooperated with the U.S. in investigating and combating terrorism and exchanging counterterrorism information. There are no specific laws in place allowing Tanzania to exchange record with the U.S. on narcotics transactions and narcotics-related money laundering.

The GOT became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2003. Tanzania is a party to the 1988 UN Drug Convention. It has not yet signed the UN Convention against Transnational Organized Crime. Tanzania is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG). 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 also continues to host the annual ESAAMLG task force meetings.

Tanzania has created a multi-disciplinary committee on money laundering and a drafting committee that has prepared new anti-money laundering (AML) legislation. A Tanzanian Ministry of Finance (MOF) official stated in August 2004 that the drafting committee was in the process of receiving comments on the language of its draft bill from various stakeholders, and that the bill would likely be presented to the Parliament in January 2005. However, the GOT delayed tabling the AML legislation in Parliament. The national multi-disciplinary committee, established with the help of ESAAMLG, revised the draft AML bill from January through May 2005, gaining additional stakeholder input. In May 2005, the Committee presented the AML legislation to the Cabinet for approval. According to officials from the MOF and the BOT, the Cabinet failed to approve and send the AML bill to Parliament due to time constraints and focus on the 2005 national elections. Representatives from the multi-disciplinary committee are hopeful that the legislation will be tabled in Parliament as early as February 2006. Among its other provisions, the proposed legislation provides for the creation of a financial intelligence unit (FIU) that will collect mandatory suspicious transaction reporting from financial institutions and will be empowered to share this information with other FIUs and foreign law enforcement agencies.

Money laundering controls and reporting requirements are not currently applied to non-bank financial institutions, such as cash couriers, casinos, hawaladars and bureaux de change. The draft AML bill

includes the expansion of money laundering controls to cover such institutions. Currently, the BOT supervises bureaux de change through annual audits and inspections, while the National Gaming Authority supervises casinos and other gaming activities involving large sums of money, including lotteries. There are no legal requirements for non-bank financial institutions to report suspicious transactions. There are currently no cross-border currency reporting requirements, even for cash couriers, although the Proceeds of Crime Act does characterize cash smuggling as a "predicate offense." The draft AML bill includes strengthened provisions to criminalize cash smuggling in and out of Tanzania.

The Government of Tanzania should finally enact and implement the anti-money laundering law that has been under review for several years. It should continue to work through the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) to establish the financial intelligence unit (FIU) mandated in the draft law and to otherwise develop a comprehensive anti-money laundering regime that comports with international standards. It should become a party to the UN Convention against Transnational Organized Crime.

Thailand

Thailand is vulnerable to money laundering from its significant underground economy as well as from all types of cross-border crime including illicit narcotics, contraband, and smuggling. Money launderers use both the banking and non-banking financial institutions and private businesses to move funds from narcotics trafficking and other criminal enterprises. As the amount of opium and heroin produced in the Golden Triangle region of Burma, Laos, and Thailand decreased during the past decade, drug traffickers transitioned to importing and distributing methamphetamine tablets, and began using commercial banks to hide and move their proceeds. Thailand is a significant destination and source country for international migrant smuggling and trafficking in persons, a production and distribution center for counterfeit consumer goods, and increasingly a center for the production and sale of fraudulent travel documents. Banks and alternative remittance systems are illegally used to shelter and move funds produced by all of these activities as well as by illegal gambling, illegal lotteries, and prostitution. The majority of reported money laundering cases is narcotics-related, and there is no pervasive evidence of money laundering ties in Thailand with international terrorist groups. The Thai black market for smuggled goods includes pirated goods as well as automobiles from neighboring nations.

Thailand's anti-money laundering legislation, the Anti-Money Laundering Act (AMLA) B.E. 2542 (1999), criminalizes money laundering for the following predicate offenses: narcotics trafficking, trafficking in women or children for sexual purposes, fraud, financial institution fraud, public corruption, customs evasion, extortion, public fraud, blackmail, and terrorist activity. On August 11, 2003, as permitted by the Thai constitution, the Royal Thai Government (RTG) issued two Emergency Decrees to enact measures related to terrorist financing that had been under consideration by the Executive Branch and Parliament for more than a year and a half. The first of these Decrees amended Section 135 of the Penal Code to establish terrorism as a criminal offense. The second Decree amended Section 3 of the AMLA to add the newly established offense of terrorism and terrorist financing as an eighth predicate offense for money laundering. The Decrees took effect when they were published. Parliament endorsed their status as legal acts in April 2004.

The current list of predicate offenses in the AMLA does not comport with international best practices, consistent with Recommendations 1 and 2 of the Forty Recommendations of the Financial Action Task Force (FATF), to apply the crime of money laundering to all serious offenses or with the minimum list of acceptable designated categories of offenses. Additionally, the definition of "property involved in an offense" in the AMLA is limited to proceeds of predicate offenses and does not extend to instrumentalities of a predicate offense or a money laundering offense. Proposed amendments

pending with the Cabinet since 2004 would expand the list of predicate offenses to include environmental crimes, foreign exchange violations, illegal gambling, arms trafficking, labor fraud, bid rigging, share manipulation, and excise tax offenses. However, even with the enactment of these additional predicate offenses, the list will still be deficient under international standards as it excludes, among other crimes, intellectual property rights offenses. The proposed amendments to AMLA would also create a forfeiture fund and authorize international asset sharing with cooperating jurisdictions.

The AMLA created the Anti-Money Laundering Office (AMLO), Thailand's financial intelligence unit (FIU), which became fully operational in 2001. When first established, AMLO reported directly to the Prime Minister. In October 2002, pursuant to a reorganization of the executive branch, AMLO was designated as an independent agency under the Minister of Justice. AMLO receives, analyzes, and processes suspicious and large transaction reports, as required by the AMLA. In addition, AMLO is responsible for investigating money laundering cases for civil forfeiture and for the custody, management, and disposal of seized and forfeited property. AMLO is also tasked with providing training to the public and private sectors concerning the AMLA. The law also created the Transaction Committee, which operates within AMLO to review and approve disclosure requests to financial institutions and asset restraint/seizure requests. The AMLA also established the Anti-Money Laundering Board, which is comprised of ministerial-level officials and agency heads and serves as an advisory board that meets periodically to set national policy on money laundering issues and to propose relevant ministerial regulations. Under the authority of MOUs with other domestic agencies as well as with 23 foreign entities, a total of 57 convictions was a result of 1,215 financial crimes investigations in 2005. AMLO, the Royal Thai Police Special Branch, and the Royal Thai Police Crimes Suppression Division are responsible for investigating financial crimes.

The Ministry of Justice also houses a criminal investigative agency, the Department of Special Investigations (DSI), which is separate from the Royal Thai Police although many DSI personnel originally were RTP officers. DSI has responsibility for investigating the criminal offense of money laundering (as distinct from civil asset forfeiture actions carried out by AMLO), and for many of the money laundering predicates defined by the AMLA, including terrorism. The DSI, AMLO, and the Royal Thai police all have authority to identify, freeze, and/or forfeit terrorist finance-related assets.

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

The Bank of Thailand (BOT), Securities Exchange Commission, and AMLO are empowered to supervise and examine financial institutions for compliance with anti-money laundering/counterterrorist financial laws and regulations. Anti-money laundering controls are also enforced by other Royal Thai Government regulatory agencies, including the Board of Trade, Securities and Exchange Commission, and the Department of Insurance. Financial institutions that are required to report suspicious activities are broadly defined by the AMLA as any business or juristic person undertaking banking or non-banking business. The land registration offices are also required to report on any transaction involving property of five million baht or greater, or a cash payment of two million baht or greater, for the purchase of real property.

The Money Exchange Act of B.E. 2485 (1942), amended in 1984, requires reporting of cash carried in or out of the country in excess of 50,000 baht (approximately $1,250), which is still enforced in theory

but is unrealistic in amount. There is no limitation on the amount of foreign currency that a person can take in or out of Thailand, but it has to be reported. A customer can transfer an unlimited amount of money through a commercial bank, with the required supporting documentation.

Although the Bank of Thailand regulates financial institutions in Thailand, bank examiners are prohibited, except under limited circumstances, from examining the financial transactions of a private individual. This prohibition acts as an impediment to the BOT's auditing of a financial institution's compliance with the AMLA or BOT regulations. Besides this lack of power to conduct transactional testing, BOT does not currently examine its financial institutions for anti-money laundering compliance. The BOT is working closely with AMLO and had hoped to begin such examinations in 2004. The BOT has now agreed that AMLO should be responsible for on- and off-site audits for AMLA compliance, although no such audits have occurred as of yet..

Thailand is not an offshore financial center nor does it host offshore banks, shell companies, or trusts. Licenses were first granted to Thai and foreign financial institutions to establish Bangkok International Banking Facilities (BIBFs) in March 1993. BIBFs may perform a number of financial and investment banking services, but can only raise funds offshore (through deposits and borrowing) for lending in Thailand or offshore. The United Nations Drug Control Program and the World Bank listed BIBFs as potentially vulnerable to money laundering activities, because they serve as transit points for funds. Thailand's 44 BIBFs are subject to the AMLA.

The Stock Exchange of Thailand (SET) requires securities dealers to have "know your customer" procedures; however, the SET does not check anti-money laundering compliance during its reviews. The Department of Insurance (DOI) is responsible for the supervision of insurance companies, which are covered under the AMLA definition of a financial institution, but there are no anti-money laundering regulations for the insurance industry. Similarly, the Cooperative Promotion Department (CPD) is responsible for supervision of credit cooperatives, which are required under the Cooperatives Act to register with the CPD. Currently, around 6,000 cooperatives are registered, with approximately 1,348 thrift and credit cooperatives engaged in financial business. Thrift and credit cooperatives are engaged in deposit taking and providing loans to the members, and are covered under the definition of a financial institution, but, as with the securities and insurance sectors, there are no anti-money laundering compliance mechanisms currently in place.

Financial institutions (such as banks, finance companies, savings cooperatives, etc.), land registration offices, and persons who act as solicitors for investors, are required to report significant cash, property, and suspicious transactions. Reporting requirements for most financial transactions (including purchases of securities and insurance) exceeding two million baht (approximately $52,000), and property transactions exceeding five million baht (approximately $130,000), have been in place since October 2000. However, AMLO has been considering a proposal to lower the threshold for reporting cash transactions to 400,000 baht (approximately $10,500). The proposal is not in effect and the likelihood of its adoption is in doubt, since (in early February 2005) the Prime Minister publicly expressed his opposition to it.

In February 2006, the AMLO Board will consider the issuance of an announcement or regulation to subject gold shops, jewelry stores, and car dealers to either mandatory transactional reporting requirements and/or suspicious transactions reporting requirements over a specified but as of yet undetermined amount. The proposal will also subject those who fail to report to a maximum fine of Bt 300,000 (approximately $78 75). The relevant ministries and regulatory authorities would then issue orders consistent with the AMLO Board pronouncement. Thailand has more than 6,000 gold shops and 1,000 gem traders that would be subject to these reporting requirements.

Thailand acknowledges the existence and use of alternative remittance systems (hawala, etc.) that attempt to circumvent financial institutions. There is a general provision in the AMLA that makes it a crime to transfer, or to receive a transfer, that represents the proceeds of a specified criminal offense

(including terrorism). Remittance and money transfer agents, including informal remittance businesses, require a license from the Ministry of Finance. Guidelines issued in August 2004 by the Ministry of Finance and the BOT prescribe that before the grant of a license, both money changers and money transfer agents are subject to onsite examination by the BOT, which also consults with AMLO on the applicant's criminal history and AML record. At present, moneychangers have to report financial transactions to the Anti-Money Laundering Office (AMLO), while remittance agents do not. Licensed agents are subject to monthly transaction reporting and a 3-year record maintenance requirement. At present, there are about 270 authorized moneychangers and five remittance agents. The Bank of Thailand limited in 2004 the annual transaction volume for agents to $60,000 for offices in the Bangkok area and $30,000 for offices located in other areas. Moneychangers frequently act as illegal remittance agents.

Pursuant to an MOU with AMLO, Royal Thai Customs shares information and evidence of smuggling and customs evasion involving goods or cash exceeding Bt 1 million (approximately $ 26,250)..

Money and property may be seized under Section 3 of the AMLA if derived from commission of a predicate offense, from aiding or abetting commission of a predicate offense, or if derived from the sale, distribution, or transfer of such money or asset. AMLO is responsible for tracing, freezing, and seizing assets. Instruments that are used to support crime such as vehicles or farms are subject to seizure under the Criminal Asset Forfeiture Act of 1991, and unlike the AMLA, require a criminal conviction as a pre-requisite to a final forfeiture. The AMLA makes no provision for substitute seizures if authorities cannot prove a relationship between the asset and the predicate offense. Overall, the banking community in Thailand provides good cooperation to AMLO's efforts to trace funds and seize/freeze bank accounts.

The Bank of Thailand (BOT) does not have any regulations that give it explicit authorization to control charitable donations, but it is working with AMLO to monitor these transactions under the Exchange Control Act of 1942. With respect to charities, there are no regulations that give the BOT explicit authorization to control charitable donations. However, the BOT is working with the Anti-Money Laundering Office to monitor these transactions under the Exchange Control Act of 1942.

In 2004, the Prime Minister's Regulations on Payment of Incentives and Rewards in Proceedings Against Assets Under the Anti-Money Laundering Act went into effect in Thailand. Under this system, investigators from AMLO and other investigative agencies receive personal commissions on the property they seize that is ultimately forfeited. The United States as well as several other countries and international organizations, including the UNODC, have criticized this system of personal rewards on the grounds that it threatens the integrity of its AML regime and creates a conflict of interest by giving law enforcement officers a direct financial stake in the outcome of forfeiture cases. The United States and others have called on the RTG to rescind the reward regulation. Despite initial promises to end the system of personal commissions to law enforcement officers, Thailand has been disappointingly slow to address and correct this discredited practice. As a consequence, the U.S. Government (USG) has ceased providing training and other assistance to AMLO while the rewards practice remains in place. In criminal cases, the forfeiture and seizure of assets is governed by the 1991 Act on Measures for the Suppression of Offenders in an Offense relating to Narcotics (Assets Forfeiture Law). The Property Examination Committee has filed 1,865 cases with assets valued at 1.64 billion baht (approximately $4 million) and 1,644 cases are on trial. Thai authorities seized the equivalent of $18.7 million in non-terrorist assets during 2005, compared to $16.52 million in 2004, and $56.3 million in 2003. The high success rate in 2003 occurred during the Prime Minister's much-criticized war on drugs that year, in which more than 2,000 extra-judicial killings occurred.

Thailand is a party to the 1988 UN Drug Convention. In September 2004, Thailand became a party to the UN International Convention for the Suppression of the Financing of Terrorism. It has signed (December 2000), but not yet ratified, the UN Convention against Transnational Organized Crime. It

has also signed (December 2003), but not yet ratified the UN Convention against Corruption. The RTG has issued instructions to all authorities to comply with UNSCR 1267, including the freezing of funds or financial resources belonging to suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list. To date, Thailand has not identified, frozen, and/or seized any assets linked to individuals or entities included on the UNSCR 1267 Sanctions Committee's consolidated list. However, AMLO has identified some suspicious transaction reports derived from financial institutions and has initiated cases that may involve terrorist activities using non-governmental or non-profit organizations as a front. Thailand has a Mutual Legal Assistance Treaty (MLAT) with a number of countries, including the United States. AMLO has memoranda of understanding on money laundering cooperation with 23 other financial intelligence units (Belgium, Brazil, Lebanon, Indonesia, Romania, UK, Finland, Republic of Korea, Australia, Portugal, Andorra, Estonia, Philippines, Poland, Mauritius, Netherlands, Georgia, Monaco, Malaysia, Bulgaria, St. Vincent and the Grenadines, Ukraine, and Myanmar). AMLO is currently pursuing FIU agreements with 15 more. It nonetheless actively exchanges information with nations with which it has not entered into an MOU, including the United States, Singapore, and Canada. Thailand cooperates with USG and other nations' law enforcement authorities on a range of money laundering and illicit narcotics related investigations. AMLO responded to 99 requests for information from foreign FIUs in 2005. Thailand became a member of the Asia/Pacific Group on Money Laundering (APG), a FATF-style regional body, in April 2001. The AMLO joined the FATF's Egmont Group of financial intelligence units in June 2001.

The Government of Thailand should continue to implement its anti-money laundering program. The money laundering law should be amended to include the minimum list of acceptable designated categories of offenses prescribed by FATF and to make the "structuring" of transactions an offense. While the AMLA already captures proceeds of crime, it should be amended to include instrumentalities of offenses. Non-bank financial institutions and businesses such as gold shops, jewelry stores and car dealers should be subject to suspicious transaction reporting requirement without regard to a threshold. The insurance and securities sectors should institute AML compliance programs. AMLO should undertake audits of financial institutions to ensure compliance with requirements of AMLA and AMLO regulations. Until the RTG provides a viable mechanism for all of its financial institutions to be examined for compliance with the AMLA, Thailand's anti-money laundering regime will not comport with international standards.

The RTG should develop and implement anti-money laundering regulations for exchange businesses and should take additional measures to address the vulnerabilities presented by its alternative remittance systems. The RTG can further strengthen its anti-money laundering regime by promulgating cross border currency control regulations that are currently pending in the Office of Secretary of the Cabinet. Thailand should ratify the UN Convention against Transnational Organized Crime. Thailand should also immediately rescind its rewards program for AMLO investigators who seize assets under the anti-money laundering laws, and for agents of other agencies that engage in such practices, as it gives the appearance of impropriety, can imperil successful prosecutions, and will eventually impede international cooperation and undermine public support for Thailand's forfeiture regime and its credibility.

Turkey

Turkey is an important regional financial center, particularly for Central Asia and the Caucasus, as well as for the Middle East and Eastern Europe. It continues to be a major transit route for Southwest Asian opiates moving to Europe. However, local narcotics trafficking organizations are reportedly responsible for only a small portion of the total funds laundered in Turkey.

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. Since tax evasion is such a large problem, the Government of Turkey (GOT) in 2005 passed a tax administration reform law, with the goal of improving tax collection. There are 21 free trade zones operating in Turkey, but there is no evidence that they are being used in trade-based money laundering schemes or terrorist financing operations. The GOT closely controls access to the free trade zones. Turkey is not an offshore financial center.

Money laundering takes place in both banks and non-bank financial institutions. Money laundering methods in Turkey include: 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, reportedly through alternative remittance systems. The funds are transferred to accounts in the United Arab Emirates, Pakistan, and other Middle Eastern countries. The money is then paid to the Pakistani and Afghan traffickers.

Turkey first criminalized money laundering in 1996. The law included a wide range of predicate offenses, including narcotics-related crimes, smuggling of arms and antiquities, terrorism, counterfeiting, and trafficking in human organs and in persons. Under the law, whoever commits a money laundering offense faces a sentence of two to five years in prison, and is subject to a fine of double the amount of the money laundered and asset forfeiture provisions. The Council of Ministers subsequently passed a set of regulations that require the filing of suspicious transaction reports (STRs), customer identification, and the maintenance of transaction records for five years. These regulations apply to banks and a wide range of non-bank financial institutions, including insurance firms and jewelry dealers.

In 2004, the GOT enacted additional anti-money laundering legislation, a new criminal law, and a new criminal procedures law. The new Criminal Law, which took effect in June 2005, broadly defines money laundering to include all predicate offenses punishable by one year's imprisonment. Previously, Turkey's anti-money laundering law comprised a list of specific predicate offenses. A new Criminal Procedures Law also came into effect in June 2005.

In July 2001, the Ministry of Finance issued a banking regulation circular requiring all banks, including the Central Bank, securities companies, post office banks, and Islamic financial houses, to record tax identity information for all customers opening new accounts, applying for checkbooks, or cashing checks. The circular also requires exchange offices to sign contracts with their clients. The Ministry of Finance also 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 to other financial entities. The requirements are intended to increase the Government's ability to track suspicious financial transactions. Turkey does not have bank secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement officials. According to anti-money laundering law Article 5, public institutions, individuals, and corporate bodies must submit information and documents as well as adequate supporting information upon the request of Turkey's Financial Crimes Investigation Board (MASAK) or other authorities specified in Article 3 of the law. Natural persons and corporate bodies from whom information and documents are requested may not withhold the requested items by claiming the protection provided by privacy provisions in order to avoid submitting the requested items. A new Banking Law was enacted in 2005 to strengthen bank supervision, pursuant to which the Banking Regulatory and Supervisory Agency (BRSA) conducts periodic anti-money laundering and compliance reviews under authority delegated by MASAK. The number of STRs currently being filed is quite low, even taking into consideration the fact that many commercial transactions are conducted in cash. A possible reason for this is the lack of safe harbor protection for bankers and other filers of STRs. In 2004, 289 STRs were filed; for the period January-November 2005, 266 STRs were filed.

Turkey does not have foreign exchange restrictions. With limited exceptions, banks and special finance institutions must inform authorities, within 30 days, about transfers abroad exceeding $50,000 or its equivalent in foreign currency notes (including transfers from foreign exchange deposits). Travelers may take up to $5,000 or its equivalent in foreign currency notes out of the country. Turkey does have cross-border currency reporting requirements.

MASAK was established by the 1996 anti-money laundering law as part of the Ministry of Finance. MASAK became operational in 1997, and it serves as Turkey's Financial Intelligence Unit (FIU), receiving, analyzing, and referring STRs for investigation. Under current law, MASAK has three functions: regulatory, financial intelligence, and investigative. MASAK plays a pivotal role between the financial community, on the one hand, and Turkish law enforcement, investigators, and judiciary, on the other. MASAK's most critical training and equipment needs are being addressed by a European Union accession project, which is expected to end in June 2006.

In November 2005, the GOT submitted to Parliament a new law under which MASAK would cede its investigative function to the Public Prosecutor's Office, while retaining its financial intelligence and regulatory roles. The proposed law would reorganize MASAK along functional lines, explicitly criminalize the financing of terrorism, and provide safe harbor protection to the filers of STRs. The law also expands the range of entities subject to reporting requirements, to include art dealers, pension funds, exchange houses, jewelry stores, notaries, sports clubs, and real estate companies. It also specifies sanctions for failure to comply. The law is currently under review in Parliament, and passage is expected in 2006. However, the current draft of the legislation does not expand upon Turkey's defining terrorism only in terms of attacks on Turkish nationals or the Turkish state.

According to MASAK statistics, it has pursued more than 2,100 money laundering investigations since its inception, but as of July 2005, only eight had resulted in convictions. One factor contributing to this low conviction rate is the fact that Turkey's police, prosecutors, judges, and investigators need additional training in dealing with financial crimes. In addition, there is a lack of coordination among law enforcement agencies, and between the courts that prosecute the predicate offenses and those that prosecute money laundering cases. Most of the cases involve non-narcotics criminal actions or tax evasion; roughly 30 percent are narcotics-related.

The GOT enforces existing drug-related asset seizure and forfeiture laws. MASAK, the Turkish National Police, and the Courts are the government entities responsible for tracing, seizing and freezing assets. According to Article 9 of the anti-money laundering law, the Court of Peace—a minor arbitration court for petty offenses—has the authority to issue an order to freeze funds held in banks and non-bank financial institutions as well as other assets, and to hold the assets in custody during the preliminary investigation. During the trial phase, the presiding court has freezing authority. Public Prosecutors may freeze assets in cases where it is necessary to avoid delay. The Public Prosecutors' Office notifies the Court of Peace about the decision within 24 hours. The Court of Peace has 24 hours to decide whether to approve the action. There is no time limit on freezes. There is no provision in Turkish law for the sharing of seized assets with other countries.

In February 2002, MASAK issued General Communiqué No. 3, which requires that a special type of STR be filed by financial institutions in cases of suspected terrorist financing. However, until the revised MASAK law is in place, terrorist financing is still not explicitly defined as a criminal offense under Turkish law. Various existing laws with provisions that can be used to punish the financing of terrorism include articles 220, 314, and 315 of the Turkish penal code, which prohibit assistance in any form to a criminal organization or to any organization that acts to influence public services, media, proceedings of bids, concessions, and licenses, or to gain votes, by using or threatening violence. To commit crimes by implicitly or explicitly intimidating and cowing people is illegal under the provisions of the Law No. 4422 on the Prevention of Benefit-Oriented Criminal Organizations. The

GOT distributes to interested GOT agencies and financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list.

Another area of vulnerability in the area of terrorist financing is the GOT's loose supervision of non-profit organizations. The General Director of Foundations (GDF) issues licenses for charities and oversees them. The GDF keeps a central registry of charities, and it requires charities to verify and prove their funding sources and to have bylaws. Charities are audited by the GDF and are subject to being shut down if they act outside the bylaws. However, the GOT does not have other oversight mechanisms, such as requiring the publication of annual reports or periodic reporting to competent authorities. Alternative remittance systems are illegal in Turkey, and in theory only banks and authorized money transfer companies are permitted to transfer funds. However, there is anecdotal evidence that alternative remittance systems exist.

The Council of Ministers promulgated a decree (2483/2001) to freeze all the funds and financial assets of individuals and organizations included on the UNSCR 1267 Sanctions Committee's consolidated list, which is distributed to all relevant agencies and financial institutions. However, the tools currently available under Turkish law for locating, freezing, seizing, and confiscating terrorist assets are cumbersome, limited, and not particularly effective. For example, there is no legal mechanism to freeze the assets of terrorists not on the consolidated list. According to MASAK statistics, no assets linked to terrorist organizations or terrorist activities were frozen in 2005. Turkey has a system for identifying, tracing, freezing, and seizing assets that are not related to terrorism, although the law allows only for their criminal forfeiture and not their administrative forfeiture. Article 7 of the anti-money laundering law provides for the confiscation of all property and assets (including derived income or returns) that are the proceeds of a money laundering predicate offense (soon to be expanded to crimes punishable by one year imprisonment), once the defendant is convicted. The law allows for the confiscation of the equivalent value of direct proceeds that could not be seized. Instrumentalities of money laundering can be confiscated under the law. In addition to the anti-money laundering law, Articles 54 and 55 of the Criminal Code provide for post-conviction seizure and confiscation of the proceeds of crimes. The defendant, however, must own the property subject to forfeiture. Legitimate businesses can be seized if used to launder drug money or support terrorist activity, or are related to other criminal proceeds. Property or its value that is confiscated is transferred to the Treasury.

The GOT cooperates closely with the United States and with its neighbors in the Southeast Europe Cooperation Initiative (SECI). Turkey and the United States have a Mutual Legal Assistance Treaty (MLAT) and cooperate closely on narcotics and money laundering investigations. Turkey is a member of the Financial Action Task Force (FATF). MASAK is a member of the Egmont Group. Turkey is a party to the 1988 UN Drug Convention, the UN International Convention for Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Turkey has signed and ratified the COE Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime, which came into force on February 1, 2005. In December 2005, Parliament's Foreign Affairs Committee adopted a draft law ratifying the UN Convention against Corruption, a step toward final ratification. However, Turkey's implementation efforts on UN anti-financial crime conventions have been weak thus far, and Turkey is probably not currently in compliance with the FATF's Special Recommendations on Terrorist Financing. The new MASAK law will improve Turkey's level of compliance with these special recommendations.

With the passage of several new pieces of legislation, the Government of Turkey took positive steps in 2005 to strengthen its anti-money laundering and counterterrorist financing regime. It now faces the challenge of decisively implementing these laws and of securing final passage of the MASAK law that will, among other provisions, specifically criminalize terrorist financing in support of international terrorist groups. Turkey should improve its coordination among the various entities charged with responsibility in its anti-money laundering and counterterrorist financing regime, including the various courts with responsibilities for these issues, in order to increase the number of successful

investigations and prosecutions. Turkey should also regulate and investigate alternative remittance networks to thwart their potential misuse by terrorist organizations or their supporters. It should also strengthen its oversight of charities.

Turks and Caicos

The Turks and Caicos Islands (TCI) is a Caribbean overseas territory of the United Kingdom (UK). 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. As of 2003, 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. In 2005, the Financial Services Commission employed a staff of 22 and recently hired an experienced regulator to bolster the on-site examination process. 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 licensed custodian. This applies to all shares issued after enactment and allows for a phase-in period for existing bearer shares of two years. Trust legislation allows establishment of asset protection trusts inoculating assets from civil adjudication by foreign governments; however, the Superintendent of Trustees has investigative powers and may assist overseas regulators. Currently, the FSC is rewriting the Trust legislation.

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 Managing Director of the FSC and the Head of the Financial Crimes Unit (FSU). the Superintendent of the FSC, the Commissioner of Police, and the Superintendent of the Criminal Investigation Department. The MLRA is authorized to disclose information it receives to domestic law enforcement and foreign governments.

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

In 1999, the FSC, acting as the secretary for the MLRA, issued non-statutory Guidance Notes to the financial sector, in order to help educate the industry regarding money laundering and the TCI's anti-money laundering requirements. Additionally, it provided practical guidance on recognizing suspicious transactions. The Guidance Notes instruct institutions to send SARs to either the Royal Turks & Caicos Police Force or the FSC. Officials forward all 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. However, 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 Government of the Turks and Caicos Islands 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. Recently, a number of on-site examinations were conducted and one resulted in an enforcement action against an institution. Notwithstanding, the current regulatory structure is not fully in accordance with international standards The Turks and Caicos Islands should criminalize the financing of terrorists and terrorism, and enhance its on-site supervision program. Turks and Caicos Islands should expand efforts to cooperate with foreign law enforcement and administrative authorities. Turks and Caicos Islands 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 Turks and Caicos Island's financial sector.

Uganda

Uganda is not a regional financial center and is not a major hub for narcotics trafficking or terror finance. It appears that a large percentage of the money laundering in Uganda stems from domestic criminal actions, often related to smuggling counterfeit products, and other financial fraud. Large drug-trafficking organizations, organized crime groups, and terror groups have historically not played a leading role in money laundering activities in the country. However, some of Uganda's weaknesses in monitoring financial transactions, and the widespread use of cash may make it a potential target for money laundering in the future. The Government of Uganda (GOU) does not effectively monitor cross-border financial activities. A draft comprehensive anti-money laundering bill based on the Financial Action Task Force's (FATF) Forty Recommendations has yet to be adopted by Parliament. The GOU anticipates the legislation will be passed after the national elections scheduled for February or March 2006.

Annual remittances from Ugandans living abroad are estimated at over $800 million. Money laundering also occurs in the informal financial sector. Many Ugandans working abroad use alternate,

cash-based, informal remittance systems to send money back to their families. The extensive use of cash instead of other financial instruments, even for major purchases such as real estate, further hinders the ability of authorities to monitor financial transactions. Many establishments in Uganda accept U.S. dollars for cash transactions. Under legislation passed in 2004, foreign exchange bureaus are not authorized to transfer money abroad. The GOU has no effective means to prevent money launderers from accessing the many charitable and faith-based organizations that operate in Uganda. Moreover, to date, the GOU has not been able to determine whether money launderers have used these entities.

Uganda does not have an offshore banking sector. The Special Economic Zones Bill of 2002 authorized the creation of export-processing zones (EPZs) and free trade areas within Uganda, and the GOU recently received a $24 million World Bank credit to establish EPZs. However, the GOU has yet to develop either EPZs or free trade areas. In 2001, Uganda criminalized narcotics-related money laundering. In 2003, the Bank of Uganda issued "Know Your Customer" guidelines for Ugandan commercial banks. Although some banks are implementing such guidelines, the GOU has been unwilling to enforce compliance. Until the daft anti-money laundering legislation passes, the GOU maintains only limited authority and ability to investigate and prosecute money laundering related violations. Despite the weaknesses in the laws, the Directorate of Public Prosecutions (DPP) reports that it is has successfully prosecuted numerous cases relating to organized crime and money laundering.

Beginning in 2004, the Bank of Uganda circulated to financial institutions the list of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list. The Bank of Uganda (BOU) has the power to freeze the assets of specific terrorist entities designated as terrorist organizations pursuant to the Anti-Terrorism Act (ATA) of 2002. The BOU also may require a bank to freeze customer assets in response to an outside request made in accord with a legally binding international convention to which Uganda has signed and ratified. The ATA criminalizes contributing, soliciting, controlling or managing funds used to support terrorism or terror organizations. Despite the ATA, GOU authorities believe they have limited powers to freeze or seize terrorist finance-related assets. The Solicitor General has said the draft anti-money laundering bill would significantly expand this authority allowing the GOU to seize all proceeds of crime.

Uganda is a member of the East and Southern African Anti-Money Laundering Group (ESAAMLG) and served as chair from August 2003 to August 2004. Uganda is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the United Nations Convention against Transnational Organized Crime. At this time, Uganda and the United States do not have formal agreements to facilitate the exchange of information and records in connection with investigations relating to narcotics, terrorism, and other crimes. Nevertheless, Ugandan authorities have cooperated with U.S. law enforcement efforts. In May 2004, at the request of the United States, the GOU detained and deported two U.S. citizens to face money laundering and wire fraud charges in the U.S.

The Government of Uganda should pass the draft legislation pending since December 2003 to provide comprehensive anti-money laundering legislation that meets international standards. The GOU should establish a Financial Intelligence Unit (FIU). The GOU and financial sector should adopt better technology for efficient monitoring of financial transactions. Finally, the GOU should provide training to bankers, police investigators and prosecutors to improve awareness of money laundering schemes and their respective duties to prevent it.

Ukraine

Despite a government crackdown on corruption, organized crime, smuggling, and tax evasion, these problems continue to plague Ukraine's economy and to provide an impetus to money laundering.

Trafficking in persons and other organized criminal activity also continue to be associated with money laundering. Among the new Government's initiatives are the reduction of import duties, new procedures for the Customs Service, and the introduction of more transparent procedures for the privatization of state enterprises. Ukraine's revised budget, passed in March 2005, eliminated the eleven Free Economic Zones (FEZs), and nine Priority Development Territories, that had operated on Ukrainian territory. Legislative loopholes had permitted companies to misuse FEZ status, and to avoid taxes and import duties. It has been nearly two years since Ukraine adopted comprehensive anti-money laundering legislation and established its anti-money laundering regime, and the Government of Ukraine has introduced numerous legislative and regulatory improvements since that time.

In September 2001, the Financial Action Task Force (FATF) placed Ukraine on the list of non-cooperating countries and territories in the fight against money laundering (NCCT). The FATF's report noted that Ukraine lacked: a complete set of anti-money laundering laws; an efficient mandatory system for reporting suspicious transactions to a financial intelligence unit; adequate customer identification requirements; and adequate resources 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. The FATF gave Ukraine until October 2002 to enact comprehensive and effective anti-money laundering legislation or face the possibility of a call on member countries to impose countermeasures.

At its September 2002 plenary, FATF extended its original October 2002 deadline until December 15, 2002. On November 28, 2002, the President 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 recommended that FATF members impose countermeasures on Ukraine. Under Section 311 of the USA PATRIOT Act, the United States designated Ukraine as a jurisdiction of primary money laundering concern on December 20, 2002. In response to the imminent threat of countermeasures, Ukraine passed further comprehensive legislative amendments in December 2002 and February 2003. 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 AML legislation, Ukraine was not only able to avoid the recommendation for countermeasures, but also 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 was conducted on January 19-23, 2004. The results of the on-site visit by the FATF evaluation team were reported to the FATF ERG prior to the Paris plenary on February 25, 2004. Ukraine was de-listed from the NCCT list in March 2004. Over one year after de-listing, Ukraine reported to the ERG on implementation of anti-money-laundering legislation. In December 2005, the Parliament passed legislation addressing the last of the FATF concerns regarding limitations on information exchange. If the President signs this law, the FATF's enhanced monitoring of Ukraine under the NCCT process may be near its end.

As a member of the Council of Europe, Ukraine has undergone three 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 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 non-drug 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 $1,000 must be declared by travelers. The National Bank of Ukraine (NBU) drafted amendments to the Act strengthening anti-money laundering requirements for banks. In particular, it requires: banks to provide information on bank owners and managers to the NBU; banks to install someone at a management level to be responsible for anti-money laundering supervision; and forbids banks to have correspondent accounts with shell banks.

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

In November 2004, the GOU approved and sent to Parliament for review a draft law "On Amending Some Legislative Acts of Ukraine on Prevention to Legalization (Laundering) of the Proceeds from Crime and Terrorist Financing." Though the Parliament did not get enough votes to adopt a law intended to implement the revised FATF Forty Recommendations on Money Laundering, the Rada plans to vote on it again. The new law would expand the sphere of primary monitoring to include retail traders, lawyers, accountants, and traders of precious metals.

Legislation passed by the Parliament in December 2005 and expected to take effect January 1, 2006 has two major provisions. First, it orders the National Bank to develop procedures obligating banks to freeze assets for two days and immediately inform the FIU whenever a party to a transaction appears on the Cabinet of Minister's list of beneficiaries of or parties to terrorist financing. Second, as discussed above, it improves the National Bank's ability to initiate information exchange internationally on both money laundering and terrorist finance, in accordance with the FATF Recommendations.

The Parliament has not yet, however, passed legislation putting in place FATF's Forty plus Nine recommendations. Instead, the government's draft law was rejected in two votes in the Parliament in

2005. The government has redrafted the law, narrowing its scope to the FATF recommendations only, and leaving for other legislation certain new authorities and bureaucratic changes that had drawn opposition in the Parliament. The government has submitted the new draft to the Parliament, but it has not yet been scheduled for a vote.

The current AML law calls for customer identification, reporting of suspicious and unusual transactions to the State Committee for Financial Monitoring, and five years of record-keeping. It also mandates the establishment of anti-money laundering procedures in 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 of relating to money laundering or terrorism financing. The AML legislation includes a "safe harbor" provision that protects reporting institutions from liability for cooperating with law enforcement agencies.

The monetary threshold beyond which transactions and operations are subject to compulsory financial monitoring was reduced in 2004 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 exists 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 (subsequently renamed the State Committee for Financial Monitoring -SCFM) by January 1, 2002, to function as Ukraine's financial intelligence unit (FIU). Under the terms of this decree, the SCFM 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. With its law of March 18, 2004, the Rada granted the SCFM the status of a Central Executive agency, subordinating it to the Cabinet of Ministers, rather than the Finance Ministry. The change elevates the SCFM's status and came into effect on January 1, 2005.

Since January 2005, the SCFM has opened five branches in Ukraine's regions, and is in the process of establishing four more. Ultimately, the SCFM plans to have 15 such branches. 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 is vested in the SCFM, which became operational on June 12, 2003, in accordance with Article 4 of the AML law.

The SCFM is an administrative agency with no investigative or arrest authority. It is authorized to collect and analyze suspicious transactions, including those related to terrorist financing, and to transfer financial intelligence information to competent law enforcement authorities for investigation. The SCFM also has 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 2005, memoranda of understanding were concluded between the SCFM and the FIUs of Russia, Slovakia, Estonia, Spain, Belgium, the Czech Republic, Colombia, Georgia, France, Serbia, Poland, Romania, Portugal, Cyprus, Brazil, Panama, Macedonia, Bulgaria, Lithuania, Italy, Slovenia, Thailand, Mexico, Peru, and Albania.

Overall, the SCFM has demonstrated a high level of competence in processing, analyzing, and developing cases to the point, some believe, of establishing the equivalent of probable cause prior to referral to law enforcement. The SCFM has responded to foreign requests for information in a timely fashion and in exceptional detail and has become a regional leader in the volume of case information exchanged with counterpart FIUs. The SCFM acknowledges the existence and use of alternative remittance systems such as hawala in Ukraine. SCFM personnel have attended seminars and exchanged information about such systems. The SCFM and security agencies monitor charitable organizations and other nonprofit entities that might be used to finance terrorism.

In 2004, the SCFM received 725,959 suspicious transaction reports (STRs), the bulk of which have been reported by banks. Approximately eight percent of these have been identified by the FIU for "active research" and 164 separate cases have been sent to competent law enforcement agencies. From January to August 2005, the SCFM received about 422,000 STRs. Over that same period, the SCFM referred 67 cases to the General Prosecutor's Office, 79 cases to the State Tax Administration, 91 cases to the Ministry for Internal Relations, and 93 cases to the Security Service. As a result of subsequent investigation, law enforcement agencies initiated 72 criminal cases, ten of which were brought to court. During the first half of 2005, law enforcement agencies (Prosecutor General's Office, Ministry of Internal Affairs, Tax Police, State Security Service) completed investigation and transferred to court 164 criminal cases on money laundering charges. While the reporting system works as intended and the financial intelligence unit (FIU) has generated cases, law enforcement authorities and prosecutors have not shown notable success in bringing those cases to successful conclusion. Observers believe the key problem to be local prosecutors who close money laundering investigations and cases arbitrarily, likely because of corruption.

Ukraine has an asset forfeiture regime. Article 59 of the Ukrainian Criminal Code provides for the forceful seizure of all or a part of the property of a convicted person for grave and special grave offenses as set forth in the relevant part of the code. With respect to money laundering, Article 209 allows for the forfeiture of criminally obtained money and other property.

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. This is a functioning system that unites data bases of 17 ministries and agencies. In order to foster better interagency cooperation, on September 22, 2005, the Cabinet of Ministers adopted a resolution establishing a Governmental Coordination Council on Functioning of a Unified State Informational System. It unites high-level governmental officials in the Cabinet of Ministers, Ministries of Economy, Finance, Interior, Customs Office and others.

A draft resolution to give the Security Service of Ukraine authority to investigate terrorist financing based on international terrorist lists is pending before the Cabinet of Ministers. There is no explicit criminal penalty for terrorist financing. However, Article 258 of the Criminal Code envisages a criminal penalty for supporting terrorism. The GOU has cooperated with U.S. 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 suspected 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 suspected terrorists and terrorist organizations on the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224. 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 the UN 1267 Sanctions Committee's consolidated list. The amendments to the law passed in December 2005 will further strengthen Ukraine's anti-money laundering regime.

In June 2004, the SCFM joined the Egmont Group. The SCFM received an invitation to participate in the Egmont working groups and in July was connected to the Egmont Secure Website (ESW), used for information exchange between FIUs. The U.S.-Ukraine Treaty on Mutual Legal Assistance in Criminal Matters was signed in 1998 and entered into force in February 2001. A bilateral Convention for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with respect to Taxes on Income and Capital, which provides for the exchange of information in administrative, civil and criminal matters, is also in force.

Ukraine is a party to the 1988 UN Drug Convention, the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Ukraine is a party to the European Convention on the Suppression of Terrorism, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Ukraine is also a signatory to the UN Convention against Corruption.

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 most significant obstacle to effective performance of the AML regime in the country is the likely compromising of money laundering cases by corrupt prosecutors and law enforcement officials at the local level. The GOU should take action to establish oversight capabilities of local investigators, prosecutors and judges to insure that cases are vigorously pursued and prosecuted. The GOU has taken laudable steps in 2005 to enhance its legal regime for combating terrorist financing, but it should amend its criminal code to criminalize the financing of terrorists and terrorism. Law enforcement agencies should give higher priority to investigating money laundering cases. Both law enforcement officers and the judiciary need a better understanding of the theoretical and practical aspects of investigating and prosecuting money laundering cases.

United Arab Emirates

The United Arab Emirates (UAE) is an important financial center in the Persian Gulf region. The UAE is still a largely cash-based society. However, the financial sector is modern and progressive. Dubai, in particular is a major international banking center. There is also a growing offshore sector. The UAE's robust economic development, political stability, and liberal business environment have attracted a massive influx of people and capital. Because of the UAE's geographic location and its role as the primary transportation and trading hub for the Gulf States, East Africa, and South Asia, and with its expanding trade ties with the countries of the former Soviet Union, the UAE has the potential to be a major center for money laundering. The large number of resident expatriates from the above regions, many of whom are engaged in legitimate trade with their homelands, or send remittances there, exacerbates that potential. Approximately 80 percent of the UAE population is comprised of non-nationals. Given the country's close proximity to Afghanistan, where most of the world's opium is produced, narcotics traffickers are increasingly reported to be attracted to UAE's financial centers.

Following the September 11 terrorist attacks in the United States, and amid revelations that terrorists had moved funds through the UAE, the Emirates' authorities acted swiftly to address potential vulnerabilities. In close concert with the United States, the UAE imposed a freeze on the funds of groups with terrorist links, including the Al-Barakat organization, which was headquartered in Dubai. Both 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. Since 2001, the UAE Government (UAEG) has taken steps to better monitor cash flows through the UAE financial system and to cooperate with international efforts to combat terrorist financing. The UAE has enacted two laws that serve as the foundation for the country's anti-money laundering (AML) and counterterrorist financing

(CTF) efforts: Law No. 4/2002, the anti-money laundering law, and Law No. 1/2004, the counterterrorism law.

Law No. 4 of 2002 criminalizes all forms of money laundering activities. The law calls for stringent reporting requirements for wire transfers exceeding $545 and currency imports above $10,900. 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. It also provides safe harbor provisions for those who report such crimes. Although the anti-money laundering law criminalizes money laundering, it is administrative Regulation No. 24/2000 that provides guidelines for how financial institutions are to monitor for money laundering activity.

This regulation requires banks, money exchange houses, finance companies, and any other financial institutions operating in the UAE to follow strict know your customer guidelines. Additionally, financial institutions must verify the customer's identity and maintain transaction details (including name and address of originator and beneficiary) for all exchange house transactions over $545 and for all non-account holder bank transactions over $10,900. The regulation delineates the procedures to be followed for the identification of natural and juridical persons, the types of documents to be presented, and rules on what customer records must be maintained on file at the institution. Other provisions of Regulation 24/2000 call for customer records to be maintained for a minimum of five years and further require that they be periodically updated as long as the account is open.

On July 29, 2004, the UAE strengthened its legal authority to combat terrorism and terrorist financing, by passing Federal Law Number 1 of 2004 on Combating Terror Crimes (Law No. 1/2004). The law sets stiff penalties for the crimes covered, including life imprisonment and the death penalty. It also provides for asset seizure or forfeiture. Under the law, founders of terrorist organizations face up to life imprisonment. The law also penalizes the illegal manufacture, import, or transport of "non-conventional weapons" or their components, with the intent to use them in a terrorist activity.

Law No. 1/2004 specifically criminalizes the funding of terrorist activities or terrorist organizations. Article 12 provides that raising or transferring money with the "aim or with the knowledge" that some or all of this money will be used to fund terrorist acts is punishable by "life or temporary imprisonment," whether or not these acts occur. Law No. 1/2004 grants the Attorney General (or his deputies) the authority to order the review of information related to the accounts, assets, deposits, transfer, or property movements on which the Attorney General has "sufficient evidence to believe" are related to the funding or committing of a terror activity stated in the law. The law also provides for asset seizure and confiscation. Article 31 gives the Attorney General the authority to seize or freeze assets until the investigation is completed. Article 32 confirms the Central Bank's authority to freeze accounts for up to seven days if it suspects that the funds will be used to fund or commit any of the crimes listed in the law. The law also allows the right of appeal to "the competent court" of any asset freeze under the law. The court will rule on the complaint within 14 days of receiving the complaint. Through 2005, there are no reported criminal convictions for money laundering or terrorist financing under either the 2002 or the 2004 laws.

Law No. 1/2004 also sets up a "National Anti-Terror Committee" with representatives from the Ministries of Foreign Affairs, Interior, Justice, and Defense, the Central Bank, the State Security Department, and the Federal Customs Authority. The Committee serves as a UAE interagency liaison, implements UN Security Council Resolutions on terrorism, and shares information with its foreign counterparts as well as with the United Nations (UN).

The UAE's national anti-money laundering committee (NAMLC) is responsible for coordinating anti-money laundering policy. It is chaired by the Central Bank (CB) 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).

The supervision of the UAE banking and financial sector (including banks, exchange houses, and investment companies) falls under the authority of the CB. The CB issues licenses to financial institutions under its supervision and can impose administrative sanctions for compliance violations. The CB issues instructions and recommendations as it deems appropriate and is permitted to take any necessary measures to ensure the integrity of the UAE's financial system. The CB has issued a number of circulars outlining the requirements for customer identification and providing for a basic suspicious transaction-reporting obligation.

Law 4/2002 provided for the establishment of the Anti-Money Laundering and Suspicious Case Unit (AMLSCU), which acts as the financial intelligence unit (FIU) and is housed within the CB. 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. The AMLSCU—a member of the Egmont Group since June 2002—exchanges information with foreign FIUs on a reciprocal basis, and has provided information relating to investigations carried out by the United States and other countries. Since December 2000, the CB has referred 108 cases to foreign FIUs.

From December 2000 to December 2005, the AMLSCU has received and investigated 3031 suspicious transactions reports (STRs). From December 2004 to December 2005, the AMLSCU received and investigated 772 STRs. No freeze orders were issued in 2005 based on STR submissions, but from December 2000 to December 2005, the CB has issued 27 freeze orders based on AMLSCU and law enforcement investigations. Twelve of those cases are in the process of prosecution for money laundering and confiscation of proceeds. The CB circulates to all financial institutions under its supervision the UNSCR 1267 Sanctions Committee's consolidated list of suspected terrorists and terrorist organizations. Since 2000, it has frozen $1,348,381 in 17 accounts based on the UNSCR 1267 list.

Some money laundering in the UAE occurs in the formal banking system, including the numerous money exchange houses, but it is likely more prevalent in the informal and largely undocumented hawala remittance system. The fact that hawala is an undocumented and nontransparent system, and is highly resilient despite 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 confronting its vulnerability to the unregulated use of hawala. New regulations to improve oversight of the hawala system were implemented in 2002, when the CB required hawala brokers to register, submit the names and addresses of senders and beneficiaries, and to file suspicious transaction reports.

As of November 30 2005, 184 hawala brokers (hawaladars) have applied to register with the CB. The CB has issued hawaladar certificates to 163 of the applicants, and the remaining 21 applicants are in the process of fulfilling CB registration requirements. The central bank conducts one-on-one training sessions with each registered hawaladar to ensure the dealer understands the record-keeping and reporting obligations. There is no accurate estimate of the total number of UAE-based hawala brokers, and there is no penalty for failure of hawaladars to register.

In April 2005, the UAE hosted its third international conference on hawala, which was attended by over 400 participants from 74 countries. Delegates included government officials, executives of supervisory institutions, banking experts, and law enforcement officials from the Middle East, United States, Latin America, Asia, and Europe. The conference statement recognized the key role that hawala and other informal funds transfer systems play in facilitating remittances, particularly those of migrant workers, although such systems can be abused for illegal activities. Speakers discussed ways to ensure hawala is regulated, without driving the system further underground.

This attention to hawala may be encouraging more people in the country to use regulated exchange houses. Representatives of money exchange business noted that their sector could transfer money anywhere, even to a private residence, for a fee competitive with hawala, persuading many to use the formal, and more secure, banking network.

There are no limits on how much cash can be imported into or exported from the country. However, the UAE Central Bank requires that individuals declare cash imports above $10,900. The regulations provide customs services with the authority to seize undeclared cash; however, enforcement is still lacking, and the declaration requirements are not well publicized. The UAE is a cash-based economy, and it is not unusual for people to carry significant sums of cash around. As such, customs officials tend to not regard large cash imports as suspicious or possibly criminal.

The 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 has participated in the Kimberley Process Certification Scheme for Rough Diamonds (KPCS) since November 2002, and began certifying rough diamonds exported from the UAE on January 1, 2003. In 2004, the UAE was the first KPCS participant country to volunteer for a "peer review visit" on internal control mechanisms.

The Dubai Metals and Commodities Center (DMCC) is the quasi-governmental organization charged with issuing Kimberly Process (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 certificate.

The Securities and Commodities Authority (SCA) supervises the country's two stock markets. In February 2004, it sent out anti-money laundering guidelines to brokers and the markets, instructing them to verify client information when opening accounts and created a reporting requirement for cash transactions above $10,900. The SCA also instructed the markets and brokers to file suspicious transaction reports for initial analysis before forwarding them to the AMLSCU for further action. The instructions also provide for a five-year record keeping requirement.

Dubai's booming property market is also susceptible to money laundering abuse. In 2002, Dubai permitted three companies to sell "freehold" properties to non-citizens. Several other emirates have announced their intention to follow suit. Abu Dhabi has passed a property law, which provides for a type of lease-hold ownership for non-citizens; although by the end of 2005 it had not yet identified any areas where expatriates can invest. The intense interest in these properties, and rumors of cash purchases, has sparked concerns about the potential for money laundering. As a result, developers have stopped accepting cash purchases, alleviating some of the concerns about money laundering activities in this sector of the economy.

The UAEG is much more sensitive since September 11 to the oversight of charities and accounting for transfers abroad. In 2002, the UAEG mandated that all licensed charities interested in transferring funds overseas must do so via one of three umbrella organizations: the Red Crescent Authority, the Zayed Charitable Foundation, or the Muhammad Bin Rashid Charitable Trust. These three quasi-governmental bodies are in a position to ensure that overseas financial transfers go to legitimate parties. As an additional step, the UAEG has contacted the governments in numerous aid receiving countries to compile a list of recognized acceptable recipients for UAE charitable assistance. The UAE Ministry of Labor and Social Affairs (MLSA) licenses and monitors registered charities in Abu Dhabi and the northern emirates. These charities are required to keep records of donations and beneficiaries and submit annual reports to the MLSA. Charities in Dubai are licensed and monitored by the Dubai Department of Islamic Affairs and Charitable Activities.

The UAE has both free trade zones (FTZs) and financial free zones (FFZs). There are a growing number of free trade zones (FTZs), with 17 already in operation and plans to establish eleven more. Every emirate except Abu Dhabi has at least one functioning FTZ. The free trade zones are monitored by emirate-level (as opposed to federal) authorities.

There are 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. However, UAE law prohibits the establishments of shell companies and trusts, and does not permit non-residents to open bank accounts in the UAE. The larger FTZs in Dubai (such as Jabal Ali free zone) are well-regulated. Although it is not impossible that some trade-based money laundering occurs in the large FTZs, there is a higher potential for it in some of the smaller FTZs in the northern emirates.

In March 2004, the UAEG passed Federal Law No. 8 Regarding the Financial Free Zones (FFZs) (Law No. 8/2004). The new law exempts FFZs and their activities from UAE federal civil and commercial laws, but subjects them and their operations to federal criminal laws including the Anti-Money Laundering Law No. 4/2002 and the Anti-Terror Law No. 1/2004. The new law and a subsequent federal decree also allowed for the establishment, in September 2004, of the UAE's first financial free zone (FFZ), known as the Dubai International Financial Center (DIFC). In September 2005, the DIFC opened its securities market—the Dubai international financial exchange (DIFX).

Law No. 8/2004 limits licenses for banking activities in the FFZs to branches of companies, joint companies, and wholly owned subsidiaries, provided that they "enjoy a strong financial position and systems and controls, and are managed by persons with expertise and knowledge of such activity." The law prohibits companies licensed in the financial free zone from dealing in UAE currency (dirham) or taking "deposits from the state's markets." It further stipulates that the licensing standards of companies "shall not be less than those applicable in the state." The law empowers the Emirates Stocks and Commodities Authority to approve the listing of any company listed on any UAE stock market in the financial free zone and the licensing of any UAE licensed broker. The law limits any insurance activity in the UAE carried out by a financial free zone company to that of reinsurance. It further gives competent authorities in the Federal Government the power to inspect financial free zones and submit their findings to the UAE cabinet. According to DFSA regulators, the DFSA due diligence process is a risk-based assessment that examines a firm's competence, financial soundness, and integrity.

DIFC regulations provide for an independent regulatory body, the Dubai Financial Services Authority (DFSA), which reports to the office of Dubai Crown Prince and an independent Commercial Court. Observers called the independence of the DFSA into question in the summer of 2004, even prior to the inauguration of the DIFC, with the high profile firing of the chief regulator and the head of the regulatory council (the supervisory authority). Subsequent to the firing, Dubai passed laws which appear to give the DFSA more regulatory independence from the DIFC, although these laws have not yet been tested. The DFSA, whose regulatory regime is generally modeled after the United Kingdom system, is the only authority responsible for licensing firms providing financial services in the DIFC.

The DFSA has licensed 21 financial institutions and 13 ancillary service providers to operate within the DIFC. The DFSA's rules prohibit offshore casinos or internet gaming sites in the UAE. The DFSA requires firms to send suspicious transaction reports to the AMLSCU (along with a copy to the DFSA). Although firms operating in the DIFC are subject to Law No. 4/2002, the DFSA has also issued its own anti-money laundering regulations and supervisory regime, creating some ambiguity as to the authority of the CB and AMLSCU within the DIFC. Discussions with the UAE central bank on a formal bilateral arrangement are ongoing. The DFSA has undertaken a campaign to reach out to other international regulatory authorities. It has signed MOUs with Turkey and the Isle of Man, and in

December 2005 the DFSA signed a regulatory protocol with the U.S. Commodity Futures Trading Commission (CFTC).

The UAE is a party to the 1988 UN Drug Convention. The UAE has signed but not yet ratified the UN Convention against Corruption and the UN Convention against Transnational Organized Crime. It has entered into a series of bilateral agreements on mutual legal assistance. The UAE is a party to all 12 UN conventions and protocols relating to the prevention and suppression of international terrorism. The UAE was very active in supporting the creation of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004; the UAE was one of the original charter signatories.

The UAEG has begun constructing a far-reaching anti-money laundering program, and it is considered a regional leader in these efforts. The UAE 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. There has been a substantial improvement on behalf of the AMLSCU in the area of information sharing with other countries.

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. Additionally law enforcement and customs officials should conduct more thorough inquiries into large undeclared cash imports and required the declaration of exports from the country. UAE officials should give greater scrutiny to trade-based money laundering in all of its forms. The Central Bank should continue its efforts to encourage hawala dealers to participate in the registration program. The UAE should implement a uniform system to monitor all charities active in the UAE, and it should engage in a public campaign to ensure all charities are aware of the requirements. It should ratify the UN Convention against Transnational Organized Crime.

United Kingdom

The United Kingdom (UK) plays a leading role in European and world finance and remains attractive to money launderers because of the size, sophistication, and reputation of its financial markets. Although 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 smuggled into and out of the UK, gatekeepers (including solicitors and accountants), and the purchase of high-value assets as disguises for illegally obtained money, and credit/debit card fraud has been on the increase since 2002.

The UK has implemented many of the provisions of the European Union's two Directives on the prevention of the use of the financial system for the purpose of money laundering, and the Financial Action Task Force (FATF) Forty Plus Nine Recommendations. Narcotics-related money laundering has been a criminal offense in the UK since 1986. The laundering of proceeds from other serious crimes is criminalized by subsequent legislation. Banks and non-bank 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 business 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.

The Proceeds of Crime Act 2002 was enacted on July 24, 2002, and entered into force on January 1, 2003. The final regulations took effect on March 1, 2004. The Act creates, for the regulated sector, a new criminal offense of failing to disclose suspicious transactions in respect to all crimes, 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 UK. 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. The total value of assets recovered by all agencies under the Act (and earlier legislation) in England, Wales, and Northern Ireland was £54.5 million (approximately $96.6 million) in 2004 and £84.4 million (approximately $149.6 million) in 2005.

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

Bank supervision falls under the Financial Services Authority (FSA). The FSA's primary responsibilities relate to the safety and soundness of the institutions under its jurisdiction. The FSA also plays an important role in the fight against money laundering through its continued involvement in the authorization of banks, and investigations of money laundering activities involving banks. The FSA regulated approximately 10,500 institutions and approved of 160,000 individuals in key positions (compliance officers, etc.) during the first half of 2003. From October of 2003, the FSA increased its regulatory role to include mortgage and general insurance agencies, totaling over 30,000 institutions. The FSA administers a civil-fines regime and has prosecutorial powers. The FSA has the power to make regulatory rules with respect to money laundering, and to enforce those rules with a range of disciplinary measures (including fines) if the institutions fail to comply.

In November 2005, the FSA fined UBS Wealth Management £100,000 (approximately $177,225) for failure to accurately report certain types of equity transactions since 1999. Abbey National, the UK's sixth largest bank, was fined £2.3 million (approximately $4.37 million) in 2003 for "extremely serious failings" in its anti-money laundering procedures during the period 2001-2003.

STRs are filed with the Financial Intelligence Division (FID), formerly the Economic Crime Bureau, of the National Criminal Intelligence Service (NCIS), which 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. The FID received approximately 32,000 STRs in 2001, 65,000 in 2002, and 100,000 in 2003. The merger of NCIS with two other law enforcement entities to form the Serious Organized Crime Agency (SOCA), announced in 2004, is designed to improve information-sharing and allow resources to be used more effectively in combating money laundering and other aspects of organized crime.

The Proceeds of Crime Act 2002 has enhanced the efficiency of the forfeiture process and increased the recovered amount of illegally obtained assets. The Act consolidates existing laws on forfeiture and money laundering into a single piece of legislation, and, perhaps most importantly, creates a civil asset forfeiture system for the proceeds of unlawful conduct. It also creates the Assets Recovery Agency (ARA), to enhance financial investigators' power to request information from any bank about whether it holds an account for a particular person. The Act provides for confiscation orders and for restraint orders to prohibit dealing with property. It also allows for the recovery of property that is, or represents, property obtained through unlawful conduct, or that is intended to be used in unlawful conduct. Furthermore, the Act shifts the burden of proof to the holder of the assets to prove that the assets were acquired through lawful means. In the absence of such proof, assets may be forfeited, even

without a criminal conviction. The Act gives standing to overseas requests and orders concerning property believed to be the proceeds of criminal conduct. The Act also provides the ARA with a national standard for training investigators, and gives greater powers of seizure at a lower standard of proof.

The Terrorism (United Nations Measures) Order 2001 makes it an offense for any individual to make any funds for financial or related services available, directly or indirectly, to or for the benefit of a person who commits, attempts to commit, facilitates, or participates in the commission of acts of terrorism. The Order also makes it an offense for a bank or building society to fail to disclose to the Treasury a suspicion that a customer or entity with whom the institution has had dealings since October 10, 2001, is attempting to participate in acts of terrorism. The Anti-Terrorism, Crime, and Security Act 2001 provides for the freezing of assets. In 2005, the UK issued 13 terrorist asset freeze orders on 28 individuals and 6 organizations.

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 increase in the workload. The Metropolitan Police responded to the growing emphasis on terrorist financing by expanding the focus and strength of its specialist financial unit dedicated to this area of investigations. This unit is now called the National Terrorist Financing Investigative Unit (NTFIU).

Charitable organizations and foundations are subject to supervision by the UK Charities Commission. Such entities must be licensed and are subject to reporting and record keeping requirements. The Commission has investigative and administrative sanctioning authority, up to and including the authority to remove management, appoint trustees and place organizations into receivership.

The UK cooperates with foreign law enforcement agencies investigating narcotics-related financial crimes. The UK is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The UK has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. The UK is a member of the FATF. 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 signed a reciprocal asset sharing agreement in March 2003). The UK also has an MLAT with the Bahamas. Additionally, there is a memorandum of understanding in force between the U.S. Immigration and Customs Enforcement and HM Revenue and Customs.

The Government of the United Kingdom should provide adequate oversight of its gaming sector. It should ratify the UN Convention against Transnational Organized Crime. The United Kingdom should continue the strong enforcement of its comprehensive anti-money laundering and 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, capital mobility regulations and overall economic stability made it a regional financial center vulnerable to money laundering, though the extent and the nature of suspicious financial transactions have been unclear. In 2002, banking scandals and mismanagement, along with massive withdrawals of Argentine deposits, led to a

near collapse of the Uruguayan banking system, significantly weakening Uruguay's role as a regional financial center. This crisis has diminished the attractiveness of Uruguayan financial institutions for money launderers in the medium term.

Uruguay is a founding member of the Financial Action Task Force for South America (GAFISUD), created in December 2000 and based in Buenos Aires. Since early 2005, the ex-director of the Government of Uruguay's (GOU) Center for Training on Money Laundering Issues (CECPLA) has served as the GAFISUD Executive Secretary. Under the Mutual Evaluation process, GAFISUD certified in 2003 that Uruguay's anti-money laundering laws and regulations met the majority of the Financial Action Task Force (FATF) Forty Recommendations; Uruguay's compliance with the FATF Special Recommendations on Terrorist Financing was not evaluated at that time. GAFISUD has 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, GAFISUD did not find evidence of major money laundering activity. In 2005, the IMF concluded a thorough examination of Uruguay's money laundering regime. The results of this examination are not yet available. Under an agreement between the IMF, World Bank and GAFISUD, the assessment may also be considered as GAFISUD's mutual evaluation of Uruguay, if the report is accepted by the GAFISUD plenary.

Over the past five years, the GOU has instituted several legislative and regulatory reforms in its anti-money laundering regime. The May 2001 Law 17,343 extends the predicate offenses beyond narcotics trafficking and corruption to include: terrorism; smuggling (value over $20,000); illegal trafficking in weapons, explosives and ammunition; trafficking in human organs, tissues and medications; trafficking in human beings; extortion; kidnapping; bribery; trafficking in nuclear and toxic substances; and illegal trafficking in animals or antiques. The courts have the power to seize and confiscate property, products or financial instruments linked to money laundering activities. Money laundering is considered a crime separate from underlying crimes such as narcotics trafficking, administrative corruption, terrorism and smuggling.

In September 2004, the Uruguayan Congress approved Law 17,835, which significantly strengthens the GOU's money laundering regime. The law incorporated all of GAFISUD's recommendations that had to be legislated, while the other recommendations were met through administrative regulations. It also includes specific provisions related to the financing of terrorism and to the freezing of assets linked to terrorist organizations, as well as to undercover operations and controlled deliveries. The first arrest and prosecution for money laundering under the new legislation occurred in October 2005. The case is still pending.

Law 17,835 of 2004 expands the realm of entities required to file suspicious activities reports (SARs) and makes reporting of such activities a legal obligation. It specifically confers to Uruguay's financial intelligence unit (FIU), Financial Information and Analysis Unit (UIAF) of the Central Bank, the role of receiving and analyzing SARs, and the authority to request additional related information. Created in 2000, the UIAF receives, analyzes, and disseminates suspicious financial reports to judicial authorities. Central Bank Circular 1722, which created the UIAF, provides the authority to respond to requests for international cooperation. In November 2004, Resolution 2002-2072 of the Central Bank Board of Directors raised the UIAF to the level of a directorate reporting directly to the Board. The UIAF has received 36 SARs in the first 11 months of 2005, more SARS than were received over the previous four years. Over the first 11 months of 2005, the UIAF also received 11 action requests from the courts and 24 information requests from foreign FIUs. While the level of staffing at the UIAF is currently very low, the Central Bank is reportedly in the process of hiring additional staff.

Central Bank regulations require all banks, currency exchange houses, stockbrokers and insurance companies to implement anti-money laundering policies, such as thoroughly identifying customers, recording transactions over $10,000 in internal databases, and reporting suspicious transactions to the

UIAF. The 2004 law makes this a legal obligation, extended to all financial intermediaries, including casinos, art dealers, real estate and fiduciary companies. Additionally, the law extends the reporting requirement to all persons entering or exiting Uruguay with over $10,000 in cash or in monetary instruments. Regulations for the 2004 law have been issued by the Central Bank for all entities it supervises, and are in the process of being issued by the Ministry of Economy and Finance for all other reporting entities, such as casinos, real estate brokers and art dealers.

Three government bodies are responsible for coordinating GOU efforts to combat money laundering: the UIAF, the National Drug Council, and the Center for Training on Money Laundering (CECPLA). The President's Deputy Chief of Staff heads the National Drug Council, which is the senior authority for anti-money laundering policy. The Director of CECPLA serves as coordinator for all government entities involved and sets general policy guidelines. The Director defines and implements GOU policies, in coordination with the Finance Ministry and the UIAF. The Ministry of Economy and Finance, the Ministry of the Interior (via the police force), and the Ministry of Defense (via the Naval Prefecture) also participate in anti-money laundering efforts. The financial private sector, most of which is foreign-owned, has developed self-regulatory measures against money laundering such as the Codes of Conduct approved by the Association of Banks and the Chamber of Financial Entities (1997), the Association of Exchange Houses (2001), and the Securities Market (2002).

Despite the power of the courts to confiscate property linked to money laundering, real estate ownership is not publicly registered in the name of the titleholder, complicating efforts to track money laundering in this sector, especially in the partially foreign-owned tourist industry. The UIAF and other government agencies must obtain a judicial order to have access to the name of titleholders. The GOU is in the process of implementing a national computerized registry that will facilitate the UIAF's access to titleholders' names.

Fiduciary companies called "SAFIs" are also thought to be a convenient conduit for illegal money transactions. As of January 1, 2006, all SAFIs are required to provide the names of their directors to the Finance Ministry. In addition, the GOU has decided to completely eliminate SAFIs as part of a comprehensive tax reform law that will be presented to the legislature in March 2006. The draft legislation will also implement a personal income tax for the first time in Uruguay.

Offshore banks are subject to the same laws and regulations as local banks, with the GOU requiring them to be licensed through a formal process that includes a background investigation. There are six offshore banks and 21 representative offices of foreign banks. Offshore trusts are not allowed. Bearer shares may not be used in banks and institutions under the authority of the Central Bank, and any share transactions must be authorized by the Central Bank. There are eight free trade zones in Uruguay, all but two being little more than warehouses for regional distribution. The other two house software development firms, back-office operations, call centers, and some light manufacturing/assembly. Some of the warehouse-style free trade zones have been used as transit points for containers of counterfeit goods bound for Brazil and Paraguay.

The GOU states that safeguarding the financial sector from money laundering is a priority, and Uruguay remains active in international anti-money laundering efforts. Uruguay is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention Against Corruption. On March 4, 2005, Uruguay ratified the UN Convention against Transnational Organized Crime. The GOU is a member of GAFISUD and the OAS Inter-American Drug Abuse Control Commission (CICAD) Experts Group to Control Money Laundering. The USG and the GOU are parties to extradition and mutual legal assistance treaties that entered into force in 1984 and 1994, respectively. The GOU has taken steps to bring it into compliance with the Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing. Some of these recommendations, such as the

criminalization of terrorism financing and provisions for the freezing of terrorist assets, were met by the 2004 money laundering law.

The Government of Uruguay took steps in 2004 and 2005 to strengthen its anti-money laundering and counterterrorist financing regime. The passage of legislation criminalizing terrorist financing places Uruguay ahead of many other nations in the region. However, Uruguay is one of only two countries in South America that is not a member of the Egmont Group of financial intelligence units. Once the UIAF is evaluated and determined to meet Egmont standards, the GOU will have greater access to financial information that is essential to its efforts to combat money laundering and terrorist financing. UIAF's becoming a member of the Egmont group, as well as the GOU's continued implementation and enforcement of its anti-money laundering and counterterrorist financing programs, should continue to be priorities for the GOU.

Uzbekistan

Uzbekistan is not considered an important regional financial center and does not have a well-developed financial system. Legitimate business owners, ordinary citizens, and foreign residents generally attempt to avoid using the Uzbek banking system for transactions, except when absolutely required, because of the onerous nature of the Government of Uzbekistan's (GOU) financial control system, the fear of GOU seizure of one's assets, and lack of trust in the banking system as a whole. As a result, Uzbek citizens have functioning bank accounts only if they are required to do so by law. They only deposit funds they are required to deposit and often resort to subterfuge to avoid depositing currency. The Central Bank of Uzbekistan (CBU) asserts that deposits from individuals have been increasing over the past three years.

Narcotics proceeds are controlled by local and regional drug-trafficking organizations and organized crime. Foreign and domestic proceeds from criminal activity in Uzbekistan are held either in cash, high-value transferable assets, such as gold or automobiles, or in foreign bank accounts.

There is a significant black market for smuggled goods in Uzbekistan. Since the GOU imposed a very restrictive trade and import regime in the summer of 2002, smuggling of consumer goods, already a considerable problem, increased dramatically. Many Uzbek citizens continue to make a living by illegally shuttle-trading goods from neighboring countries, Iran, the Middle East, India, Korea, Europe, and the U.S. The black market for smuggled goods does not appear to be significantly funded by narcotics proceeds. It is likely, however, that drug dealers use the robust black market to clean their drug related money.

Reportedly, the unofficial, unmonitored cash-based market creates an opportunity for small-scale terrorist or drug-related laundering activity destined for internal operations. For the most part, the funds generated by smuggling and corruption are not directly laundered through the banking system, but through seemingly legitimate businesses such as restaurants and high-end retail stores. There appears to be virtually no money laundering through formal financial institutions in Uzbekistan because of the extremely high degree of supervision and control over all bank accounts in the country exercised by the CBU, the Ministry of Finance and the state-owned and controlled banks. Although Uzbek financial institutions are not known to engage in illegal transactions in U.S. currency, illegal unofficial exchange houses, where the majority of cash-only money laundering takes place, deal in local soum and U.S. dollars. Moreover, drug dealers and others can transport their criminal proceeds in cash across Uzbekistan's porous borders for deposit in the banking systems of other countries, such as Kazakhstan, Russia or the United Arab Emirates.

Money laundering from the proceeds from drug-trafficking and other criminal activities is a criminal offense. With regard to drugs, 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 narcotics trafficking. Penalties for money laundering are from ten to fifteen years imprisonment, under Article 243 of the Criminal Code. This article defines the act of money laundering to include as punishable acts the transfer; conversion; exchange; or concealment of origin, true nature, source, location, disposition, movement and rights with respect to the assets derived from criminal activity. There has not yet been a complete assessment of the implementation and use of this legislation.

The CBU and the National Security Service (NSS) closely monitor all banking transactions to ensure that money laundering does not occur in the banking system. Banks are required to know, record, and report the identity of customers engaging in significant transactions, including the recording of large currency transactions at thresholds appropriate to Uzbekistan's economic situation. All transactions involving sums greater than $1000 in salary expenses for legal entities and $500 in salaries for individuals must be tracked and reported to the authorities. The CBU unofficially requires commercial banks to report on private transfers to foreign banks exceeding $10,000. Depending on the type and amount of the transaction, banks are required to maintain records for time deposits for a minimum of three years, possibly not sufficient time to reconstruct significant transactions. The law protects reporting individuals with respect to their cooperation with law enforcement entities. However, reportedly, the GOU has not adopted "banker negligence" laws that make individual bankers responsible if their institutions launder money.

Parliament passed a new law in August 2004 to combat money laundering and terrorist financing. This law, scheduled to take effect in January 2006, requires certain entities to report cash transactions above $26,000 (approximately), as well as suspicious transactions. In addition, this law also covers some non-banking financial institutions, such as investment foundations, depositaries and other types of investment institutions; stock exchanges; insurers; organizations which render leasing and other financial services; organizations of postal service; pawnshops; lotteries; and notary offices. It does not include intermediaries such as lawyers, accountants, or broker/dealers. Although casinos are illegal, GOU enforcement is generally lax and several exist openly in Tashkent.

The Law on Banks and Bank Activity (1996), article 38, stipulates conditions under which banking information can be released to law enforcement, investigative and tax authorities, prosecutor's office and courts. Different conditions for disclosure apply to different types of clients—individuals and institutions. In September 2003, Uzbekistan enacted a bank secrecy law that prevents the disclosure of client and ownership information for domestic and offshore financial services companies to bank supervisors and law enforcement authorities. In all cases, private bank information can be disclosed to prosecution and investigation authorities, provided there is a criminal investigation underway. The information can be provided to the courts on the basis of a written request in relation to cases currently under consideration. Protected banking information also can be disclosed to tax authorities in cases involving the taxation of a bank's client.

Existing controls on transportation of currency across borders, would, in theory, facilitate detection of the international transportation of illegal source currency. When entering/exiting the country, foreigners and Uzbek citizens are required to report all currency they are carrying. Residents and non-residents may bring the equivalent of $10,000 into the country tax-free. Amounts in excess of this limit are assessed a one-percent duty. Non-residents may take out as much currency as they brought in. However, residents are limited to the equivalent of $2,000. Residents wishing to take out higher amounts must obtain authorization to do so; amounts over $2,000 must be approved by an authorized commercial bank and amounts over $5,000 must be approved by the CBU.

International business companies are permitted to have offices in Uzbekistan and are subject to the same, if not stricter, regulations as domestic businesses. Offshore banks are not present in Uzbekistan and other forms of exempt or shell companies are not officially present.

In accordance with Uzbekistan's Code of Criminal Procedure, investigation of money laundering offenses falls under the jurisdiction of the Ministry of Internal Affairs (MVD). The Department of Investigation of Economic Crimes within the Ministry conducts investigations of all types of economic offenses. A specialized structure within the NSS and the Department on Combating Economic Crimes and Corruption in the Office of the Prosecutor General also are authorized to conduct investigations of money laundering offenses. There are no known arrests or prosecutions for money laundering or terrorist financing since January 1, 2002, except for one case following the suicide bombings of the Spring 2004. Unofficial information from numerous law enforcement officials indicates that there have been few, if any, prosecutions for money laundering under article 243 of the Criminal Code since its enactment in 2001. The GOU appears to lack a sufficient number of experienced and knowledgeable agents to investigate money laundering.

Article 155 of Uzbekistan's Criminal Code and the law "On Fighting Terrorism" criminalize terrorist financing. The latter law names the NSS, the MVD, the Committee on the Protection Of State Borders, the State Customs Committee, the Ministry of Defense, and the Ministry for Emergency Situations as responsible for implementing the counterterrorist legislation. The law names the NSS as the coordinator for government agencies fighting terrorism.

The GOU has the authority to identify, freeze, and seize terrorist assets. Uzbekistan has circulated to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the names of individuals and entities included on the UN 1267 consolidated list. In addition, the GOU has circulated the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 to the CBU, which has, in turn, forwarded these lists to banks operating in Uzbekistan. According to the CBU, no assets have been frozen.

Other than a plan to step up enforcement of currency regulations, the GOU has taken no steps to regulate or deter alternative remittance systems such as hawala, black market exchanges, trade-based money laundering, or the misuse of gold, precious metals and gems. We are not aware of any legislative initiatives under consideration. Although officially there is complete currency convertibility, in reality convertibility requests can be significantly delay or refused. In the second half of 2005, the GOU has taken steps to further restrict convertibility, leading to a slightly higher black market exchange rate for the soum.

The GOU closely monitors the activities of charitable and non-profit entities, such as NGOs, that can be used for the financing of terrorism. In February 2004, the Cabinet of Ministers issued Decree # 56 to allow the government to vet grants to local NGOs from foreign sources, ostensibly to fight money laundering and terrorist financing. Given the degree of supervision of charities and other non-profits, and the level of threat Uzbekistan itself faces from the Islamic Movement of Uzbekistan (IMU), a designated terrorist organization, it is extremely unlikely that the NSS would knowingly allow any funds to be funneled to terrorists through Uzbekistan-based charitable organizations or NGOS.

Uzbekistan has established systems for identifying, tracing, freezing, seizing, and forfeiting proceeds of both narcotics-related and money laundering-related crimes. Current laws include the ability to seize items used in the commission of crimes such as conveyances used to transport narcotics, farm facilities (except land) where illicit crops are grown or which are used to support terrorist activity, legitimate businesses if related to criminal proceeds and bank accounts. The banking community, which is entirely state-controlled and with few exceptions, state-owned, cooperates with efforts to trace funds and seize bank accounts. Uzbek law does not allow for civil asset forfeiture, but the Criminal Procedure Code provides for "civil" proceedings within the criminal case to decide forfeiture issues. As a practical matter, these proceedings are conducted as part of the criminal case. No new legislation or changes in current law are under active consideration by the GOU regarding seizure or

forfeiture of assets. The obstacles to enacting such laws are largely rooted in the widespread corruption that exists within the country.

In 2000, Uzbekistan set up a fund to direct confiscated assets to law enforcement activities. In accordance with the regulation the assets derived from the sale of confiscated proceeds and instruments of drug-related offenses were transferred to this fund to support entities of the NSS, the MVD, the State Customs Committee, and the Border Guard Committee, all of which are directly involved in combating illicit drug-trafficking. According to the GOU, a total of 115 million soum (approximately $97,000) has been deposited into this fund since its inception. Roughly $80,000 has been turned over to Uzbek law enforcement agencies. In 2004, however, the Cabinet of Ministers issued an order to close the Special Fund as of November 1, 2004. Under the new procedure, each agency manages the assets it seizes. There is also a specialized fund within the MVD set up to reward those officers who directly participate in or contribute to law enforcement efforts leading to the confiscation of property. This fund has generated 20 percent of its assets from the sale of property confiscated from persons who have committed offenses such as the organization of criminal associations, bribery and racketeering. The GOU enthusiastically enforces existing drug-related asset seizure and forfeiture laws. The GOU has not been forthcoming with information regarding the total dollar value of assets seized from crimes. Reportedly, existing legislation does not permit sharing of seized narcotics assets with other governments.

The GOU realizes the importance of international cooperation in the fight against drugs and transnational organized crime and has made efforts to integrate the country in the system of international cooperation. Uzbekistan has entered into agreements with Uzbek supervisors to facilitate the exchange of supervisory information including on-site examinations of banks and trust companies operating in the country. Uzbekistan has entered into bilateral agreements for the cooperation or exchange of information on drug related issues with the United States, Germany, Italy, Latvia, Bulgaria, Poland, China, Iran, Pakistan, the CIS, and all the countries in Central Asia. It has multilateral agreements in the framework of the CIS, under the Shanghai Cooperation Organization and under memoranda of understanding. An "Agreement on Narcotics Control and Law Enforcement Assistance" was signed with the United States on August 14, 2001, with two supplemental agreements that came into force in 2004

Uzbekistan does not have a Mutual Legal Assistance Treaty with the United States. However, Uzbekistan and the United States have reached informal agreement on mechanisms for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing and other serious crime investigations. In the past, Uzbekistan has cooperated with appropriate law enforcement agencies of the USG and other governments investigating financial crimes and several important terrorist-related cases. Uzbekistan joined the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG), a FATF-style regional body, at the most recent plenary meeting of that body in December 2005.

The GOU is an active party to the relevant agreements concluded under the CIS, CAEC, ECO, Shanghai Cooperation Organization and the "Six Plus Two" Group. Uzbekistan is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism and to the UN Convention against Transnational Organized Crime.

A lack of trained personnel, resources, and modern equipment hinder Uzbekistan's efforts to fight money laundering and terrorist financing. The GOU should continue to refine its pertinent legislation to bring it up to international standards. Uzbekistan also should expand the cross-border currency reporting rules to cover the transfer of monetary instruments, gold, gems and precious metals. Access to financial institution records should be given to appropriate regulatory and law enforcement agencies so that they can properly conduct compliance examinations and investigations. Uzbekistan should

establish a Financial Intelligence Unit to receive and analyze the suspicious transaction reports it proposed to require.

Vanuatu

Vanuatu's offshore sector is vulnerable to money laundering, as Vanuatu has historically maintained strict banking secrecy provisions that have the effect of preventing law enforcement agencies from identifying the beneficial owners of offshore entities registered in the sector. Due to allegations of money laundering, and in response to pressure from the Financial Action Task Force (FATF), a few United States-based banks announced in December 1999 that they would no longer process U.S. dollar transactions to or from Vanuatu. The Government of Vanuatu (GOV) responded to these concerns by introducing reforms designed to strengthen domestic and offshore financial regulation. The GOV passed amendments to four of its main legislations relative to money laundering and terrorist financing during its last session of Parliament in November 2005. The four pieces of legislation effected are the Mutual Assistance in Criminal Matters Act No. 31 of 2005, the Financial Transaction Reporting Act No. 28 of 2005, the Counter-Terrorism and Transnational Organised Crime Act No. 29 of 2005, and the Proceeds of Crime Act (Amendment) Act No. 30 of 2005.

Vanuatu's financial sector includes four licensed banks (that carry on domestic and offshore business) and one credit union, all of which are regulated by the Reserve Bank of Vanuatu. Since the passage of the International Banking Act of 2005, the Reserve Bank of Vanuatu regulates the offshore sector that includes seven banks and approximately 4,750 "international companies" (i.e., international business companies or IBCs), as well as offshore trusts and captive insurance companies. These institutions were once regulated by the Financial Services Commission. This change was one of many recommendations of the 2002 International Monetary Fund Module II Assessment Report (IMFR) that found Vanuatu's onshore and offshore sectors to be "non-compliant" with many international standards.

IBCs may be registered using bearer shares, shielding the identity and assets of beneficial owners of these entities. Secrecy provisions protect all information regarding IBCs and provide penal sanctions for unauthorized disclosure of information. These secrecy provisions, along with the ease and low cost of incorporation, make IBCs ideal mechanisms for money laundering and other financial crimes.

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

Although the amendments have been withdrawn from Parliament twice, FTRA amendments were finally passed in November 2005. The amendments include mandatory customer identification requirements; broaden the range of covered institutions required to file STRs to include auditors, trust companies, and company service providers; and provide safe harbor for both individuals and institutions required to file STRs. In addition to STR filings, financial institutions will now be required to file currency transaction reports (CTRs), which involves any single transaction in excess of VT 1 million (approximately $9,100) or its equivalent in a foreign currency, and wire transfers into and out

of Vanuatu in excess of VT 1 million. The amendments also require financial institutions to maintain internal procedures to implement reporting requirements, appoint compliance officers, establish an audit function to test their anti-money laundering and terrorist financing procedures and systems, as well as provide the VFIU a copy of their internal procedures. Failure to do so will result in a fine or imprisonment for an individual, or a fine in the case of a corporate entity. The amendments supersede any inconsistent banking or other secrecy provisions and clarify the FIU's investigative powers.

Regulatory agencies in Vanuatu have instituted stricter procedures for issuance of offshore banking licenses under the International Banking Act No. 4 of 2002, and continue to review the status of previously issued licenses. All financial institutions, both domestic and offshore, are required to report suspicious transactions and to maintain records of all transactions for six years, including the identities of the parties involved.

The Serious Offenses (Confiscation of Proceeds) Act 1989 criminalized the laundering of proceeds from all serious crimes and provided for seizure of criminal assets and confiscation after a conviction. The Proceeds of Crime Act (2002) 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. A new development to the Proceeds of Crime Act No. 30 of 2005 was an insertion of Section 74A, which now cover the cross-border movement of currency. After the passing of the bill in Parliament in November 2005, all incoming and outgoing passengers to and from Vanuatu will be legally obligated to declare to the Department of Customs cash exceeding one million Vatu in possession (approximately $9,100).

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

The amended International Banking Act has now placed Vanuatu's international and offshore banks under the supervision of the Reserve Bank of Vanuatu. Section 5(5) of the Act states that if existing licensees wish to carry on international banking business after December 31, 2003, the licensee should have submitted an application to the Reserve Bank of Vanuatu under Section 6 of the Act for a license to carry on international banking business. If an unregistered licensee 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 or imprisonment. Under Section 19 of the Act, the Reserve Bank can conduct investigations where it suspects that an unlicensed person or entity is carrying on international banking business. Since this time, three international banking businesses have had their licenses revoked.

One of the most significant requirements of the amended legislation is the banning of shell banks. As of January 1, 2004, all offshore banks registered in Vanuatu must have a physical presence in Vanuatu, and management, directors, and employees must be in residence. At the September 2003 plenary session of the Asia/Pacific Group on Money Laundering (APG), Vanuatu noted its intention to draft new legislation regarding trust companies and company service providers. 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 with standards set by the International Associations of Insurance Supervisors.

In November 2005, Vanuatu passed the Counter-Terrorism and Transnational Organized Crime Act No. 29 of 2005. The aim of the Act is to implement UN Security Council Resolutions and Conventions dealing with terrorism and transnational organized crime, to prevent terrorists from

operating in Vanuatu or receiving assistance through financial resources available to support the activities of terrorist organizations, and to criminalize human trafficking and smuggling.

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 had removed Vanuatu from its list of "uncooperative tax havens," following Vanuatu's earlier announcement that it would implement measures under the Harmful Tax Initiative. This move by OECD has made Vanuatu the first country to secure removal from the list of uncooperative tax havens.

In addition to its membership the Asia Pacific Group on Money Laundering, Vanuatu is a member of the Offshore Group of Banking Supervisors, the Commonwealth Secretariat, and the Pacific Island Forum. Its Financial Intelligence Unit became a member of the Egmont Group in June 2002. The GOV acceded to the UN Convention against Transnational Organized Crime on January 4, 2006. Vanuatu is a party to the UN International Convention for the Suppression of the Financing of Terrorism.. The VFIU has a memorandum of understanding with Australia.

The Government of Vanuatu should immobilize bearer shares and require complete identification of the beneficial ownership of international business companies (IBCs). It should implement all the provisions of its Proceeds of Crime Act and enact all additional legislation that is necessary to bring both its onshore and offshore financial sectors into compliance with international standards. Vanuatu should also become a party to the 1988 UN Drug Convention.

Venezuela

Venezuela is a major drug-transit country. Its proximity to drug producing countries, weaknesses in its anti-money laundering system, and corruption continue to make Venezuela vulnerable to money laundering. The main source of money laundering is believed to be from proceeds generated by Colombia's cocaine and heroin trafficking organizations. Trade-based money laundering, such as the Black Market Peso Exchange, through which money launderers furnish narcotics-generated dollars in the United States to commercial smugglers, travel agents, investors, and others in exchange for Colombian pesos, remains a prominent method for laundering narcotics proceeds. It is reported that many of these black market traders ship their wares through Venezuela's Margarita Island free trade zone. Reportedly, some money is also laundered through the real estate market in Margarita Island.

Venezuela is not a regional financial center, nor does it have an offshore financial sector. The relatively small but modern banking sector, which consists of 52 banks, primarily serves the domestic market. The majority of these banks, about 90 percent, belong to the Venezuelan Association of Banks. Membership is voluntary and meetings are held monthly.

Some positive steps were taken by Venezuela in 2005 to combat money laundering. In September, following three years of debate by the National Assembly, the Organic Law Against Organized Crime was passed. Prior to the passage of the new law, the 1993 Organic Drug Law provided the only legal mechanism for the investigation and prosecution of money laundering crimes. Under the 1993 law, a direct connection between illegal drugs and their proceeds had to be proven to establish a money laundering offense, and the Government of Venezuela (GOV) was only able to freeze assets of

individuals charged in international drug trade or in money laundering cases directly related to narcotics trafficking. Under the 2005 Organic Law Against Organized Crime, money laundering is now a separate offense, punishable by a sentence of eight to twelve years in prison. Moreover, those who cannot establish the legitimacy of possessed or transferred funds, or have awareness of the illegitimate origins of those funds, can be charged with money laundering, without any connection to drug-trafficking.

In addition to establishing money laundering as a separate offense, the Organic Law Against Organized Crime also broadens asset forfeiture and sharing provisions, adds conspiracy as a criminal offense, strengthens due diligence requirements, and provides law enforcement with stronger investigative powers by authorizing the use of modern investigative techniques such as the use of undercover agents. The passage of this law, along with recent amendments to the Law Against the Trafficking and Consumption of Narcotics and Psychotropic Substances, effectively brings Venezuela's Penal Code in line with the 1988 UN Drug Convention. However, given that the judicial and law enforcement sectors are rife with corruption, it is too early to know what, if any, impact these new laws will have on the growing problem of money laundering. The new law also did not adequately criminalize terrorist financing.

Since 1997, the Superintendence of Banks and Other Financial Institutions (SBIF) has implemented controls to prevent and investigate money laundering under Resolution 333-97 of 1997. These controls include strict customer identification requirements and the reporting of both currency transactions over a designated threshold and suspicious transactions. Under the Organic Law Against Organized Crime, these controls were expanded beyond their application to all banks (commercial, investment, mortgage, private), insurance and reinsurance companies, savings and loan institutions, financial rental agencies, currency exchange houses, money remitters, money market funds, capitalization companies, and frontier foreign currency dealers. They now also cover casinos, real estate agents, construction companies, car dealerships, hotels and the tourism industry, travel agents, and dealers in precious metals and stones. These entities are required to file suspicious and cash transaction reports with Venezuela's financial intelligence unit (FIU), the Unidad Nacional de Inteligencia Financiera (UNIF), which was created under the SBIF in July 1997 and began operations in June 1998. Under the original draft of the Organic Law Against Organized Crime, the UNIF would have become an autonomous entity with investigative powers, independent of the SBIF, but the relevant clauses were removed just prior to the law's passage.

The UNIF receives suspicious transaction reports (STRs) and reports of currency transactions exceeding 4.5 million bolívares (approximately $2,100) from institutions regulated by the SBIF, the Office of the Insurance Examiner, the National Securities and Exchange Commission, the Bureau of Registration and Notaries, the Central Bank of Venezuela, and the Bank Deposits and Protection Guarantee Fund, as well as the other entities now included under the Organic Law Against Organized Crime. Some institutions regulated by the SBIF, such as tax collection entities and public service payroll agencies, are exempt from the reporting requirement. The SBIF also allows certain customers of financial institutions—those who demonstrate "habituality" in the types and amounts of transactions they conduct—to be excluded from currency transaction reports filed with the UNIF. A system has been developed for electronic receipt of currency transaction reports (CTRs), but STRs must be filed in paper format. Under the new Organic Law Against Organized Crime, obligated entities are forbidden to reveal reports filed with the UNIF or suspend accounts during an investigation without official approval. Obligated entities are also subject to sanctions for failure to file reports with the UNIF.

In addition to STRs and CTRs, 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 that exceed 4.5 million bolívares. The UNIF does not, however, receive reports on the transportation of currency or monetary instruments into or out of Venezuela. 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 filing of CTRs and STRs and "know your customer" policies. Each currency exchange house in the country has and employs systems to electronically transmit transaction reports to the SBIF and the Public Ministry. However, inadequate foreign exchange controls established in 2003 by the GOV's Commission for Administrative Control of Currency Exchange (CADIVI) present opportunities to circumvent regulations applicable in the banking and financial institution sectors. Procedures to limit the potential for laundering funds through the stock market are also thought to be inadequate.

The UNIF analyzes STRs and other reports, and refers those deemed appropriate for further investigation to the Public Ministry (the Office of the Attorney General). Approximately 30 percent of the STRs received by the UNIF are sent to the Public Ministry for further investigation. 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, the SBIF or the Public Ministry, or by order of a Judge of Control, bank secrecy may be waived, making Venezuela one of the few countries in Latin America that does not have restrictive bank secrecy laws.

Prior to the passage of the 2005 Organic Law Against Organized Crime, there was no special prosecutorial unit for the prosecution of money laundering cases under the Public Ministry, which is the only entity legally capable of initiating money laundering investigations. Only the drug prosecutors received STRs from the UNIF and conducted money laundering investigations, and there were only 20 drug prosecutors for all of Venezuela, most of who lacked the technical financial experience to successfully prosecute money laundering cases. As a result, there have only been three money laundering convictions in Venezuela since 1993, and all of them were narcotics-related. Under the Organic Law Against Organized Crime, a new unit will be established, the General Directorate Against Organized Crime, with specialized technical expertise in the analysis and investigation of money laundering and other financial crimes.

The 2005 Organic Law Against Organized Crime has also expanded Venezuela's mechanisms for freezing assets tied to illicit activities. Prior to the passage of the Organic Law Against Organized Crime, the assets had to be linked to a crime such as narcotics trafficking—or money laundering directly related to narcotics trafficking—and pass through a lengthy judicial process. With the passage of the Organic Law Against Organized Crime, a prosecutor may now solicit judicial permission to freeze or block accounts in the investigation of any crime included under the Organic Law Against Organized Crime.

The 2005 Organic Law Against Organized Crime counts terrorism as a crime against public order and defines some terrorist activities. The law also establishes punishments for terrorism of up to 20 years in prison. However, the Organic Law Against Organized Crime does not establish terrorist financing as a separate crime, nor does it provide adequate mechanisms for freezing terrorist assets.

The UNIF has been a member of the Egmont Group since 1999 and has signed bilateral information exchange agreements with counterparts worldwide. Venezuela participates in the Organization of American States Inter-American Commission on Drug Abuse Control (OAS/CICAD) Money Laundering Experts Working Group and is a member of the Caribbean Financial Action Task Force (CFATF). A mutual evaluation of Venezuela was conducted by CFATF in 2004 and presented to the CFATF plenary in 2005. The GOV is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the OAS Inter-American Convention Against Terrorism, and has signed, but not yet ratified, the UN Convention against Corruption. The GOV continues to share money laundering information with U.S. law enforcement authorities under the 1990 Agreement Regarding

Cooperation in the Prevention and Control of Money Laundering Arising from Illicit Trafficking in Narcotics Drugs and Psychotropic Substances, which entered into force on January 1, 1991. Venezuela also has a Mutual Legal Assistance Treaty (MLAT) with the United States, but the treaty has not entered into force.

The Government of Venezuela has taken several important steps to expand its anti-money laundering regime with the passage of the Organic Law Against Organized Crime. The passage of this bill has provided law enforcement and judicial authorities the much-needed tools for the effective investigation and prosecution of money laundering derived from all serious crimes, broadened asset forfeiture and sharing provisions, strengthened due diligence requirements, strengthened the capabilities of the Public Ministry to successfully investigate and prosecute crimes related to money laundering, and expanded the mandate of UNIF. However, the deletion of those portions of the proposed law that would have made the UNIF autonomous may undercut the effectiveness of the unit, and attention will have to be paid to make sure that does not happen.

Venezuela should also create and enact legislation to criminalize the financing of terrorism, as well as institute measures to expedite the freezing of terrorist assets. Although the passage of the Organic Law Against Organized Crime indicates an increased willingness to strengthen the GOV's abilities to fight money laundering, legislation criminalizing the financing of terrorism and allowing for the freezing of terrorist assets is necessary to bring Venezuela into full compliance with international standards for combating financial crimes.

Vietnam

Vietnam is not an important regional financial center. The Vietnamese banking sector is underdeveloped and the Government of Vietnam (GVN) controls the flow of all U.S. dollars in official channels. The nature of the banking system makes it unlikely that major money laundering or terrorist financing is currently occurring in financial institutions. However, a "drug economy" does exist 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 use gold shops and other informal mechanisms to remit or receive funds from overseas. Official inward remittances in 2005 were estimated to be $3.8 billion while estimates are that double that amount came through unofficial channels. Reportedly, an unknown percentage of transactions in the informal remittance systems come from narcotics proceeds.

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 (MPS) specialized counternarcotics agency the authority to require disclosure of financial and banking records when there is a suspected violation of the law. The Penal Code governs money laundering related offenses.

In June 2005, GVN issued Decree 74/2005/ND-CP on the Prevention and Combating of Money Laundering. The Decree covers acts committed by individuals or organizations to legitimize money or property acquired from criminal activities. The Decree applies to banks and non-banking financial institutions. The State Bank of Vietnam (SBV) and the MPS take primary responsibility for preventing and combating money laundering. The decree does not cover counterterrorist finance.

SBV supervises and examines financial institutions for compliance with anti-money laundering/counter terrorist financing regulations. Financial institutions are responsible for knowing and recording the identity of their customers. They are required to report cash transactions conducted

in one day with aggregate value of VND 200 million ($13,000) or more, or equivalent amount in foreign currency or gold. The threshold for savings transactions is VND 500 million ($31,000). Furthermore, financial institutions are required to report all suspicious transactions. Banks are also required to maintain records for seven years or more. Banks are responsible for keeping information on their customers secret, but they are required to provide necessary information to law enforcement agencies for investigation purposes.

Foreign currency (including notes, coins and traveler's checks) in excess of $7,000 and gold of more than 300 grams must be declared at customs upon arrival and departure. There is no limitation on either the export or import of U.S. dollars or other foreign currency provided that all currency in excess of $7,000 (or its equivalent in other foreign currencies) is declared upon arrival and departure, and supported by appropriate documentation. If excess cash is not declared, it is confiscated at the port of entry/exit and the passenger may be fined.

The 2005 Decree on Prevention and Combating Money Laundering provides for provisional measures to be applied to prevent and combat money laundering. Those measures include 1) suspending transactions; 2) blocking accounts; 3) sealing or seizing property; 4) seizing violators of the law; and, 5) taking other preventive measures allowed under the law.

The 2005 Decree also provides for the establishment of an Anti-Money Laundering Information Center within the State Bank of Vietnam (SBV). This center will function as the sole body to receive and process information. It will have the right to request concerned agencies to provide information and records for suspected transactions. Senior officials of the center will be appointed by the Governor of the SBV. The center is awaiting final approval from the Government before it can be formally established. SBV acts as the sole agency responsible for negotiating, concluding and implementing international treaties and agreements on exchange of information on transactions related to money laundering. SBV is seeking donors' assistance to strengthen its supervision capabilities in the context of Vietnam integrating into the world economy.

The MPS is responsible for investigating money laundering related offences. There is no information available on arrests and/or prosecutions for money laundering or terrorist financing since January 1, 2005. MPS is also responsible for negotiating and concluding international treaties on judicial assistance, cooperation and extradition in the prevention and combat of money laundering related offenses.

Vietnam is a party to the UN International Convention for the Suppression of the Financing of Terrorism. Vietnam plans to draft separate legislation governing counter terrorist financing, though they will not set a specific time frame for this drafting. Currently SBV circulates to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. To date no related assets have been identified.

Vietnam is a party to the 1988 UN Drug Convention. Under existing Vietnamese legislation, there are provisions for seizing assets linked to drug trafficking. In the course of its drug investigations, MPS has seized vehicles, property and cash, though the seizures are usually directly linked to drug crimes. Final confiscation requires a court finding. Reportedly, MPS can notify a bank that an account

is "seized" and that is sufficient to have the account frozen. However, MPS is not allowed to seize assets in order to investigate them; they must receive separate information that confirms and/or proves the money is laundered before it can be frozen. A further restriction of their investigative powers is that Vietnam authorities cannot act on information or investigative findings provided by outside agencies.

The U.S. Drug Enforcement Agency (DEA) is engaged in a number of investigations targeting significant ecstasy and marijuana trafficking organizations, composed primarily of Viet Kieu (overseas

Vietnamese), in both the United States and Canada. These drug trafficking networks are capable of laundering tens of millions of dollars per month back to Vietnam, exploiting U.S. financial institutions to wire or transfer money to Vietnamese bank and remittance accounts, as well as engaging in the smuggling of bulk amounts of U.S. currency and gold from the United States into Vietnam.

The Government of Vietnam should promulgate all necessary regulations to fully implement the 2005 degree on the Prevention and Combating of Money Laundering. Vietnam should also pass legislation governing the prevention and suppression of terrorism financing. Vietnam should ratify the UN Convention Against Transnational Crime. Vietnam should enforce cross border currency controls, including the use of gold as an alternative remittance system. Vietnam should become a member of the Asia/Pacific Group on Money Laundering (APG).

Yemen

The Yemeni financial system is not yet well-developed. Thus, the extent of money laundering is not known. Alternative remittance systems, such as hawala, are prevalent. Although hawalas are subject to limited monitoring by the Central Bank of Yemen (CBY), widespread usage of alternative remittance systems constitutes a vulnerability to money laundering. The banking sector is relatively small, with only 17 commercial banks, including four Islamic banks, one of which was recently acquired by the CBY and may be liquidated. The CBY supervises the banks. Local banks account for approximately 62 percent of the total banking activities, while foreign banks cover the other 38 percent.

Yemen's parliament passed comprehensive anti-money laundering legislation (Law 35) in April 2003. The legislation criminalizes money laundering for a wide range of crimes, including narcotics offenses, kidnapping, embezzlement, bribery, fraud, tax evasion, illegal arms trading, and monetary theft, and imposes penalties of three to five years of imprisonment. Yemen has no specific legislation relating to terrorist financing, but Cabinet Decision 247 issued in 2005 directs the CBY and the Ministry of Legal Affairs to amend Law 35 to include terrorist financing. The Ministry of Interior (MOI) also has a unit to investigate terrorist financing. According to the law, both the MOI and CBY report their findings to the Attorney General for enforcement.

Law 35 requires banks, financial institutions, and precious commodity dealers to verify the identity of persons and entities that open accounts (or in the case of the dealers, for those who execute a commercial transaction), to keep records of transactions for up to ten years, and to report suspicious transactions. In addition, the law requires that reports be submitted to an information-gathering unit within the CBY. The unit acts as the financial intelligence unit (FIU), which in turn reports to the Anti-Money Laundering Committee (AMLC).

The FIU is severely understaffed, with a total of three employees at the main office. Eighteen field inspectors for banking supervision also serve as investigators for the FIU. The FIU has no database and is not networked internally or to the rest of the CBY. The CBY provides training to other members of the government to assist in elements of anti-money laundering enforcement, but lack of capacity severely hampers any attempts by the FIU to control illicit activity.

The AMLC is composed of representatives from the Ministries of Finance, Foreign Affairs, Justice, Interior, Industry and Trade, the Central Accounting Office, the General Union of Chambers of Commerce and Industry, the CBY, and the Association of Banks. The AMLC is authorized to issue regulations and guidelines and provide training workshops related to combating money laundering efforts. In addition, Law 35 grants the AMLC the right to exchange information with foreign entities. The head of the AMLC is empowered by law to ask local judicial authorities to enforce foreign court verdicts based on reciprocity. Also, the law permits the extradition of non-Yemeni criminals in accordance with international treaties or bilateral agreements.

Prior to passage of the anti-money laundering law, the CBY issued Circular 22008 in April 2002, instructing banks and financial institutions that they must verify the legality of all proceeds deposited in or passing through the Yemeni banking system. The circular stipulates that financial institutions must positively identify the place of residence of all persons and businesses that establish relationships with them. The circular also requires that banks verify the identity of persons or entities that wish to transfer more than $10,000, when they have no accounts at the banks in question. The law also prohibits the transfer of more than $10,000 cash in or out of the country without permission from the CBY, although this is rarely enforced.

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 and "Core Principles for Effective Banking Supervision." The CBY issued Circular No. 4 on December 9, 2003, ordering banks to set up intelligence gathering units specializing in investigating and monitoring suspicious funds and transactions in their regulatory structures. In 2005, however, no reports were filed with the FIU by commercial banks and there were no prosecutions.

Based on the UN 1267 Sanctions Committee's consolidated list of suspected terrorists and terrorist organizations, as well as the list of Specially Designated Global Terrorists issued by the U.S. pursuant to E.O. 13224, and Yemen's own Council of Ministers' directives, the CBY issued two circulars (75304 and 75305) to all banks operating in Yemen. These circulars directed the banks to freeze the accounts of 144 persons, companies, and organizations, and to report any findings to CBY. However, since the February 2004 addition of Sheikh Abul Majid Zindani to the UN 1267 Sanctions Committee's consolidated list, the Yemeni Government has made no known attempt to enforce the sanctions and freeze his assets. In such high-profile cases, information sharing is limited by a lack of political will, as well as a lack of enforcement capacity.

A law was passed in 2001 governing charitable organizations. This law entrusts the Ministry of Labor and Social Affairs with overseeing their activities. The law also imposes penalties of fines 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. In 2005, 21 charities were questioned as part of continuous supervision in coordination with the Ministry of Labor and Social Affairs, but there were no prosecutions. Cabinet Decision 378 granted the FIU authority to investigate gold shops, insurance companies, and real estate brokers in order to enhance procedures to combat terrorist financing. The FIU also has the legal authority to investigate transactions in the Aden free zone, but has reportedly not yet asserted that authority.

Yemen is a member of the Middle East and North Africa Financial Action Task Force (MENAFATF). Yemen is a party to the 1988 UN Drug Convention and the Arab Convention for the Suppression of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. It is not a party to the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Yemen is making slow progress in enforcing its domestic anti-money laundering program. The passage of the 2003 anti-money laundering legislation represents a significant first step in meeting international standards. However, international cooperation with criminal investigations is still in the initial development stages. The CBY is still organizing its enforcement mechanism. The FIU staff capabilities need to be enhanced. Its effectiveness will demonstrate the government's commitment to ending money laundering. The fact that the FIU has not received any suspicious transaction reports during 2005 is a serious concern. Yemen should also examine the prevalence of alternative remittance systems such as hawala and trade-based money laundering. As a next step, Yemen should enact specific legislation with respect to terrorist financing and forfeiture of the assets

of those suspected of terrorism. It should ratify the UN Convention against Transnational Organized Crime. It should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Zambia

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

The Prohibition and Prevention of Money Laundering Act of 2001 makes money laundering a criminal offense in Zambia, 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.

The anti-money laundering law does not contain specific provisions on the financing of terrorism; the Government of the Republic of Zambia (GRZ) 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, the GRZ established an anti-money laundering unit under the DEC. The main purpose of the unit is to lead efforts within the GRZ to counter money laundering and enforce the Prevention of Money Laundering Act. In the same year, three officers of a commercial bank were tried and convicted for money laundering offenses. In 2004 and 2005, the DEC conducted numerous investigations of money laundering, resulting in several arrests. Trials in these cases are pending. The penalty for money laundering is imprisonment for a term not exceeding ten years and/or a fine.

In 2003, Zambia signed the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) memorandum of understanding. In 2005, Zambia's Central Bank was an active participant in ESAAMLG activities. Zambia holds the presidency of the organization for 2005 and 2006. Zambia is not a signatory to the UN International Convention for the Suppression of the Financing of Terrorism. Zambia is a party to UN Convention Against Transnational Organized Crime. Zambia is a party to the 1988 UN Drug Convention.

The Government of Zambia should establish a fully operational Financial Intelligence Unit in accordance with international standards. Zambia should become a party to the UN International Convention for the Suppression of the Financing of Terrorism. Zambia should also criminalize terrorist financing and implement counterterrorist financing regulations that comport with the FATF recommendations, including the Special Recommendations on Terrorist Financing.

Zimbabwe

Zimbabwe is not a regional financial center, but it faces a serious and growing problem with official corruption and many other common risk factors associated with money laundering. These risk factors include the following: a flourishing parallel exchange market; widespread evasion of exchange controls by legitimate businesses; company ownership through nominees; an increasingly understaffed bank supervisory authority; a lack of trained investigators or regulators for financial crime enforcement; financial institutions that are determined to bypass the regulatory framework; limited asset seizure authority; a laissez-faire attitude toward compliance with the law on the part of elements of the business community; ready acceptance of the U.S. dollar in transactions; and significant gold exports and illegal gold trading.

The Government of Zimbabwe (GOZ) criminalized narcotics-related money laundering in the "Anti-Money Laundering Act." In 2004, the GOZ passed more expansive legislation, the Anti-Money Laundering and Proceeds of Crime Act ("The Act") that extended the anti-money laundering law to all serious offenses. The Act required banks to maintain records sufficient to reconstruct individual transactions for at least six years. It mandated a prison sentence of up to five years. The Act also addressed terrorist financing and authorized the tracking and seizure of assets. Given the GOZ's history of selective use of the legal system against its opponents, the Act has raised human rights concerns, although its use to date has not been associated with any reported due process abuses or provoked any serious public opposition.

Over the past two years, the GOZ has arrested many prominent Zimbabweans for activities that it calls "financial crimes." Most of these "crimes" involved violations of currency restrictions that criminalize the externalization of foreign exchange activities conducted by many Zimbabwean businesses with substantial volumes of imports or exports (i.e. transferring assets offshore). To date, the Act has not been employed in the prosecution of individuals for such offenses.

However, despite having the legal framework in place to combat money laundering, the growing economic vulnerability of the population and the decline of judicial independence raise concerns about the continued capacity and integrity of Zimbabwean law enforcement. The GOZ prefers to prosecute financial crimes under the Criminal Procedures and Evidence Act, because it allows for those charged to be held in custody for up to 28 days. The Reserve Bank of Zimbabwe (RBZ), and not the Ministry of Anti-Corruption, is the lead agency for prosecuting money laundering offenses.

When requested, the local banking community has overtly cooperated with the GOZ in the enforcement of laws involving tracking of assets; however, increasingly burdensome GOZ regulations and a hostile business climate have led to growing circumvention of the law. The banking community and the RBZ have cooperated with the U.S. in global efforts to identify individuals and organizations associated with terrorist financing.

Zimbabwe is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Zimbabwe has yet to sign the UN International Convention for the Suppression of the Financing of Terrorism. Zimbabwe joined the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) in August 2003 but has yet to sign the ESAAMLG Memorandum of Understanding.

Zimbabwe should become a party to both the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. It should sign the MOU for the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) and participate actively in that body.