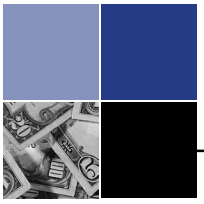
2003

National Money Laundering Strategy

ONDCP



Foreword

The fight against money laundering and terrorist financing is an ongoing campaign that forms a critical part of our national security. The *2003 National Money Laundering Strategy*, the second since the attacks of September 11th, reasserts our commitment to securing the financial system not only from criminals but also from the financiers of terror. Dismantling the financial infrastructure of criminal organizations and terrorist networks is the strategic baseline we are implementing for both short and long term effect. To succeed in this endeavor, we must continue to use all of the powers available to the U.S. government – financial, administrative, law enforcement, regulatory, and diplomatic – to attack this issue on all fronts.

While we made important strides over the past five years to concentrate our attention on the abuse of the financial system by criminals, the techniques criminals and terrorists use to exploit the financial system continue to evolve. Building on the successes and experience of the past, we are resolved to remain vigilant and proactive in our efforts to disrupt and dismantle the organized criminal and terrorist activities that threaten not only our financial system but also our national security.

It is in this spirit that we present the *2003 National Money Laundering Strategy*. To achieve our goals, we will continue to engage in a sustained and united effort, facing the ongoing challenges posed by money laundering and terrorist financing. The *2003 Strategy* outlines broadly our plan to meet these ongoing and ever-evolving threats to our national security with concerted resolve, foresight, and vigilance.

John W. Snow
Secretary of the Treasury

John Ashcroft
Attorney General

Table of Contents

Executive Summary

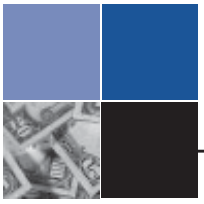
The *2003 National Money Laundering Strategy* reflects the U.S. government's ongoing commitment to attack money laundering and terrorist financing on all fronts, including the formal and informal components of both the domestic and international financial systems. Armed with important new authorities provided by the USA PATRIOT Act, we are taking coordinated and aggressive action using all available tools, including law enforcement actions, appropriate financial regulation and oversight, and coordination with our private sector and international partners. While we continue to make significant progress, much remains to be done to confront the ever-changing, global threat of money laundering and terrorist financing.

The *2003 Strategy* represents a continuation of our past efforts, and a commitment to move forward by identifying, disrupting, and dismantling high value terrorist financing and money laundering organizations and networks. The central tenet of our *2003 Strategy* is the ever-increasing need for all relevant U.S. government agencies, our foreign government counterparts, and our partners in the private sector to pool our collective expertise and coordinate our activities to stop the laundering of criminal proceeds and to staunch the flow of funds to terrorists. By attacking the financial infrastructure of complex criminal organizations and terrorist networks, we do long term damage to their ability to perpetuate their operations.

To achieve these objectives, the *2003 Strategy* focuses on three major goals: (1) to cut off access to the international financial system by money launderers and terrorist financiers more effectively; (2) to enhance the Federal government's ability to target major money laundering organizations and systems; and (3) strengthen and refine the anti-money laundering regulatory regime for all financial institutions to improve the effectiveness of compliance and enforcement efforts.

The *2003 National Money Laundering Strategy* includes, among other items, a commitment to accomplish the following:

- Block and seize terrorist assets and identify and designate terrorist organizations. To date, over 315 terrorist-related entities have been designated and over $136 million in assets frozen.
- Target countries and institutions that facilitate money laundering and terrorist financing, including using the full range of measures provided by Section 311 of the USA PATRIOT Act.
- Take law enforcement action against high value money laundering targets, including those with ties to major narcotics trafficking operations.
- Improve the effectiveness of compliance and enforcement efforts to continue to strengthen and refine the anti-money laundering regulatory regime for all financial institutions by identifying new and emerging threats that can be addressed through regulation, improving the effectiveness of anti-money laundering controls through greater communication, guidance, and information-sharing with the private sector, and enhancing regulatory compliance and enforcement efforts.
- Encourage foreign countries throughout the world to adopt and adhere to international standards to inhibit the flow of illicit funds, both through the formal and informal financial sectors, and to assist in developing and enhancing anti-money laundering regimes in targeted countries to enable them to thwart terrorist financing.
- Improve the Federal government's partnership with the private financial sector to increase information-sharing and close the gaps in the financial system that allow abuse by money launderers and terrorist financiers.



Introduction

The *2003 National Money Laundering Strategy* both targets terrorist financing as a top priority and directs improvement of our ongoing efforts to combat money laundering. It embodies our conviction, deepened by our growing experience in this area, that the broad fight against money laundering is integral to the war against terrorism.

At the same time, the *2003 Strategy* continues to embrace anti-money laundering efforts as key to attacking all kinds of other criminal activity, including narcotics trafficking, white collar crime, organized crime, and public corruption. Resources devoted to fighting money laundering and financial crimes reap benefits far beyond addressing the financial crimes they directly target. Financial investigations expose the infrastructure of criminal organizations; provide a roadmap to those who facilitate the criminal activity, such as broker-dealers, bankers, lawyers and accountants; lead to the recovery and forfeiture of illegally-obtained assets; and support broad deterrence against a wide range of criminal activity. Thus, the *2003 Strategy* is intended to sharpen our ongoing efforts to combat money laundering by ensuring that law enforcement agencies and task forces use and share all available financial databases and analytical tools, focusing law enforcement personnel and other resources on high-impact targets and financial systems, and improving Federal government interaction with the financial community.

Although money laundering and terrorist financing differ in certain ways,[1] they share many of the same methods to hide and move proceeds. Moreover, both depend on a lack of transparency and vigilance in the financial system. Accordingly, our efforts to identify and target shared-methods to place, layer, and transfer money -- such as by using the informal financial sector, including alternative remittance systems; bulk currency shipments; money transmitters; money changers; and commodity-based trade--will help us combat both those who launder criminal proceeds and those who finance terrorism.

The 2003 Strategy recognizes that in an era that continues to be plagued by terrorist attacks, the Federal government's efforts to combat money laundering and terrorist financing necessarily take place in an environment where some of the personnel and other resources previously devoted to anti-money laundering enforcement have been redirected to counter-terrorism activities. The *2003 Strategy* strives to meet this challenge and continue to achieve major successes against both terrorist financing and money laundering and financial crime, by leveraging our resources in a variety of ways.

Enhanced coordination and information sharing are essential. The USA PATRIOT Act provided authority to enhance the flow of financial information relevant to money laundering and terrorist financing (1) within the Federal government; (2) between the government and financial institutions; and (3) among the financial institutions themselves. Under the *2003 Strategy*, we are utilizing these new authorities to forge dynamic new partnerships across all relevant government agencies and the financial sector to combat terrorist financing and money laundering.

To enhance the Federal government's efforts to combat terrorist financing, money laundering, and other financial crimes, on March 3, 2003, the Department of the Treasury established the Executive Office of Terrorist Financing and Financial Crimes (EOTF/FC). This new office works closely with other Treasury offices, other Federal and state government agencies, foreign government counterparts, and the private sector to prevent terrorists and other criminals from

[1] Briefly, money laundering depends on the existence of an underlying crime, while terrorist financing does not. Methods for raising funds to support terrorist activities may be legal or illegal, and the transactions tend to be smaller and much less observable than, for example, the typical narcotics money laundering transaction. Moreover, money laundering investigations are initiated to achieve prosecution and forfeiture. Terrorist financing investigations share these objectives; however, their ultimate aim is to identify, disrupt and cut off the flow of funds to terrorists, whether or not the investigation results in prosecutions.

abusing the domestic and international financial systems and to identify, block, and dismantle sources of terrorist financing.

The *2003 Strategy* directs law enforcement to leverage assets by focusing efforts on high-impact targets, such as terrorist fundraisers and the heads of narcotics money laundering organizations. In this latter area, Federal law enforcement agencies are working collaboratively to develop a unified national list of drug organization targets, called the "Consolidated Priority Organization Target List" (CPOT), which targets those believed to be primarily responsible for the domestic drug supply. This effort allows law enforcement to focus collective investigative resources on particular high impact targets, including major drug money launderers.

Significantly, law enforcement will aggressively exploit the points of common vulnerability between "ordinary" criminal money laundering and terrorist financing. A recent North Carolina-based cigarette smuggling case exemplifies this kind of synergy. The case began when local law enforcement in North Carolina observed activity that led them to suspect inter-state cigarette smuggling and shared this information with Federal law enforcement. Thereafter, Federal Bureau of Investigations (FBI) intelligence agents, Alcohol, Tobacco and Firearms (ATF) and Internal Revenue Service-Criminal Investigation (IRS-CI) agents, with continuing close cooperation from local and Canadian law enforcement, conducted an investigation that revealed a massive cigarette smuggling and tax evasion scheme, in which Lebanese members of a Charlotte, North Carolina, Hizballah Cell were smuggling untaxed cigarettes from North Carolina to Michigan and using the proceeds to provide financial support and military equipment to terrorists in Beirut, Lebanon. The case culminated in Federal prosecutors convicting 18 people for material support of terrorism and other crimes involved in the smuggling scheme. The lead defendant, Mohammed Hammoud, was sentenced in February 2003, to 155 years in prison.

Similarly, pursuant to the *2003 Strategy*, we will take full advantage of the combination of regulatory and criminal enforcement, including the vital role played by the financial sector in helping to deter and detect money laundering and terrorist financing. A robust regulatory system is essential to the success of our anti-money laundering/counter-terrorist financing efforts. The USA PATRIOT Act expanded our anti-money laundering regime to all financial institutions by requiring the establishment of anti-money laundering programs, creating the requirements for customer identification/verification programs, and enhancing recordkeeping and suspicious activity reporting requirements. The *2003 Strategy* takes full advantage of the greater transparency and more effective regulatory scrutiny the USA PATRIOT Act made possible to strengthen the partnership between government and the financial sector, in order to identify and combat terrorist financing and money laundering.

Over the past year, the Treasury Department, through the Financial Crimes Enforcement Network (FinCEN), has issued many of the regulations necessary to implement the Act's various anti-money laundering/terrorist financing provisions, further enhancing the civil regulatory regime. These implementing regulations make financial transactions more transparent, provide the government with more information about financial activity in new sectors, and deter misuse of the U.S. financial system by money launderers and terrorists. They also promote closer cooperation between the public and private sector. By requiring financial institutions to concentrate enhanced due diligence and suspicious activity monitoring on terrorist financing and money laundering schemes or typologies, they enable financial institutions to provide a much more effective first line of defense against money laundering, terrorist financing, and other financial crime. The information provided by financial institutions under the PATRIOT Act not only helps prevent money laundering and other financial crime, but also plays an important role in creating the type of audit trail that law enforcement can use to investigate money laundering and terrorism financing.

Continuing improvement of international cooperation is vital to law enforcement's efforts to combat terrorist financing and money laundering alike. In particular, the United States continues to pursue bilateral and multilateral designations of terrorist-related entities to block assets and cut off worldwide channels of terrorist funding. The United States plays a primary role in setting international standards to address money laundering and terrorist financing by working through the Financial Action Task Force (FATF) and the FATF-

style regional bodies (FSRBs). In this role, the united states continues to facilitate FATF's close collaboration with the World Bank, the International Monetary Fund (IMF), the UN Counter Terrorism Committee (UN/CTC), and other multilateral bodies to ensure that countries are assessed against their anti-money laundering/counter-terrorist finance regimes based on the FATF standards and are identified to receive priority technical assistance to enable full compliance with the standards.

The 2003 *Strategy* seeks to guide improvement in the anti-money laundering/counter terrorist financing regimes in foreign jurisdictions through bilateral outreach and technical assistance programs, as well as, through coordination with the international donor community. Our efforts will be backed, if necessary, by the authority provided by the USA PATRIOT Act to designate a foreign jurisdiction, foreign financial institution, type of international transaction, or type of account as a "primary money laundering concern," and to require U.S. financial institutions to take specified countermeasures. The United States also will work to strengthen multilateral and bilateral law enforcement cooperation on an operational level, including international information sharing and mutual legal assistance.

For 2003, the *National Money Laundering Strategy* has three overarching Goals:

1. *Safeguard the International Financial System from Money Laundering and Terrorist Financing*

2. *Enhance the United States Government's Ability to Identify, Investigate, and Prosecute Major Money Laundering Organizations and Systems*

3. *Ensure Effective Regulation*

Each of these Goals builds on the strategic framework and developments from previous strategies, and each is discussed in greater detail belowrecent achievements, as discussed in greater detail below.

Goal 1

"Safeguard the International Financial System from Money Laundering and Terrorist Financing"

Introduction

The modern financial system of the United States, like that of other developed nations, is vitally and inseparably integrated with the entire international financial system. This underlying reality means that international cooperation is critical to addressing the threats of terrorist financing and money laundering. Since both the formal and informal sectors of the international financial system can be accessed from virtually any point on the globe, it will continue to be susceptible to abuse by terrorist and criminal organizations unless countries throughout the world work together to identify, attack and punish its abuse. Accordingly, the United States will continue to rely heavily upon, and promote, close cooperation with our international partners to achieve collective success.

Our efforts to combat terrorist financing and money laundering require that we utilize our intelligence, law enforcement, and administrative powers. Among other things, they involve broadening and strengthening the legal, financial, and regulatory infrastructure of countries around the world to better secure the international financial system against abuse by terrorist groups and other criminal organizations.

The *2003 Strategy* for denying terrorist and other criminal organizations use of the international financial system focuses on six objectives for our work domestically and within the multilateral organizations:

- ◊ Blocking terrorist and illicit assets and cutting off worldwide channels of terrorist and illicit funding.
- ◊ Establishing and promoting international standards to be adopted by countries to ensure that their financial systems are adequately protected from abuse by terrorist and other criminal organizations.
- ◊ Ensuring that countries throughout the world consistently implement these international standards.
- ◊ Focusing efforts on financing mechanisms suspected of being of particular use by terrorist and other criminal organizations.
- ◊ Facilitating international information sharing.
- ◊ Enhancing outreach and cooperation with the private sector.

This comprehensive strategy has achieved significant results with respect to the fight against terrorist financing. These results are described in Appendix A, and are summarized below. Among the noteworthy achievements are the following:

- 315 terrorist-related entities and individuals are currently designated by the United States pursuant to E.O. 13224. The international community has frozen over $136 million in over 1400 accounts and transfers worldwide.
- 170 countries have blocking orders in force against the assets of terrorists, and 52 countries have submitted names to the United Nations Sanctions Committee for designation.
- In October 2002, fifty (50) nations combined to jointly designate Jemaa Islamiya (JI), an al-Qaida related terrorist network in Southeast Asia, as a terrorist group -- the most widespread show of support of any terrorist designation to date.
- Since September 11, 2001, the estimated worldwide total of assets seized pursuant to investigations with a possible terrorist link has risen to over $60 million .

- Since September 11, 2001, the Department of Justice has prosecuted over 45 individuals for "providing material support" to terrorists or for operating illegal transmitting businesses which illegally transferred millions of dollars to Iraq and other Middle Eastern countries. These cases include:

  ◊ On February 19, 2003, a Federal grand jury indicted Professor Sami Al-Arian, three overseas leaders of Palestinian Islamic Jihad (PIJ), and four members of the Tampa, Florida, PIJ cell headed by Al-Arian, for conspiracy to commit racketeering, murder, and for knowingly providing material support to PIJ, a designated foreign terrorist organization (FTO). PIJ is a Syrian-based organization that, as part of the Palestinian-Israeli conflict, has engaged in a campaign of suicide bombings and armed attacks that have killed hundreds of innocent people, including American tourists traveling in Israel.

  ◊ On December 18, 2002, a Federal grand jury in Dallas, Texas, returned a superceding indictment (following an initial indictment in February 2002), charging Ghassen Elashi, the chairman of the Holy Land Foundation for Relief and Development and HAMAS leader Mousa Abu Marzook, the Holy Land Foundation's most significant early donor, for prohibited financial dealings with terrorists.

  ◊ On February 10, 2003, Enaam Arnaout, Executive Director of the Benevolence International Foundation, pleaded guilty in Chicago to operating his charity as a Racketeer Influenced Corrupt Organization (RICO) enterprise and failing to tell donors that their money was being used to support violent *jihad.*

  ◊ On February 26, 2003, a Federal prosecutor unsealed criminal charges and brought criminal cases against persons in Syracuse, New York and Boise, Idaho, for allegedly financing terrorism through charities known as "Help the Needy" and "The Islamic Association of North America."

  ◊ Federal prosecutors, supported by FBI, ATF and IRS-CI agents, with close cooperation from local and Canadian law enforcement, convicted 18 people for material support and other crimes involved in a massive cigarette smuggling and tax evasion scheme, in which Lebanese members of a Charlotte, North Carolina, Hizballah Cell smuggled untaxed cigarettes from North Carolina to Michigan and used the proceeds to provide financial support and military equipment to terrorists in Beirut, Lebanon. The lead defendant, Mohammed Hammoud, was sentenced on February 20, 2003, to 155 years in prison.

- In March 2003, federal prosecutors in Brooklyn unsealed indictments against two Yemeni nationals, including Mohammed Ali-Hassan al-Moayad who boasted that he had provided some $20 million to Usama bin Laden, for engaging in a plot to raise funds from U.S. sources for al Qaida and HAMAS. These individuals are in German custody, and the United States is seeking their extradition.

- Since October 2001, the U.S Bureau of Immigration and Customs Enforcement (BICE) has seized over $28 million in bulk cash smuggling as a result of enhanced targeted efforts to capture illicit cross-border flows of money that may be related to terrorism.

A. Blocking Assets and Cutting off Worldwide Channels of Terrorist Funding

Identifying and interdicting terrorist assets in order to prevent terrorist activities will always be a primary objective of the U.S. international strategy. The U.S. government will continue to work with our partners abroad to freeze the assets of terrorist supporters and networks. This objective requires unparalleled cooperation, not only among our allies throughout the world, but among all parts of the United States government dedicated to this endeavor -- from intelligence and law enforcement to the diplomatic and regulatory communities.

Public designation of terrorist-related entities and blocking of assets has been a highly visible weapon in

the financial war on terrorism. The *2003 Strategy* calls for us to continue to wield this weapon against terrorists and their supporters and facilitators in order to prevent the collecting, receiving, consolidating, managing and moving of assets through the world's financial system.

Currently, 315 individuals and entities are designated under the U.S. Executive Order 13224 as terrorists or terrorist supporters, and 36 are designated as Foreign Terrorist Organizations (FTOs), and more than $136 million worldwide has been frozen, as a result of (1) the UN 1267 Sanctions Committee's continuous efforts to add names to its list of al Qaida-linked individuals and entities whose assets UN members are obligated to freeze and (2) our ability to persuade other nations to follow U.S. domestic designation/blocking efforts.[2] On numerous occasions, the United States has also sought to designate jointly, with our allies, individuals and entities as terrorists or terrorist supporters. A comprehensive list of all joint designations can be found in Appendix B.

U.S. designation efforts are underscored by the obligations imposed by United Nations Security Council Resolutions (UNSCRs) 1373 and 1455. UNSCR 1373 obliges all member states, among other things, to, freeze the assets of all terrorists without delay; criminalize the financing of terrorism; and prevent their nationals or other persons from providing material support or safe haven to terrorists. UNSCR 1455 is directed specifically at terrorists and terrorist supporters linked to al Qaida, Usama bin Laden (UBL), and the Taliban. UNSCR 1455 establishes and provides for ongoing updating of a list of al Qaida, UBL, and Taliban-linked individuals and entities whose assets member states are obligated to freeze. The United States has been by far the largest contributor of names to this list to date, yet as a result of our international efforts, many other allies are now taking their own actions, pursuant to their own investigations, to crack down on the individuals and entities that support these terrorist networks.

The U.S. and international actions to designate terrorists and their supporters publicly do much more than simply freeze specific terrorist-related assets. They also (1) help shut down the pipeline through which designated parties move money and operate financially in mainstream financial sectors; (2) inform third parties, who may be unwittingly financing terrorist activity, of their association with supporters of terrorism; (3) deter non-designated parties, who might otherwise be willing to finance terrorist activity; (4) expose terrorist financing "money trails" that may generate leads to previously unknown terrorist cells and financiers; (5) force terrorists to use potentially more costly and/or less efficient or reliable informal means of financing their activities; and (6) support our diplomatic efforts to strengthen other countries' capacities to combat terrorist financing through adopting and implementing legislation to comply with the obligations of UNSCRs 1455 and 1373.

B. Establishing International Standards

The measures described above target funds that have already entered the international financial system. Establishing international standards and ensuring their effectiveness is a long term element of this Strategy. It is designed to make it more difficult and expensive for criminals and terrorists to access the international financial system in the first place, and to make their fund movements more transparent if and when they do so.

We will continue to work diligently through the Financial Action Task Force (FATF) – the premier standard--setting body in the international campaign against money laundering and terrorist financing. Created by the G-7 in 1989, the FATF has since grown to 33 members, along with numerous observers, including the United Nations, IMF, and World Bank. FATF's primary mission is to articulate international standards for countries to adopt and implement in the areas of money laundering and terrorist financing, and to seek the greatest possible level of worldwide compliance with these standards.

The next two sections discuss the development of FATF's international standards – the Forty Recommendations on Money Laundering and the Eight Special Recommendations on Terrorist Financing –

[2] An aggregate of over $36 million in terrorist-related assets has been frozen since September 11, 2001 in the United States alone. Due to the collapse of the Taliban and the granting of licenses to designated entities, approximately $30 million has been unfrozen and, at present, the U.S. has $5.7 million frozen.

which, when taken together, represent the full range of measures that countries should have in place to combat money laundering and terrorist financing. They are followed by a section that discusses the measures that FATF, the United States, and the international community at large have taken to maximize the level of worldwide compliance with these standards.

The FATF Forty Recommendations on Money Laundering

The FATF Forty Recommendations on Money Laundering (the Forty Recommendations) represent the international standard for anti-money laundering regimes. They cover the complete range of measures that should be included in a national anti-money laundering regime, and focus on such areas as regulatory controls, supervisory mechanisms, and criminal laws, as well as international cooperation.

The Forty Recommendations were first articulated in the early 1990s and updated in 1996. As they have been applied and implemented throughout the world, ambiguities and gaps have been identified. Moreover, money laundering methods and techniques change as new measures to combat money laundering are implemented and new technologies are developed. Therefore, in 2001, FATF embarked on a review of the Forty Recommendations to ensure that they remain comprehensive and up-to-date. This major international undertaking culminated in June 2003, when the FATF unveiled the revised Forty Recommendations that substantially expand the scope and enhance the effectiveness of the international anti-money laundering standards. The revision also provided an opportunity for other countries to benefit, as the United States has, from the key anti-money laundering provisions of the USA PATRIOT Act, including tighter controls on foreign correspondent banking and transactions with foreign political officials.

The more significant revisions include the following:

- Expansion of the predicate offenses that must be covered by a criminal money laundering statute.
- Tougher customer due diligence requirements, including those that relate to the identification of the beneficial owners of corporate vehicles.
- Extension of appropriate anti-money laundering requirements to the full range of financial institutions and to other professions that serve as gateways to the financial system.
- Tighter requirements relating to correspondent banking, third party introducers, foreign political officials, and the issuance of bearer shares.
- Banning of shell banks worldwide.
- Requirements to establish financial intelligence units.
- Enhanced international cooperation related to money laundering.

As will be discussed in more detail below, the revised Forty Recommendations represent the new international standard with which countries around the world should endeavor to comply, and against which they will be assessed by the international community, including such international bodies as the IMF and the World Bank.

The FATF Eight Special Recommendations on Terrorist Financing

Though highly relevant to an effective counter-terrorist financing regime, the Forty Recommendations generally focus on the broader fight against money laundering. In response to the September 11, 2001 terrorist attacks, and under the leadership of the United States, the FATF expanded its mandate to address terrorist financing specifically to ensure that international standards covered all measures necessary to combat terrorist financing. On October 31, 2001, the FATF issued the Eight Special Recommendations on Terrorist Financing. The Eight Special Recommendations now represent the international standard for counter-terrorist financing regimes in the same way that the Forty Recommendations represent the international standard for anti-money laundering regimes.

The Eight Special Recommendations state that countries should take the following measures as international standards for countering terrorist financing:

I. Ratify the UN International Convention for the Suppression of the Financing of Terrorism and implement relevant UN Resolutions against terrorist financing.
II. Criminalize the financing of terrorism, terrorist acts, and terrorist organizations.
III. Freeze and confiscate terrorist assets.
IV. Require financial institutions to report suspicious transactions linked to terrorism.
V. Provide the widest possible assistance to other countries' law enforcement and regulatory authorities for terrorist financing investigations.
VI. Extend anti-money laundering requirements to alternative remittance systems.
VII. Require financial institutions to include accurate and meaningful originator information in money transfers
VIII. Ensure that non-profit organizations cannot be misused to finance terrorism.

Given the novelty of some of the issues incorporated into these new standards, the FATF has been working to elaborate on the Eight Special Recommendations by issuing interpretative notes and best practice guidance to assist countries in applying the Special Recommendations.

To date, the FATF has issued:

- An interpretative note on Special Recommendation VI establishing the minimum legal and regulatory requirements to which all money or value transfer services should be subjected.

- A draft best practices paper on Special Recommendation VI providing guidance on the full range of measures for countries to consider when establishing a regulatory regime for ARS, such as *hawala*.

- An interpretative note on Special Recommendation VII articulating the scope of the requirement and specifying the precise information that must be included in wire transfers.

- A draft best practices paper on Special Recommendation VIII calling for increased transparency and oversight of charities to ensure that financiers of terrorism cannot misuse non-profit organizations.

In the coming months, FATF plans to issue an interpretative note and best practices paper on Special Recommendation III to establish the steps necessary to implement effectively a terrorist asset blocking and confiscation regime. The United States will continue to lead and support these efforts to elucidate and implement these special recommendations.

In the field of international standard setting, the United States is also sponsoring and supporting an effort in the Organization of American States (OAS) to modify the Inter-American Drug Abuse Control Commission (CICAD) Model Regulations on Money Laundering to reflect the need to address the problems of terrorist financing. Under the U.S. presidency, the OAS CICAD Experts Working Group met in June 2003 to draft terrorist financing related amendments to the Model Regulations that will be based on the FATF standards and the related UN Security Council Resolutions concerning terrorist financing.

C. Ensuring Global Compliance with International Standards

Establishing international standards is only the first step toward denying terrorists and criminals access to the international financial system. Without vigorous and consistent implementation of these standards throughout the globe, terrorists and criminals will enter the international financial system at the point of least resistance, and preventive national efforts will be rendered considerably less effective.

Ensuring global compliance with international standards is accomplished through a three-prong strategy that includes: (i) objectively assessing all countries against the international standards; (ii) providing capacity-building assistance for key countries in need; and (iii) ensuring appropriate consequences for countries and institutions that fail to take reasonable

steps to implement standards to prevent terrorist financing and money laundering.

Global Assessments

The IMF and the World Bank

At the 2001 Annual Meeting of the IMF, World Bank and the FATF Style Regional Bodies in late September 2001, the United States and the G-7 stressed the importance of integrating anti-money laundering and counter-terrorist financing issues into the international financial institutions' financial sector assessments, surveillance, and diagnostic activities. As a result, and after a year of preparatory work among the FATF, the IMF and World Bank, in the fall of 2002, the Executive Boards of the IMF and World Bank endorsed a 12 month pilot project to assess global compliance with the anti-money laundering and counter-terrorist financing standards articulated by the FATF.

These assessments are being conducted by the IMF and World Bank, in the context of their financial sector assessment programs. The FATF and the FSRBs are participating in these assessments. By October 2003, between 46 and 56 assessments are expected to be completed during the project using this methodology. As of mid-May 2003, half the assessments were in progress. The United States will support efforts to make these assessments a permanent part of IMF and World Bank surveillance.

FATF

The FATF itself not only sets anti-money laundering and counter-terrorist financing standards, but also assesses countries against these standards. As discussed below, FATF further ensures appropriate consequences for countries that do not cooperate with international efforts.

The FATF is active in the following assessment initiatives:

- As a condition of membership, FATF members are obliged to participate in a peer review process called "mutual evaluations." Through this process, FATF members assess each other against the FATF standards, and develop plans to enhance each member's compliance

- As discussed above, FATF participates in the IMF/World Bank pilot program by providing experts for various assessment missions

- At its June 2003 Plenary, FATF announced its plans to work cooperatively with the international donor community – represented by the newly established Counter-Terrorism Action Group (CTAG) – and the United Nations to assess countries' compliance with the areas of overlap between the Eight Special Recommendations and the requirements of UNSCR 1373

FATF-Style Regional Bodies

FATF membership is limited to 33 members. There is also a small group of countries that are candidates for membership in the coming years. Participation in the international FATF system, however, is not limited, and over 100 countries throughout the world are members of FATF-Style Regional Bodies (FSRBs). These FSRBs participate as observers in all FATF meetings; assess their members against the FATF standards; and in many cases, participate in the IMF/World Bank assessment program. Currently, there are six FSRBs:

- Asia/Pacific Group Against Money Laundering (APG)

- Caribbean Financial Action Task Force (CFATF)

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

- GAFISUD (covering South America)

- Inter-Governmental Action Group against Money Laundering (GIABA) (covering West Africa)

- Moneyval (covering Central and Eastern Europe)

In addition, Central Asian and Middle Eastern Countries are working with the FATF to establish FSRBs. The establishment of such groups will be an important part of the U.S. government strategy to expand the scope of anti-money laundering and counter-terrorist financing efforts throughout the world using these bodies. The United states will continue to leverage the existance of FSRB's to expand the establishment of internationally-established anti-money laundering regimes throughout the world.

Capacity Building

In an effort to ensure global compliance with international standards, the United States helps build capacity, both bilaterally and through a number of different multilateral fora. On a bilateral basis, the United States regularly delivers anti-money laundering and counter-terrorist financing technical assistance, including legislative drafting, FIU development, judicial and prosecutorial training, financial supervision, and financial crime investigatory training. the U.S. government will build on its assistance efforts to date and will continue to deiver needed technical assistance around the world. Recent examples of bilateral anti-money laundering technical assistance include:

- In February 2003, an interagency U.S. team joined several FATF counterparts in assisting the Philippines to draft anti-money laundering legislation that meets international standards. Enactment of this legislation by the Philippines legislature, and its signing into law by President Arroyo, allowed the Philippines to successfully avoid the imposition of counter-measures by the FATF.

- In December 2002, an interagency U.S. team visited Turkey to help strengthen that country's counter-terrorist financing capabilities. The United States provided guidance on drafting new legislation to comply effectively with U.N. Resolution 1373, and on creating a separate entity to administer blocking orders.

- In May 2003, the United States assisted Serbia in enacting its anti-money laundering law; creating an FIU, and assessing the FIU's technical assistance needs, including analytical training and IT network guidance. The U.S. delegation proceeded to Podgorica, Montenegro, to assess progress on the Montenegrin anti-money laundering regime, construct a timeline by which legal and operational measures could be expected to be implemented, and gauge the current and future Montenegrin needs.

- From 2002-2003, a Treasury resident advisor and DOJ attorney provided Russian officials and legislators with a variety of anti-money laundering assistance. This assistance included advice on writing anti-money laundering legislation to meet international standards, developing regulatory policy, and establishing Russia's Financial Intelligence Unit--the Financial Monitoring Committee (FMC)-- to monitor financial transactions. Russia's efforts to be removed from the FATF Non Cooperative Countries and Territories (NCCT) list were successful, and Russia became a full member of the FATF in June 2003. Russia's FMC is a full member of the Egmont Group of Financial Intelligence Units.

- In 2002-2003 , an attorney from DOJ's Asset Forfeiture and Money Laundering Section (AFMLS) conducted several consultations with the Government of Albania regarding the money laundering and terrorist financing investigation of a UN Security Resolution listed person and the assets that were frozen pursuant to that investigation. In addition, AFMLS attorneys worked closely with the Ministries involved in drafting the new money laundering legislation, providing comments and advice, and finally met with the members of Parliament responsible for passing the legislation. Based upon this final meeting, the government agreed to revise parts of the law and submit it to a vote. The law was subsequently enacted.

- The United States has provided several countries with regulatory training, training related to trade-based money laundering, and financial investigative training.

In addition to its bilateral efforts, the United States has pressed for increased international burden sharing in the anti-money laundering/terrorist financing area, and has participated in the establishment of CTAG to coordinate the international provision of anti-terror-

ism training and technical assistance. Terrorism and international crime present a significant worldwide threat. Donor countries throughout the world must therefore join in ensuring that key developing countries have the capacity to protect their financial systems. Under the *2003 Strategy*, the United States will work intensively with our partners in the international donor community over the next year to ensure that mechanisms exist to coordinate the delivery of technical assistance and allow for appropriate burden sharing.

As noted above, the United States, along with other G-7 countries, has emphasized the need for the IMF and World Bank to increase their involvement in strengthening financial regulatory frameworks and to provide anti-money laundering and counter-terrorist financing technical assistance. The Executive Boards of the IMF and World Bank have responded by calling for both institutions to provide more technical assistance to members, particularly for capacity building and enhancing legal and institutional frameworks. The growing number of anti-money laundering and counter-terrorist financing assessments being conducted by these institutions will provide the basis for more systematic identification and prioritization of technical assistance needs. In addition, the World Bank, along with the IMF, has been leading the effort to establish an international mechanism for information sharing in order to coordinate and optimize the delivery of technical assistance.

Each of these efforts will be important in building the capacity of countries worlwide to ensure their ability to comply with established international standards.

Targeting Countries and Institutions That Fail to Implement Anti-Terrorist Financing and Money Laundering International Standards

As important as it is to establish international standards and to assist countries in their compliance efforts, it is equally imperative that countries refusing to cooperate face appropriate consequences. Ideally, these consequences arise from multilateral processes. However, the United States always reserves the right to use the tools provided by Congress to safeguard its financial sector from abuse by terrorists and criminals. The most important of these tools -- both multilateral and domestic -- play a significant role in the 2003 Strategy, and are discussed below.

The FATF Non-Cooperative Countries and Territories (NCCT) Process

Since 2000, the FATF has been engaged in a major initiative to identify NCCT's in the fight against money laundering. Specifically, this has involved developing a process to identify critical weaknesses in anti-money laundering systems that serve as obstacles to international cooperation in this area. The aim of this process is to reduce the vulnerability of financial systems to money laundering by ensuring that all jurisdictions adopt and implement sufficient measures for the prevention, detection, and punishment of money laundering.

In June 2000, the FATF issued an initial list of 15 NCCT jurisdictions. One year later, in June 2001, four countries – the Bahamas, the Cayman Islands, Liechtenstein, and Panama – were removed from the list after implementing significant reforms to their anti-money laundering regimes. At the same time, Burma, Egypt, Guatemala, Hungary, Indonesia and Nigeria were added to the list. In September 2001, the FATF identified two new jurisdictions – Grenada and Ukraine – as non-cooperative. Since then, FATF has removed 9 more of the listed countries – Dominica, Grenada, Hungary, Israel, Lebanon, the Marshall Islands, Niue, St. Kitts and Nevis and St. Vincent and the Grenadines – from the NCCT list after they implemented significant reforms. As a result of pressure created by the listing process, many of the 10 countries remaining on the NCCT list have now enacted most, if not all, of the necessary anti-money laundering legislation, and several of these countries are also now working toward implementing their new regimes. Most of the other countries on the list are actively engaged in enacting legislative reforms. A summary of the reforms each country has enacted can be found in Appendix C.

The United States will continue to work within the context of this process to pressure governments to make necessary changes to their relevant laws and preactices to ensure compliance with international standards and expectations.

USA PATRIOT Act Section 311

Section 311 of the USA PATRIOT Act authorizes the Secretary of the Treasury -- in consultation with the Attorney General and the Secretary of State -- to

designate a foreign jurisdiction, institution, class of transaction, or type of account as a "primary money laundering concern." This authority allows the Secretary to require U.S. financial institutions to take one or more special measures with respect to such designation. Once such a designation has been made, there are five specific special measures that can be imposed, either individually, jointly or in any combination:

- Enhanced record-keeping and reporting of certain financial transactions
- Information relating to beneficial ownership
- Information relating to certain payable-through accounts
- Information relating to certain correspondent accounts
- Prohibitions or conditions on opening or maintaining certain correspondent or payable-through accounts

To date, the United States has twice invoked Section 311 in support of the FATF NCCT process. In December 2002, in response to FATF's call for countermeasures on Ukraine and Nauru, the Treasury Department began the Section 311 process by formally designating those two jurisdictions as primary money laundering concerns, and announcing the intention to apply one of the statutory special measures. Ukraine responded to this designation by quickly enacting anti-money laundering legislation that met international standards, resulting in FATF lifting its call for countermeasures and obviating the need for the United States to proceed with the Section 311 process. FATF and the United States will continue to monitor the situation in Ukraine to ensure that the new law is effectively implemented.

Nauru, a jurisdiction that has provided licenses to several hundred shell banks, did not move as quickly as Ukraine to address its deficiencies. As a result, on April 17, 2003, the Department of the Treasury issued a Notice of Proposed Rulemaking, which, when finalized, will require U.S. financial institutions to terminate correspondent relationships with Nauru-licensed institutions. Since then, Nauru has enacted legislation that it claims will eliminate all Nauru-licensed shell banks within six months. The United States will continue to examine the situation in Nauru to ensure that the Nauru financial sector does not provide criminals a point of entry into the international financial system.

Section 311 is also available to target entities beyond those called for by the FATF NCCT process. As stated above, the provision authorizes the Secretary of the Treasury to target not just foreign jurisdictions, but also foreign institutions, classes of transactions, or types of accounts. In the coming year, the Treasury Department will examine the use of this authority to target foreign institutions involved in facilitating money laundering or terrorist financing.

D. Addressing Financing Mechanisms of Particular Concern

In addition to the broad international initiatives described above, the United States will continue to focus on specific financing mechanisms that are particularly vulnerable or attractive to terrorist financiers and money launderers. The U.S. government will employ a variety of interagency collaborative efforts, including Organized Crime Drug Enforcement Task Forces (OCDEF); High Intensity Financial Crimes Areas (HIFCAs); High Intensity Drug Trafficking Areas (HIDTAs); and Suspicious Activities Reports (SAR) Review Teams to identify criminal activities, the proceeds of which might be used to finance terrorism.

In this regard, the *2003 Strategy* will particularly focus on the following:

Charities

Curtailing the practice of financing terror through ostensibly charitable institutions is an important element in the global fight against terrorist financing. To address this problem, the United States is taking aggressive measures to (1) identify and shut down those charities that have ties to terrorist organizations; and (2) prevent legitimate charities from being abused by terrorist financiers without disturbing legitimate charitable donations and charitable work.

Under the authority of Executive Order 13224, the United States has designated 23 charitable organizations as having ties to al Qaida or other terrorist groups, including the Holy Land Foundation for Relief and Development that acted as a funding vehicle for the HAMAS terrorist organization. Many of our international partners have also closed down suspect charities, often seizing their assets and/or arresting the individuals responsible for the abuse of these organizations.

Internationally, we have worked bilaterally with key jurisdictions, and also multilaterally through the FATF, to prioritize this issue. As noted above, a key step in this process involves the FATF's articulation of Special Recommendation VIII as an international standard, and its issuance of a best practices paper on the protection of charities and other non-profit organizations (SR VIII). Pursuant to the establishment of these standards, several jurisdictions, including the Gulf States, have undertaken actions to monitor how their charitable organizations operate, especially in conflict zones, in order to protect them from abuse or infiltration by terrorists and their supporters.

Domestically, we are working with the private non-profit sector to develop self-monitoring mechanisms for charitable and non-governmental organizations. Treasury officials have met with charitable sector watchdog and accreditation organizations, including the *Better Business Bureau Wise Giving Alliance* and the *International Committee on Fundraising Organizations*, to raise their awareness of the threat posed by terrorist financing. In addition, in 2002, the Treasury Department developed voluntary best practices guidelines for all U.S.-based charities. The guidelines, which are consistent with the principles espoused by the FATF and in the private sector, focus on financial controls and vetting of potential foreign recipients. They call for rigorous, self-imposed financial oversight; high levels of disclosure and transparency; and immediate severing of all ties to any foreign recipient associated with a terrorist organization. Although wholly voluntary, if implemented with sufficient resources and diligently adhered to in practice, the guidelines offer a means by which charities can protect themselves against terrorist abuse, enhance donor confidence, and significantly reduce the risk of a blocking order.

Hawala/Alternative Remittance Systems

The terrorist attacks of September 11, 2001 brought into sharp focus the ease with which terrorist financiers and other criminals can use alternative remittance systems (ARS), also known as informal value transfer systems (IVTS), or *hawala*,[3] to move and launder large amounts of money quickly and surreptitiously. The very features that make *hawala* attractive to legitimate customers – efficiency, reliable access to remote or under-developed regions, potential anonymity, and low cost – also make the system attractive for the transfer of criminal proceeds or terrorist-related funds. These informal systems of transferring money are prevalent throughout the world, including South Asia, the Middle East, Europe, and North America. In some countries, *hawala* is illegal; in others, it is unregulated. Since ARS such as *hawala* have largely escaped financial regulatory scrutiny, it is difficult to measure accurately the total volume of financial activity associated with such systems.

The United States has already taken steps to regulate *hawala* and other ARS. Money remitters (informal or otherwise) must register as a "money services business" (MSB). As a result of Bank Secrecy Act regulations issued by FinCEN, well over 14,000 MSBs--money transmitters, money order businesses, traveler's check businesses, and currency exchangers -- have registered with the federal government since the December 31, 2001 deadline, and are also required to report suspicious activities.[4] The PATRIOT Act also makes it a crime for a money transfer business owner or operator to move funds that the owner knows are either the proceeds of a crime, or are intended to be used for an unlawful activity, including terrorism.

[3] The word "*hawala*" refers to a fast and cost-effective method for the worldwide remittance of money or value, particularly for persons who may not have ready access to the regulated financial sector. In *hawala*, an individual in one country gives funds to a *hawala* broker, who notifies a counterpart (usually of the same extended family or ethnic group) in another country, to transfer an equivalent amount of money to a recipient in that country. The transaction occurs informally, outside the regulated financial system, without using financial instruments that would create a "paper trail".

[4] To increase awareness within the diverse MSB community nationwide about their obligations under the new MSB rules, FinCEN is conducting an outreach campaign, which includes advertising, community outreach, and distributing educational materials.

Failure by money service business principals to register with FinCEN, and/or failure to obtain a state license, also are federal crimes.[5]

Using this new authority, the United States has succeeded in disrupting the operations of several illegal money remitters potentially implicated in terrorist financing. Recent investigations in Buffalo, Brooklyn, Detroit, Denver, Minneapolis and Seattle, have led to charges involving the illegal transmission of funds to Yemen, Iraq and elsewhere. In each of these investigations, the illegal transmission of funds to a country associated with terrorist activities formed a predicate for possible links to the financing of terrorism. Tracing those funds after they reach the destination countries is a complicating factor, but an essential, element in a terrorist financing charge.

We are also working bilaterally and multilaterally to ensure the integrity and transparency of ARS worldwide. FATF Special Recommendation VI, discussed above, addresses this issue by requiring countries to register or license ARS, and subjects them to all the FATF Recommendations that apply to banks and nonbank financial institutions. In addition, at a conference on *hawala* in the United Arab Emirates (UAE) in May 2002, nearly 40 countries drafted and agreed upon the *Abu Dhabi Declaration on Hawala*, which sets forth a number of principles calling for the regulation of *hawala*, including adoption of FATF Special Recommendation VI. Shortly thereafter, the UAE government announced that it would impose a licensing requirement on *hawala* operators operating within its borders. Other countries responded by developing regulatory requirements for the first time. This development significantly enhances information gathering and sharing and financial transparency in the informal financial sector.

In addition to our work to ensure the integrity and transparency of ARS, we are working bilaterally and multilaterally to identify and address the factors that contribute to the use of ARS for legitimate purposes. These factors vary by country and can include the low cost, convenience, security, speed, and ease of access to ARS, as opposed to the formal financial sector. A bilateral initiative with Mexico suggests that greater competition and technological innovation can increase the use of the formal system over ARS. Building upon this, we have broadened our work on remittances by co-chairing the APEC Finance Ministers Working Group on ARS to examine the economic and institutional factors contributing to the use of ARS in the Asia-Pacific region. We have also encouraged the multilateral development banks to study existing ARS networks and to consider ways to increase the use of the formal system, which would allow better monitoring of compliance with AML/CFT standards.

As part of our international effort to combat the exploitation of ARS by terrorists and money launderers, the United States also provides training and technical assistance to other countries. For example, FinCEN hosted an international conference on ARS (IVTS) in Oaxaca, Mexico on October 9, 2002, which covered money laundering risks and law enforcement and regulatory challenges posed by ARS.[6]

The United States government will continue to focus our efforts on the regulatory, institutional, and enforcement elements of this financial vehicle and to create greater transparency and accountability in such movement of funds globally.

Bulk Cash Smuggling

Bulk cash smuggling is yet another means of transferring resources used by both money launderers and terrorists. In the United States alone, BICE has executed 650 bulk cash seizures, totaling $28 million, including more than $19 million with a Middle East connection. But disrupting bulk cash smuggling requires a global approach. To identify and attack bulk cash movements, we are working with the international community to ensure mandated inbound/outbound currency reporting at reasonable levels (*e.g.*, the U.S. reporting threshold is $10,000).

[5] See 18 U.S.C. § 1960.

[6] At the Oaxaca Conference, FinCEN shared key findings from its domestic law enforcement outreach efforts with international law enforcement officials. Speakers included representatives from Italy, the United Kingdom, Pakistan, Bahrain, the International Monetary Fund, and the World Bank

In addition, we will work to foster international cooperation among intelligence-gathering; law enforcement; customs; and immigration officials to share information about potential terrorist financing smugglers/couriers. In this regard, we are continuing to explore the creation of bilateral, and possibly multilateral, customs-to-customs Hotlines, where appropriate, to exchange "real time" bulk currency information on large-value cross-border cash transfers. In addition, the U.S. government is exploring the use of international fora, like the FATF typologies exercises, both to better the understand the contours of this problems and to address the risks in the multilateral or regional fashion.

A recent narco-terrorist investigation illustrates our successful law enforcement efforts to combat bulk cash smuggling. The investigation revealed that a Colombian national, affiliated with the Revolutionary Armed Forces of Colombia (FARC) Narco-Terrorist group and guerilla army, was an active money launderer who was engaged in bulk cash smuggling. When he attempted to transport 182,000 Euros into the United States, BICE agents arrested him on October 22, 2002, for failure to obtain a state money-transmitting license, in violation of 18 U.S.C. 1960, and seized the money. The investigation is ongoing.

Trade-Based Money Laundering and Terrorist Financing

Both terrorist financiers and money launderers may use trade-based mechanisms to raise, launder, and move their funds. Trade-based schemes move money intended for criminal purposes, including terrorism, by means of commerce in either licit or illicit goods.[7] For instance, we now know that the Taliban and the FARC rely on international narcotics trafficking to raise funds to support their terrorist activities. Moreover, as we have learned from experience with these terrorist entities, the associations terrorist groups establish with narcotics traffickers give them ready access to the arms traffickers, smugglers, and illicit communications and transportation facilitators that service narcotics organizations.

Similarly, major international drug traffickers rely extensively on trade-based money laundering schemes to disguise and move the illicit proceeds of drug crimes. For instance, Colombian drug cartels use a complex trade-based money laundering system, the Black Market Peso Exchange (BMPE), to launder billions of dollars annually in cash proceeds from illegal narcotics sales in the United States. Those who use the BMPE to move funds seek to evade the reporting and record keeping requirements of the Bank Secrecy Act, as well as Colombian foreign exchange and import laws and tariffs, by using drug proceeds in the United States to buy U.S. trade goods, such as major household appliances, consumer electronics, liquor, cigarettes, used auto parts, and precious metals. Such goods are then imported or smuggled into Colombia, where they are sold in the normal stream of commerce.[8]

Under the *2003 Strategy*, we will continue to investigate the use of licit and illicit international trade commodities, including diamonds, gold, honey,

---

[7] Appendix D provides a detailed description of trade-based money laundering and terrorist financing.

[8] The BMPE launders drug proceeds through the following steps:

1. Colombian cartels export narcotics to the United States, where the illegal drugs are sold for U.S. dollars.
2. The cartels contact a peso broker in Colombia to launder their drug money.
3. The peso broker agrees to exchange pesos that he controls in Colombia for U.S. dollars that the cartel controls in the United States—i.e., the peso broker buys the cartel's U.S. dollars, paying the cartel with pesos in Colombia. At this point, the cartel has effectively laundered its money and is out of the BMPE process.
4. The peso broker uses contacts in the United States to place the drug dollars he purchased from the cartel into the U.S. banking system, and "sells" these narcotics proceeds to legitimate Colombian importers, who place orders for items and make payments through the peso broker.
5. The peso broker uses contacts in the United States to purchase the requested items from U.S. manufacturers and distributors, and pays for these goods using a variety of methods, including his U.S. bank accounts.
6. The purchased goods are shipped to Caribbean or South American destinations, sometimes via Europe or Asia, and are then smuggled or otherwise fraudulently moved into Colombia, where the importer pays the peso broker for the merchandise with Colombian pesos and takes possession of his goods, having avoided paying extensive Colombian import and exchange tariffs. The peso broker, who has made money charging both the cartels and the importers for his services, uses the pesos paid by the importers to buy more dollars in the United States from the cartels, and the cycle begins again.

cigarettes, and the pirating of intellectual property as well as narcotics, to fund terrorism. We will also continue our efforts to identify under- and over-invoicing schemes that mask the movement of terrorist and criminal funds.

To counter trade-based terrorist financing and money laundering systems, it is essential that the government utilize bilateral and multilateral mechanisms, including the sharing of law enforcement tools designed to address trade-based money laundering and terrorist financing schemes. In this regard, BICE has developed a state-of-the-art database system, the *Numerically Integrated Profiling System* ("NIPS"), which identifies anomalous trade patterns for imports/exports to/from the United States. BICE has demonstrated this system to other nations, including Colombia, and more recently, the UAE, with important resultsand bilaterl leads and information. We will continue to pursue sharing trade-based data bilaterally and on a regional basis, to identify and attack anomalous activities that might mask terrorist financing and/or money laundering. We also will provide international training on trade-based money laundering and terrorist financing schemes.[9] In addition, we will continue to combat illicit international trade commodities, such as narcotics, by building on existing domestic and international law enforcement and investigative authorities and initiatives.

Cyber Crime

The Department of the Treasury is currently working with other government agencies and departments to develop an effective approach for investigating and interdicting terrorist cyber-fundraising activities. In this regard, we will take all possible action to preserve the integrity of the financial system and the vitality of e-commerce, while stopping the flow of terrorist-related funds. See Appendix H, Terrorist Financing Online.

E. Facilitating International Information Sharing

Information sharing is critical to fighting terrorism and financial crime. An essential element of our efforts to identify and dismantle terrorist financing is the ability to access terrorist-related information quickly from our international partners. To improve the flow of financial information related to terrorist financing or money laundering, we have worked to establish and expand international information-sharing channels. Through FinCEN, the U.S. Financial Intelligence Unit (FIU), we have directed the attention of the Egmont Group, which now represents 84 FIUs from various countries around the world, to terrorist financing. Since September 11, 2001, at the urging of the United States, the Egmont Group has taken steps to leverage its information collection and sharing capabilities to support the global war on terrorism. On October 31, 2001, FinCEN hosted a special Egmont Group meeting that focused on the role of FIUs in the fight against terrorism. The FIUs agreed to: (1) work to eliminate impediments to information exchange; (2) make terrorist financing a form of suspicious activity to be reported by all financial sectors to their respective FIUs; (3) undertake joint studies of particular financial activities vulnerable to abuse by money laundering and terrorist financing (e.g. *hawala)*; and (4) sanitize cases so that they can be used for training purposes. Egmont has conducted, and will continue to host, training sessions to improve the analytical capabilities of FIU staffs around the world.

The United States is committed to supporting the expansion and enhancement of FIUs worldwide, and FinCEN is currently mentoring several FIU's which are under consideration for admission to the Egmont Group. By expanding the Egmont Group, we will increase the sharing of relevant information through established channels as well as to spur the amount of financial data analysis conducted and shared worldwide.

[9] In addition, we will continue to combat the use of trade-based terrorist financing and money laundering in commodities. The Department of the Treasury and BICE, in consultation with the Departments of Justice and State, have developed an international training program that sensitizes foreign customs and law enforcement officials to trade-based money laundering schemes and introduces them to BICE-developed software used to combat it. BICE presented an inaugural trade-based money laundering program in Abu Dhabi and Sharjah / Dubai, United Arab Emirates (UAE) from October 10-17, 2002. The program included detailed presentations on money laundering in general and trends in commodity and trade-based money laundering in particular, as well as on terrorist financing issues; organizing and presenting a money laundering case; and a demonstration of the Numerically Integrated Profiling System, using UAE data. This inaugural event was a successful first step in providing assistance to priority countries in the Middle East. Additional programs were conducted in Qatar and Kuwait, and more are planned for Pakistan and India.

F. Outreach and Cooperation with the Private Sector

The private sector often serves as the front-line in the war against terrorist financing. To date, cooperation with the private sector, including banks and trade associations, has been essential to increasing our vigilance against the abuse of our financial system by terrorist groups. With the expansion of our anti-money laundering provisions to new segments of the financial community pursuant to the USA PATRIOT Act, we will expand such cooperation. During the coming year, we will continue to work with our domestic financial community, including banks, credit card issuers and redeemers, and internet service providers, among others, to enhance their abilities to detect and report possible terrorist-related activities, thereby augmenting the value of our regulatory regime and its public-private partnership to the government's fight against terrorist financing.

In particular, we intend to improve cooperation with the private sector by: (1) increasing the amount of information the Federal government provides with respect to its ongoing efforts; (2) providing feedback on the usefulness of the private sector's efforts; (3) educating the private sector to recognize terrorist financing-related typologies and "red flags"; (4) reinvigorating the law enforcement-industry partnership to develop "best practices" for corporations to follow to avoid BMPE transactions and (5) enhancing ongoing due diligence efforts, while balancing the demands on institutions. These initiatives aim to enhance the ability of both the public and private sectors to insulate the financial system from abuse, while ensuring the free flow of capital and commerce. Such efforts will also enhance the government's abilities to uncover and disrupt terrorist financing schemes and networks.

Goal 2

Enhance the United States Government's Ability to Identify, Investigate and Prosecute Major Money Laundering Organizations and Systems

Introduction

At a time when the Federal government's law enforcement mission must increasingly focus on protecting our nation from terrorist attack, we will make the most of existing anti-money laundering/terrorist financing resources by directing them where they will have maximum impact. We will do this by making money laundering a primary—not merely an ancillary—part of any attack on substantive crimes that generate illicit proceeds and/or that facilitate terrorism, and by targeting the financial infrastructure through which illicit proceeds are placed and moved.

Regardless of the predicate offenses generating illicit proceeds, where the proceeds take the form of large volumes of cash, the money itself becomes an "Achilles heel" for the criminals. We will exploit this vulnerability and follow the money downstream, to identify the professionals moving and laundering illicit proceeds through the global financial systems, and upstream, to identify perpetrators of the substantive offenses.

In this regard, Federal and state anti-money laundering laws and regulations provide criminal and civil investigators with the legal authority to investigate suspicious behavior and to identify and attack significant criminal activity, including drug trafficking, white collar crime, fraud, and corruption, as well as terrorism. These statutes and regulations also provide strong support for the seizure and forfeiture of criminal proceeds, instrumentalities of the crime, and facilitating property.

Anti-money laundering laws and regulations are most effectively applied using interagency and international cooperation to identify and target vulnerabilities in financial systems and mechanisms and the financial professionals who, either knowingly or unwittingly, place and move illicit funds, corrupt and abuse otherwise legitimate financial sectors. Recent examples of significant cases developed by these methods are described in Appendix E.

The *2003 Strategy* continues and further develops our efforts to identify and attack financial systems by improving our efforts in seven key areas:

- Enhancing Interagency Coordination.
- Ensuring that Law Enforcement Agencies and Task Forces Use and Share Financial Databases and Analytical Tools.
- Focusing Law Enforcement Personnel and Other Resources on Highest-Impact Targets and Financial Systems.
- Utilizing New and Improved Statutory and Regulatory Authorities.
- Increasing International Operational Cooperation.
- Improving United States Government Interaction with the Financial Community.
- Helping State and Local Governments Investigate and Prosecute Money Laundering and Financial Crime Cases.

A. Enhancing Interagency Coordination

The Federal government will continue to develop and use interagency mechanisms, such as Organized Crime Drug Enforcement Task Forces (OCDETF), High Intensity Drug Trafficking Areas (HIDTAs), and High Intensity Financial Crimes Areas (HIFCAs), as well as the Joint Terrorism Task Force (JTTF),[10] the National Joint Terrorism Task Force (NJTTF),[11] and the Foreign Terrorist Asset Targeting Group (FTAT-G).,to ensure that money laundering and asset seizure and forfeiture are fundamental components of all significant investigations undertaken or supported by any of these Task Forces, and that enhanced coordination and consultation routinely occurs among them. These interagency Task Forces leverage scarce anti-money laundering law enforcement resources by targeting key money laundering professionals and financial mechanisms, such as bulk cash movement[12] and wire remissions, that are most abused by criminals.

HIFCAs have been created specifically to identify and address money laundering in designated geographical areas. HIFCA Task Forces seek to improve the quality of federal money laundering and other financial crime investigations by concentrating the expertise of the participating Federal and state agencies in a unified task force, utilizing all FinCEN, Drug Enforcement Agency (DEA) Special Operations Division, and BICE Money Laundering Coordination Center financial databases. As called for in the *2002 Strategy*, we are currently reviewing the operation of the HIFCAs in order to enhance their potential and ensure that they complement other appropriate interagency initiatives and task forces.

To help coordinate the use of investigative resources aimed at the most significant drug trafficking/drug money laundering organizations, in July 2002, the Attorney General established, through OCDETF, the Consolidated Priority Organization Target (CPOT) List. The CPOT list allows the Federal government to better track the collective use of investigative resources aimed at the highest-value narcotics money laundering targets, and to evaluate more precisely the impact of these law enforcement efforts.

Effectively attacking the financial infrastructure of the most significant drug trafficking organizations requires us to focus, as a primary, not ancillary matter, on the mechanisms and financial systems used to move and launder billions of dollars of illicit funds. Recognizing that an interagency, strategic attack on the financial infrastructure of international drug trafficking is essential to destabilize these activities, under the *2003 Strategy*, we are taking aggressive steps to develop an interagency anti-drug-money laundering financial intelligence center, to serve as a drug-money laundering intelligence and operations center at law enforcement headquarters. It is anticipated that this center, currently in the initial planning stages, will consist of money laundering investigators, prosecutors, and analysts dedicated exclusively to reviewing and acting upon all law enforcement and other financial information in order to develop the highest value targets, identify and disseminate information about developing trends and patterns, and help coordinate financial attacks on the systems, geographic locations, and individuals by and through which drug proceeds are moved and laundered.

---

[10] JTTFs are teams of federal, state and local law enforcement officers and personnel who work shoulder-to-shoulder to investigate and prevent acts of terrorism. These task forces are important "force multipliers" in the war on terror, pooling multi-agency expertise and ensuring the timely collection and sharing of intelligence, including financial intelligence, absolutely critical to prevention efforts. Although the first JTTF came into being in 1980, the total number of task forces has nearly doubled since September 11, 2001. Today, there are 66 JTTFs, including one in each of the FBI's 56 main field offices and ten in smaller offices. More than 2,300 personnel work on these task forces nationwide including approximately 1,700 federal agents and 649 full-time officers from state and local agencies.

[11] The NJTTF was created at FBI Headquarters in July 2002, and includes representatives from 30 other government agencies representing the intelligence, law enforcement, defense, diplomatic, public safety and homeland security communities. The National JTTF collects terrorism information and intelligence, including financial information and intelligence, and funnels it to the 66 JTTFs, various terrorism units within the FBI, and partner agencies. Agency representatives assist the FBI with all aspects of terrorism investigations.

[12] In the international arena, BICE, under the supervision of the Department of Homeland Security, will initiate bilateral Bulk Cash Movement Task Forces that will utilize inbound/outbound cash reporting laws of each nation, to identify and attack anomalies.

B. Ensuring that Law Enforcement Agencies and Task Forces Use and Share Financial Databases and Analytical Tools

At present, each Federal law enforcement agency collects information relevant to its own cases. For example, the United States Postal Service has a database that identifies and traces the movement from point-of-sale to final deposit of potentially suspicious Postal Money Orders sold in the United States. Similarly, in the area of trade-based money laundering, such as the Black Market Peso Exchange System, BICE's Numerically Integrated Profiling System ("NIPS") identifies anomalous trading patterns. Likewise, BICE's Money Laundering Coordination Center and DEA's Special Operations Division each have their own financial databases.

Each of these databases and analytic tools is useful by itself, but currently there is no single intelligence center that consolidates all of the information separately available in Federal agencies to provide a one-stop point of information and analysis on trends and statistics in money laundering cases. Such information is essential in order to improve our ability to develop an accurate threat assessment and implement measures that will most effectively address that threat. One of the functions of the interagency anti-drug-money laundering financial intelligence center
described above will be to utilize all available financial and other sources of financial information to compile trends and patterns of drug-money laundering. A second important function will be to identify significant money laundering targets and disseminate the leads for investigation. The center will also support and, where appropriate, help coordinate multi-district criminal investigations.

FinCEN Databases and Analytic Resources

FinCEN's databases and resources play an important role in U.S. enforcement efforts against money laundering, terrorist financing, and other financial crimes. Money laundering laws and techniques have changed significantly since FinCEN was created in 1990. Consequently, FinCEN must evolve in order to keep pace with, and anticipate, these changes. As our FIU, FinCEN must develop and implement new generations of analytical tools that provide enhanced capabilities to track money laundering activity across multiple BSA databases and provide faster, more efficient cross-linkages with law enforcement and other national information sources. FinCEN has already taken some necessary steps in this regard. In particular, it has enhanced Federal, state and local law enforcement access to BSA data by expanding its "Gateway Program," and by creating new resource centers, such as its Geographic Threat Assessment and Non-Traditional Methodologies Sections.

Beyond these developments, under the *2003 Strategy*, FinCEN will continue to improve its Gateway Program in order to streamline law enforcement access to BSA data and provide a de-confliction mechanism for law enforcement entities. In addition, the Department of the Treasury will thoroughly re-examine FinCEN's crucial role in the Federal government's anti-money laundering and anti-terrorist financing programs and identify any necessary improvements in the anti-money laundering information delivery systems. FinCEN's databases and resources will play an important role in the interagency anti-drug-money laundering financial intelligence center, described above.

C. Focusing Law Enforcement Personnel and Other Resources on Highest-Impact Targets and Financial Systems

Our *2003 Strategy* calls for those districts bringing the largest number of money laundering prosecutions to continue their aggressive and productive efforts.[13] Numbers alone, however, do not necessarily ensure the most effective use of scarce[14] money laundering enforcement resources. To do that, we must ensure that we are successfully targeting and disabling *significant* money launderers.

[13] Attached as Appendix I are the Highlights of money laundering defendants sentenced in FY2001.

[14] Our challenge is especially acute in light of the recent extension of SAR filing requirements. SAR filing requirements have been extended to the money service business industry, broker-dealers, and casinos, and SAR requirements for other types of financial institutions are being finalized. In order to review, analyze, and investigate these reports with maximum efficiency, we have developed SAR Review Teams, composed of representatives from Federal, state, and local law enforcement agencies, typically with the participation of an Assistant U.S. Attorney, to evaluate all SARs filed in the team's respective Federal district.

Accordingly, under the *2003 Strategy*, we will make even greater efforts to concentrate enforcement resources on cases that will shut down systems and organizations moving illicit proceeds. In particular, we will apply the lessons learned and information obtained from past operations to ongoing and future efforts in order to: (1) encourage, enhance, and pursue cutting-edge bilateral operations; (2) identify and attack bulk cash movements systematically and enhance national targeting of bulk cash mechanisms through bi-lateral relationships with currency-importing/exporting countries; (3) identify and attack drug money laundering systems, such as the Colombian Black Market Peso Exchange; and (4) address illegal money remitters through the appropriate use of Section 373 of the USA PATRIOT Act,[15] that enhanced the BSA's "unlicensed money remitter" provision. FinCEN's registration of specified money service businesses, including money remitters, will enhance law enforcement's ability to target those who fail to register; register falsely; and/or knowingly deal with criminal proceeds.

One important example of new efforts to focus law enforcement resources on large money laundering financial systems is the Department of Homeland Security's (DHS) *Operation Cornerstone. Operation Cornerstone* is a new financial investigations program to identify vulnerabilities in financial systems through which criminals launder their illicit proceeds, bring the criminals to justice, eliminate the vulnerabilities, and develop a working partnership with industry representatives to share information and close industry-wide security gaps that could be exploited by money launderers and other criminal organizations. *Operation Cornerstone* will:

- Identify and assess the means and methods used by criminals to exploit financial systems in order to transfer, launder and otherwise mask the true source of criminal proceeds.

- Work with specific private sector industries to gather new information and reduce vulnerabilities found within existing financial systems.

- Assign a dedicated special agent to each of the 25 field offices of BICE to liaison with the private sector.

- Investigate and prosecute criminal organizations exploiting emerging traditional and non-traditional financial systems.

- Work with financial institution security teams to help them understand how criminal organizations exploited financial systems in their industry.

- Provide the private sector with a quarterly report that details specific examples of how certain U.S. financial systems are being exploited by criminal organizations to transfer, launder or mask the true source of criminal proceeds. The report will provide recommendations to industry on how to detect and prevent such exploitation.

In addition to these investigative efforts, we will enhance and leverage our existing money laundering enforcement resources through more focused training efforts. A crucial component of any anti-money laundering effort is a well-trained cadre of financial specialists. As it takes many years to develop an experienced financial investigator, and as many of our most experienced investigators are reaching retirement age, we will continue to focus on hiring and training law enforcement personnel skilled in financial investigations and analysis. For the same reasons, we will emphasize and, where necessary, expand the training of financial analysts. Because banks, as well as other financial institutions, can play an important role in detecting and attacking money laundering, we will also make concerted efforts to develop and expand the role of the private sector.

D. Utilizing New and Improved Statutory and Regulatory Authorities

The United States will aggressively utilize all new and previously-existing legislation to identify and attack the financial infrastructure of financial criminals and money launderers. As discussed above, we are already

[15] Codified at 18 U.S.C. 1960.

using the host of new or enhanced authorities provided by the USA PATRIOT Act, as well as existing BSA and anti-money laundering criminal and civil provisions, to track, seize, freeze and forfeit money, and impose sanctions on lax jurisdictions. For example, as discussed earlier, U.S. law enforcement is aggressively using the re-invigorated provisions of 18 USC 1960 to target the illegal movement of funds through the domestic and international wire transfer systems.

We also are using the International Economic Emergency Powers Act (IEEPA) sanctions authority, under Executive Order 12978 and the Foreign Narcotics Kingpin Designation Act, to deny drug traffickers access to the U.S. financial system by freezing their assets and prohibiting U.S. businesses from any dealings with individuals and businesses associated with named major drug kingpins. In February 2003, the Department of the Treasury's Office of Foreign Assets Control (OFAC) successfully targeted the extensive financial network controlled by Cali cartel leaders Miguel and Gilberto Rodriguez Orejuela by designating 137 companies and individuals as Specially Designated Narcotics Traffickers (SDNTs). This OFAC action targeted a Colombian money exchange business and a stock brokerage firm that actively moved millions of dollars through the U.S. financial system on a monthly basis.

In March 2003, OFAC targeted 2 new Colombian cartel leaders, Joaquin Mario and Guillermo Valencia Trujillo, and their financial network of 58 companies and individuals. This SDNT action was coordinated with a multi-agency drug task force and the U.S. Attorney's Office in Tampa, Florida.

In May 2003, OFAC utilized a blocking action under E.O. 12978, which was strengthened by the USA PATRIOT Act, to "block pending investigation" of the bank accounts of several U.S. and Bahamian companies that were controlled by SDNT individuals designated in the February and March 2003 SDNT actions. Since the inception of the SDNT program in 1995, OFAC has named 824 Colombian drug cartel individuals and businesses.

In consultation with the Departments of Justice, State and Defense, and the Central Intelligence Agency, Treasury's OFAC coordinated the annual worldwide drug kingpin designation process established by the Foreign Narcotics Kingpin Designation Act to recommend the designation of new drug kingpins to the President. On June 2, 2003, the White House announced seven new drug kingpins. The 2003 action named three "foreign entities" as drug kingpins. These include two narco-terrorist groups: including the Revolutionary Armed Forces of Colombia and the United Self-Defense Forces of Colombia, a Colombian paramilitary force. The third drug Kingpin group is the United Wa State Army, which is a Burmese ethnic guerilla army. The two Colombian entities were previously named as foreign terrorist organizations by the U.S. government. To date, a total of 38 foreign persons have been named as foreign drug kingpins by the President.

These designations seriously inhibit a designated individual and entity from conducting business as usual. They absolutely prohibit financial dealings with U.S. individuals and firms, and increase pressure on any host country to investigate and/or take other steps to stop the designated individual and entity from operating.

E. Increasing International Operational Cooperation[16]

Significant domestic money laundering investigations inevitably lead beyond U.S. borders. To successfully investigate and prosecute persons involved in complex, transnational money laundering schemes, and to seize and forfeit assets and instrumentalities located abroad, U.S. law enforcement agencies must work closely with our foreign counterparts. This type of international cooperation and coordination is becoming increasingly critical in the global fight against money laundering, as well as terrorist financing, and is a central component of our *2003 Strategy*.

The United States has built a strong record of successful cooperative international investigations and/or mutual legal assistance with a number of foreign jurisdictions, including Canada, Hong Kong, Italy, Spain, Switzerland, the United Kingdom and most

[16] Non-operational international matters are discussed primarily in Goal 1.

recently, Colombia. Many cooperative relationships grow from our training and technical assistance projects and are enhanced by our international forfeited assets sharing program.[17] The United States will build upon these strong relationships; develop new ones; and apply a "lessons learned" approach to ensure that we can pursue international financial investigations as seamlessly and aggressively as possible.

F. Improving United States Government Interaction with the Financial Community

From both a regulatory and information-sharing perspective, working with the financial services community is essential to any effective money laundering/terrorist financing enforcement strategy. Under the *2003 Strategy*, the Federal government will take steps to greatly increase cooperation among law enforcement, financial regulators, and financial institutions.

In the past, despite various obstacles inhibiting communications between Federal law enforcement and the financial community, we achieved some success in fostering regular interaction—for instance, through the Bank Secrecy Act Advisory Group—as well as on an *ad hoc*, situation-specific basis, particularly post September 11, 2001. Now, however, Section 314 of the USA PATRIOT Act has provided a framework that significantly enhances the ability of the Federal government, including both regulators and law enforcement, to communicate directly with, and receive information from, financial institutions where terrorist financing or money laundering is reasonably suspected.

Under Section 314 (a), the Department of the Treasury has established a system in which FinCEN serves as an information conduit between Federal law enforcement agencies and financial institutions to facilitate the sharing and dissemination of information relating to suspected terrorists and money launderers.[18] The mechanism, which requires financial institutions to search recent records upon receiving a name from FinCEN, permits law enforcement to locate the accounts and transactions of suspects quickly and without compromising pending investigations. If matches are found, law enforcement will follow up with the financial institution directly. Since issuing the regulation implementing this provision, Treasury and FinCEN have worked closely with the financial and law enforcement communities to address the operational problems with the system and to assess the volume of requests. While considerable progress has been made, and the results of the searches have been successful, there is still room for additional progress to accommodate both the need to protect private customer information and law enforcement's need to obtain investigatory information as quickly as possible, while preserving the confidentiality of ongoing investigations. We will continually seek to improve balancing these factors as part of our *2003 Strategy*.

In addition, Section 362 of the PATRIOT Act required the Secretary of the Treasury to establish a network within FinCEN to allow financial institutions to file Bank Secrecy Act reports electronically through a secure network, and for FinCEN to provide financial institutions with alerts regarding suspicious activities that warrant immediate and enhanced scrutiny. To implement this provision, FinCEN has established the *PATRIOT Act Communications System* ("*PACS*"), which is now operational. E-filing will expedite reporting for financial institutions; reduce their costs of complying with filing BSA reports; and make information available to law enforcement faster.

Interagency SAR Review Teams also play a role in promoting cooperation and coordination between the financial community and law enforcement.[19] SAR Review Teams, located throughout the United States, will be encouraged to conduct regular meetings with compliance officers at financial institutions to provide

[17] Attached as Appendix J are the most recent figures from the Departments of Treasury and Justice for equitable sharing to foreign countries. Although the total amounts shared will vary from year to year, the significance of these sharing efforts cannot be understated.

[18] While the final rule establishing this mechanism will apply to all financial institutions, in the short term, as a practical matter, the ability to communicate quickly will likely be limited to traditional financial institutions, such as banks and securities brokers.

[19] FinCEN currently has public-private partnerships with the financial industry, which have been used to exchange information and provide appropriate guidance on BSA-related issues. The SAR Team-financial sector interaction will enhance these ongoing efforts.

the private sector with feedback and training on SARs. These meetings also will enable government and the private sector to discuss trends and developments in money laundering/terrorist financing activity.

G. Helping State and Local Governments Investigate and Prosecute Money Laundering and Financial Crime Cases

We are strongly committed to leveraging and enhancing the role of state and local governments, so that in the years ahead, they can play an increasingly important role in money laundering prevention, detection, and enforcement. As discussed above, state and local participation is already occurring on a routine basis in some of the most significant anti-money laundering investigations through OCDETFs, HIDTAs, HIFCAs, and individual agency task forces. We will continue to support state and local participation in these interagency Task Forces. We also will provide training and will continue to review and improve the means and methods by which non-Federal law enforcement agencies can access investigative information possessed by the Federal government. OCDETF has agreed to fund a series of 24 financial investigation training courses in locations around the United States over the next 2 years. DOJ is coordinating this OCDETF-funded financial training. In addition, federal law enforcement will continue to work with state and local law enforcement to ensure that we obtain as much information as possible from money couriers identified and stopped by state and local authorities, and that we aggressively pursue leads downstream and upstream in the money channels.

The investigation and development of money laundering cases can pose challenges to many local law enforcement agencies. The cases are often complex, labor intensive, and evolve over extended periods of time. Many local law enforcement agencies lack the budgetary resources to assign investigators to these cases and to build up a body of expertise in pursuing them. For these reasons, state and local participation in interagency law enforcement task forces is crucial to our success.

Access to financial information is essential as well. FinCEN's Gateway Program, discussed above, is an important tool for supporting the involvement of state and local law enforcement in anti-money laundering/terrorist financing efforts. Gateway not only provides state and local law enforcement with essential access to BSA data for use in their own money laundering investigations, it also incorporates an "alert" process, which notifies requesting agencies of other queries on the same subjects that have been received through Gateway. This alert system promotes more coordinated and vigorous pursuit of violators, and provides a mechanism that facilitates the "de-confliction" of investigative efforts that may overlap when multiple jurisdictions investigate the same targets.

In addition, during the past few years, the U.S. government has successfully used the Financial Crime-Free Communities (C-FIC) Support Program, a law enforcement-oriented grant program, to enable state and local governments to undertake innovative anti-money laundering initiatives. Between September 2000 and September 2003, C-FIC will have provided over $9 million in seed capital to 22 recipients. These funds have been used to institute state and local counter-money laundering enforcement efforts to detect and prevent money laundering and related financial crimes, whether related to narcotics or other underlying offenses. C-FIC grants helped state and local communities marshal information and expertise to build innovative approaches to money laundering control and enforcement,[20] and provided additional support to various HIFCA Task Forces.

As part of the closeout of the C-FIC program during 2003-2004, the Bureau of Justice Assistance will prepare a C-FIC Program Evaluation Report, which will examine how C-FIC grant resources were used by the grantees; evaluate the effectiveness of the grants and the C-FIC program and whether the C-FIC grants achieved their intended objectives; provide specific examples of benefits to the United States generated by the grant recipients; evaluate the overall impact of the C-FIC grant program; and make recommendations, if any, for how to conduct a similar grant program in the future, should the need arise. Short summaries of some of the more significant grants to date, and the results achieved thereby, are set forth in Appendix F.

[20] As one grant recipient, the San Diego Police Department, stated, "It is no exaggeration to say that C-FIC funds have provided the *only* opportunity for local law enforcement . . . to engage in an effective assault on money laundering. The cases are simply too lengthy and complex, and staff power too limited, to commit existing resources on a meaningful level." San Diego Police Department C-FIC Renewal Request, September 2002, pp. 25-26 (emphasis in the original.)

Goal 3

Ensure Effective Regulation

Introduction

The *2002 Strategy* affirmed our commitment to a robust anti-money laundering regulatory regime that plays an essential role in our overall money laundering strategy. Issued in the wake of the USA PATRIOT Act's landmark amendments to the Bank Secrecy Act, the *2002 Strategy* articulated a core focus on the aggressive implementation of these provisions and close cooperation between the public and private sectors to deny money launderers and terrorist financiers easy access to the financial sector. This remains a top priority. In this regard, the *2003 Strategy* is a continuation of last year's efforts.

This essential continuity does not mean, however, that we will be anything less than aggressively proactive, both in identifying new and emerging threats that can be addressed through regulation, and in evaluating the effectiveness of the regulations issued to date and seeking ways of improving them. Accordingly, this year's *Strategy* contains the following objectives for 2003:

- Strengthen and refine the anti-money laundering regulatory regime for all financial institutions.
- Improve the effectiveness of anti-money laundering controls through greater communication, guidance, and information sharing with the private sector.
- Enhance regulatory compliance and enforcement efforts.

A. Strengthen and Refine the Anti-Money Laundering Regulatory Regime for All Financial Institutions

The anti-money laundering provisions of Title III of the USA PATRIOT Act, together with the many regulations the Treasury Department has issued since November 2001 to implement the Act, aim to strengthen areas in which our financial services sector may be vulnerable to abuse. The legislation reflects strong Congressional resolve to expand and improve our anti-money laundering regulatory regime and protect our financial system from evolving money laundering/terrorist financing threats. Following passage of the Act, the Department of the Treasury, along with FinCEN, the Federal functional regulators, the Department of Homeland Security, and the Department of Justice, began the task of drafting regulations to implement the many revisions to the Bank Secrecy Act. This process continues today.

From the outset, we have committed ourselves to meeting the challenge of developing implementing regulations that simultaneously effectuate the purpose of the anti-money laundering provisions, respect and reasonably protect the business activities of financial institutions, and ensure that regulations do not unduly infringe upon the legitimate privacy interests of our citizens. Striking this balance remains essential to the success of our ongoing regulatory efforts.

In implementing the Act, we are guided not only by the express statutory language, but also by certain core principles that form the cornerstones of our anti-money laundering regulatory policy:

- Enhance the flow of critical financial information;
- Prevent regulatory arbitrage;
- Focus financial institution reporting require ments on information that is useful to law enforcement;

- Protect important privacy interests; and
- Protect the financial system.

Since passage of the Act, we have—

- Expanded our basic anti-money laundering program requirements to the major financial services sectors, including the securities industry, the futures industry, insurance companies, and unregistered investment companies, such as hedge funds;
- Issued regulations to permit and facilitate the sharing of critical information between law enforcement and financial institutions, as well as among financial institutions themselves;
- Issued a series of regulations aimed at minimizing risks presented by international correspondent banking;
- Issued regulations requiring financial institutions to implement customer identification and verification procedures; and
- Expanded the universe of financial institutions reporting suspicious activities to FinCEN.

Appendix G contains a summary of the anti-money laundering provisions of the USA PATRIOT Act that have been implemented.

In 2003 and beyond, we will do the following:

❖ ***Complete Regulations Implementing the Anti-Money Laundering Provisions of Title III of the USA PATRIOT Act***

Our top priority is to complete the formal rulemaking process implementing the provisions of the USA PATRIOT Act. Important tasks include issuing final regulations to ensure that the appropriate level of due diligence is applied to correspondent accounts maintained for foreign financial institutions, and issuing final regulations that expand the anti-money laundering regime to a variety of financial institutions.

❖ ***Review, on an Ongoing Basis, the Effectiveness of Anti-Money Laundering Regulations, Including those Implemented Pursuant to the USA PATRIOT Act***

The anti-money laundering provisions of the USA PATRIOT Act and the implementing regulations triggered profound changes in the financial services industry. But issuing final regulations is only the beginning of our work. We must now take a critical look at the regulations, assess how they are working in practice, and make adjustments, when necessary, to ensure that they continue to achieve our anti-money laundering and anti-terrorist financing goals, without imposing unnecessary burdens.

This review must be a continuing process because the financial services sector is dynamic and money laundering and terrorist financing risks changeable. Indeed, the volume of regulations called for under the USA PATRIOT Act and the compressed time frame in which they were to be issued, which Congress recognized was necessary and appropriate post September 11, 2001, require from the government an even greater, more formal commitment to evaluate our efforts.

In October 2002, then-Treasury Deputy Secretary Kenneth Dam created a new task force within the Department of the Treasury, the Treasury USA PATRIOT Act Task Force, to undertake this review and serve as the point of contact with the financial services industry, law enforcement, the regulators, and Congress on issues relating to anti-money laundering regulation. This year, the Task Force will provide a report that outlines the results of our initial review of regulations issued to date. The Task Force will continue, as it has since its formation, to meet with financial regulators, the regulated community, law enforcement, and consumers to gain their insights and recommendations as to how to improve the regulations that have been issued, in light of experience gained through implementation. The report will contain preliminary findings and, if necessary, recommended regulatory or statutory changes. This report and the Task Force's future work will focus on assessing the effectiveness of the regulations, as well as the cost and burden they impose on financial institutions.

Beyond that, the Task Force will devote itself to finding ways to improve the effectiveness of our anti-money

laundering regime. Through existing mechanisms, such as the Bank Secrecy Act Advisory Group, and new ones, such as the Task Force, the whole of the Federal government, with input and assistance from the private sector, must work together to optimize our anti-money laundering regime.

❖ ***Ensure Continued Cooperation Among the Financial Regulators***

Federal and state banking, securities, and futures regulators have been, and continue to be, on the front line of responding to evolving money laundering threats. At the Federal level, the financial regulators continue to be a vital component of successful implementation of the USA PATRIOT Act, contributing both expertise and resources to the process. The Department of the Treasury and FinCEN's USA PATRIOT Act implementation efforts centered on establishing several interagency working groups dedicated to the Act's various provisions. Federal regulators participate centrally in these working groups, reviewing legal and policy issues and drafting regulatory language. Once the regulatory language is in place, the regulators' work to ensure industry compliance begins. Already, the regulators have begun the process of developing examination procedures and industry guidance. Under the *2003 Strategy*, we will continue to work together to ensure uniform and consistent application of the regulations.

❖ ***Reduce Cyber Vulnerabilities***

Since the number of financial transactions conducted electronically is increasing exponentially, we must minimize the vulnerability of electronic payment methods to money laundering, terrorist financing, and other criminal activity. As called for by the *2002 Strategy*, the Departments of Justice and Treasury have recently issued a report examining the ability of terrorists to raise funds over the Internet. A copy of the report, outlining key issues that we will address going forward, is attached as Appendix H.

Law enforcement and regulatory officials must work closely with the private sector to reduce the vulnerability of cyber systems to electronic attack. Banks and other depository institutions are required by law and supervisory guidance to have policies and procedures to maintain the integrity of their data and systems. We will work with financial institutions to further protect their electronic systems from intrusions by alerting them to recent incidences of and trends in cyber crimes and continue our efforts in this area.[21]

❖ ***Work with International Partners and Through International Organizations to Encourage the Adoption of Similar Anti-Money Laundering Regulations Throughout the World***

In many important respects, anti-money laundering regulations issued pursuant to the USA PATRIOT Act raise the international regulatory bar. But if the rest of the world does not follow our lead, our goals will be undermined. Not only will tainted funds find other ways into the financial system, but the U.S. financial services industry may find itself at a competitive disadvantage if it insists on rigorous due diligence and anti-money laundering procedures where others do not. Goals One and Two discuss the international aspects of our anti-money laundering strategy, but it bears emphasizing that the Federal government must aggressively seek to encourage all jurisdictions to adopt similar controls.

B. Improve the Effectiveness of Anti-Money Laundering Controls Through Greater Communication, Guidance, and Information Sharing

The flow of information has proven to be one of the most important elements of an effective anti-money laundering regime. The *2003 Strategy* identifies several key information sharing priorities.

❖ ***Expand Partnership with the Financial Services Industry***

Since passage of the USA PATRIOT Act, we have maintained active consultations with the financial services industry, with the result that the private sector has come to play an invaluable role in our efforts to develop the Act's implementing anti-money laundering regulations. Not only have we been able to rely on established relationships with the banking, securities,

[21] *See* T. Glaessner, T. Kellermann, and V. McNevin, *Electronic Security: Risk Mitigation in Financial Transactions* (June 2002).

futures, and insurance industries, among others, but we have also forged new relationships with the many other types of financial institutions that are now or will soon be subject to anti-money laundering regulation and oversight.

To fully promote the role of the financial services industry in the regulatory process, we have moved beyond the traditional role contemplated by the Administrative Procedures Act, whereby industries affected by proposed regulations have the opportunity to submit formal comments. Although this aspect of the financial services industry's multifaceted involvement in the regulatory process remains important, we have increasingly emphasized communication between the affected industries and policy makers even before rules are issued in proposed form. With respect to the rules affecting correspondent banking relationships, for example, the banking and securities industry provided valuable input from the outset concerning business models and existing controls placed on such relationships.

Finally, we recognize that perhaps the most important role played by the financial services industry has been, and will continue to be, to provide accurate and constructive feedback on the application of regulations. We are committed to ensuring that the regulatory scheme meets our enforcement goals without imposing undue burden and expense. Our best sources of information on such issues are the institutions that have to operate under them.

- ***Improve the Quality and Timeliness of Regulatory Guidance and Feedback Provided to Regulated Entities***

Because so many new types of financial institutions are subject to anti-money laundering controls, and the financial services sector is dynamic by its very nature, new fact patterns constantly arise that were not contemplated when regulations were first issued. While industry is charged with ensuring that they are in full conformity with the law, we are committed to providing clear, timely guidance so that financial institutions will be in a position to meet their legal obligations. We will also focus on better informing regulated institutions how information required to be collected or reported is used, and what types of data law enforcement finds most useful.

Specifically, we will work to provide guidance through the continued review and analysis of Suspicious Activity Reports; feedback and guidance from the regulators on an industry-specific basis, especially for financial institutions newly subject to Bank Secrecy Act regulation; the Bank Secrecy Act Advisory Group; Operation Cornerstone; and other informal methods.

- ***Further Strengthen the Public/Private Exchange of Information***

A key goal of the USA PATRIOT Act is to enhance coordination and information flow between the Federal government and the private sector. This information exchange must flow both ways—from the financial institutions to the government, and from the government to financial institutions. To this end, we will continue to work to improve information exchange mechanisms, both formal and informal, and will work closely with financial institutions to inform them about changes in money laundering methods and threats.

- ***Improve the Process for Dialog with Interested Parties Regarding Privacy Issues***

Automated information systems and advanced information processing techniques have made privacy a significant national concern, and the growing importance of anti-money laundering regulation has heightened the need for fuller and more in-depth analysis of privacy issues. Systems used for analyzing and disseminating BSA and related information must ensure that the information is well protected. Similarly, law enforcement use of reported financial information in such systems must maintain the security of the data involved and respect the appropriate privacy interests of the nation's citizens.

We are committed to ensuring thoughtful government consideration of privacy issues, and will seek to develop a mechanism for effectively addressing and promoting meaningful dialog--both within the government, and between the government and concerned citizens--about them. We will consider how to achieve anti-money laundering goals in ways that are consistent with minimizing burdens and protecting individual privacy. To the extent feasible, the Federal government will continuously address and review these issues in light of new technological developments.

C. Enhance Regulatory Compliance and Enforcement Efforts

❖ *Further Strengthen the Civil Enforcement and Examination of Money Laundering Regulations*

Comprehensive examination and credible enforcement of BSA regulatory requirements form is an integral part of an effective anti-money laundering regime. These objectives have always been important and have been reflected in previous strategies; however, the USA PATRIOT Act has required us to place renewed emphasis on them. First, as a result of the Act, financial institutions are subject to additional and increasingly complex requirements that will require corresponding changes to examination modules and procedures. Second, we are now in the process of extending BSA regulation to a host of new categories of financial institutions not previously subject to the range of anti-money laundering controls. Accordingly, we will take all steps necessary to provide for the appropriate examination of these entities.

1. Civil Enforcement

Authority for the civil enforcement of the BSA currently resides with FinCEN.[22] Over the past year, FinCEN has applied a variety of available sanctions against financial institutions for violations of the BSA, including the assessment of a $20 million civil monetary penalty against Banco Popular de Puerto Rico in January 2003.[23]

Going forward, FinCEN will continue to build on this foundation and exercise its available BSA civil enforcement remedies, whether alone or in conjunction with its regulatory and enforcement partners, to ensure compliance. In particular, FinCEN will take steps to develop civil cases, where appropriate, that address non-compliance across the spectrum of financial institutions subject to the BSA. This will include the assessment of penalties and other appropriate remedies as the facts warrant, that will serve to remind the financial industry as a whole of the importance of maintaining effective BSA compliance programs. As part of this effort, the Federal government will seek greater cooperation among law enforcement, regulators, Treasury, and FinCEN to ensure consistency in pursuing and applying appropriate remedies to BSA non-compliance matters. Treasury and FinCEN will also meet with the financial regulators to develop proposals for improving the Federal government's ability to consistently enforce civil compliance with the BSA, and will review the issue of delegating enforcement authority to the other financial regulators to enhance BSA compliance.

---

[22] FinCEN has delegated BSA examination authority to various supervisory agencies. See 31 C.F.R. 103.56(b). Based on examinations conducted by these agencies, findings are sometimes referred to FinCEN for consideration of civil BSA penalties. Under Title 12, certain federal supervisory agencies (Office of the Comptroller of the Currency; Office of Thrift Supervision; Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; and National Credit Union Administration) also have remedies available, including the assessment of civil money penalties, for failure to comply with Title 12 suspicious activity reporting and BSA compliance program requirements.

[23] In 2002, FinCEN assessed two civil money penalties, issued 33 letters of warning, 27 cautionary letters, and closed 16 other less significant matters referred to it for review. In January 2003, Banco Popular de Puerto Rico entered into a deferred prosecution agreement with the U.S. Department of Justice for failing to file Suspicious Activity Reports (SARs), in violation of Title 31 USC 5318(g)(l) and 5322(a), and agreed to forfeit $21.6 million to the United States. Concurrently, FinCEN assessed a $20 million civil money penalty against Banco Popular de Puerto Rico for BSA violations.

On April 3, 2002, Sovereign Bank, Wyomissing, Pennsylvania entered into a Consent to the Assessment of Civil Money Penalty to pay $700,000, without admitting or denying FinCEN's determination that the institution failed to file timely approximately 2,000 CTRs. On August 23, 2002, Great Eastern Bank of Florida, Miami, Florida entered into a Consent to the Assessment of Civil Money Penalty to pay $100,000, without admitting or denying FinCEN's determination that the institution failed to file complete SARs in a timely manner for reportable transactions by at least 20 customers.

Also, in November 2002, the federal government prosecuted Broadway National Bank for its failure to maintain an adequate anti-money laundering program; failure to file SARs concerning approximately $123 million in suspicious bulk cash and structured cash deposits; and aiding and assisting customers to structure approximately $76 million in transactions to evade currency reporting requirements. Broadway National Bank pleaded guilty and was assessed a $4 million fine.

2. *Examination*

The banking regulators, the Securities and Exchange Commission, and the Commodity Futures Trading Commission have already begun the process of developing new examination procedures in light of the changes brought about by the PATRIOT Act. With the issuance of final regulations, the task of examination begins. As always, educating the regulated community about the new requirements is an integral part of successful implementation. This process has already begun, and will continue. The Department of the Treasury and FinCEN will assist the regulators, helping to ensure consistency in the interpretation of the regulations and making necessary adjustments to the regulatory text.

In addition, the Department of the Treasury and FinCEN are committed to meeting the major challenge of providing for appropriate examination of the broad and diverse range of financial institutions that are or will be newly subject to anti-money laundering regulation under the BSA, but have no existing federal anti-money laundering regulator. Anti-money laundering examination is not an exact science, and anti-money laundering compliance is not susceptible to formulaic implementation across industry sectors. Nevertheless, under the *2003 Strategy*, we pledge to do all possible to ensure that we maintain an effective and consistent examination regime to keep up with the expanding scope of our anti-money laundering regulations.

As a first step toward meeting this goal, we will work to ensure that the examiners of the industries newly subject to BSA regulation aggressively undertake to educate them about their new responsibilities, and assist in developing programs and procedures that target the money laundering risks. Education and outreach are important to ensure that parts of the financial services industry with less experience with comprehensive federal regulation are fully informed of their obligations and understand how to achieve full compliance with the law.

3. *Work with State Governments to Ensure that there is a Consistent and Comprehensive Anti-Money Laundering Regime in the United States*

State, and in some instances, tribal and municipal governments have and will continue to play an important role in our overall anti-money laundering strategy. This is especially true as we expand anti-money laundering regulation to categories of financial institutions that are predominantly regulated at the state level. All government, whether Federal, state, tribal or local, has an interest in ensuring that our financial sector is not subject to unnecessarily duplicative or inconsistent regulation. In a spirit of mutual respect, based on our system of federalism, we will work to actively engage these partners to ensure that inconsistencies are removed.

Among other things, under the *2003 Strategy*, we will work vigorously to improve the process for raising and discussing issues with non-Federal regulators. These regulators may potentially play important roles in ensuring the overall effectiveness of anti-money laundering regulation, and often possess much greater in-depth knowledge of particular financial institutions in their jurisdictions. The key is coordination. With respect to money transmitters, for example, communication between state and Federal regulators is essential, given the intersection of the two regulatory schemes. Moreover, we wish to ensure that the thoughts, views, and experience of non-Federal regulators are incorporated into the Federal regulatory regime.

4. *Strengthen Regulatory Oversight of ARS*

As noted in Goal 1, ARS, such as *hawala*, are vulnerable to money laundering. To date, law enforcement's experience has been that alternative remittance transmitters often maintain limited, if any, reviewable account and transaction records ledgers. This paucity of standardized record-keeping is complicated by the fact that the records may be impossible to decipher without the help of an insider, and that the notations memorializing specific transactions are often destroyed within a short period of time. In addition,

alternative remittance transmitters may serve customers without asking many questions about their true identity, the true ownership of the funds or other questions relevant to an effective anti-money laundering program, and there may be significant use of nominee account holders.

Such activities are not permitted for a money transmitter operating in the United States. Money transmitters and other ARS are subject to comprehensive record keeping requirements under the BSA. We intend to ensure that these institutions are meeting their reporting and record keeping requirements under the BSA, and will institute enforcement actions against those who do not comply with the regulations. To this end, we will continue our outreach efforts to educate the industry about the regulatory requirements. We will also continue to work closely with law enforcement to identify additional ways to better ensure compliance with existing laws and regulations.

List of Appendices

Appendix A

Recent Significant Cases in the War Against Terrorist Financing

Benevolence International Foundation: Enaam Arnaout, Executive Director of Benevolence International Foundation (BIF), an Illinois charity recognized as a tax deductible charitable organization, had a relationship with Usama bin Laden and his associates. Through BIF, Arnaout illicitly obtained funds for terrorist organizations using funds from both knowing and unsuspecting donors. Arnaout, a Syrian-born naturalized U.S. citizen, has been in federal custody since he was arrested April 30, 2002 on perjury charges. On October 9, 2002, he was charged in a multi-count indictment that included charges of providing material support knowing that such support would be used to engage in overseas violence. It was alleged that these moneys covertly supported al Qaida, the Chechen mujahideen, and armed violence in Bosnia. The indictment further alleged that BIF, which was not itself indicted but whose assets were frozen and subject to forfeiture, operated together with Arnaout and other individuals and entities, as a criminal enterprise that engaged in a pattern of racketeering activity, raised funds and provided other material support for the violent activities of terrorist organizations in various areas of the world. On February 10, 2003, Arnaout pled guilty to a racketeering conspiracy, admitting that donors of BIF were misled to believe that their donations would support peaceful causes when, in fact, their funds were expended to support violence overseas. Arnaout also admitted providing various items to support fighters in Chechnya and Bosnia-Herzegovina, including boots, tents, uniforms, and an ambulance. On August 18, 2003, Arnout was sentenced to over 11 years' imprisonment and ordered to pay over $315,000 restitution to the UN High Commission on Refugees.

Sami Omar Al-Hussayen & Help the Needy: The Department of Justice recently took concerted law enforcement actions in Idaho and Syracuse, NY in an investigation involving a Michigan-based charity known as the Islamic Assembly of North America (IANA). IANA's Internet web sites contain messages calculated to raise funds and recruit persons for anti-U.S. violence and jihad.

On February 12, 2003, a University of Idaho graduate student and Saudi citizen named Sami Al-Hussayen was indicted in Boise on seven counts of visa fraud and four false statement offenses. The charges are based in part on Al-Hussayen's failure to include his association with IANA on a student visa renewal form. Al-Hussayen has been a registered agent of IANA's since May 11, 2002, and is also listed as the administrative contact on a number of IANA-operated websites. Between January 1997 and December 2002, approximately $300,000 of unexplained (non-student aid) funds flowed through various bank accounts controlled by Al-Hussayen. Approximately one-third of the money transmitted to these accounts from overseas was ultimately remitted to IANA and other associates. According to the indictment, in June 2001 an IANA website posted an article entitled "Provisions of Suicide Operations," which suggested the use of aircraft as instruments of suicide attacks.

On February 18, 2003, in Syracuse, NY, four defendants and two organizations, including "Help The Needy," were charged with conspiring to transfer funds to Iraq in violation of International Emergency Economic Powers Act (IEEPA), as well as twelve counts of money laundering and one count of conspiracy to commit money laundering. Founded in 1993, Help the Needy describes its mission as a relief effort to Iraq. Among the defendants was its founder, Dr. Rafil Dhafir, listed as IANA's vice president. Dhafir, Osameh Al-Wahaidy, and Ayman Jarwan were arrested on February 25, 2003, and search warrants were executed at 11 different locations. On April 22, 2003, Al Wahaidy pled guilty to a felony charging him with an IEEPA violation. On April 25, 2003, Jarwan pled guilty to conspiring to violate IEEPA by sending money to Iraq, and conspiring to defraud the United States by impairing and impeding the calculation and collection of taxes.

Mohammed Ali Hasan Al-Moayad: On January 4, 2003, prosecutors in Brooklyn, NY, filed a criminal complaint charging Mohammed Al-Moayad with conspiring to provide material support and resources to Al Qaida and Hamas. On January 9, 2003, a criminal complaint was filed charging Al-Moayad's assistant, Mohammed Moshen Yahya Zayead, with the same charges. Al-Moayad is a prominent Yemeni cleric whose name appears as a reference on Al Qaida training camp documents. Al-Moayad solicited funds from persons in the United States, claiming that he had provided over $20 million to al Qaida and that he could guarantee that the remitted funds would be applied solely to jihad activities. On January 10, 2003, al Moayed and Zayed were arrested in Germany, where they had traveled to receive a large donation. On January 11, 2003, a German court found the U.S. charges sufficient and ordered them detained. In March 2003, in Frankfurt, Germany, a judge ruled that the U.S. had presented sufficient evidence to support extradition of Al-Moayad and Zayed. As of this writing, the extradition is pending.

United States v. Sami Al-Arian, et al: On February 19, 2003 in Tampa, FL, ProfessorSami Al-Arian and seven others were charged in a fifty-count indictment for using facilities in the United States, including the University of South Florida and affiliated non-profit research foundations, to serve as the North American base of Palestinian Islamic Jihad (PIJ), a designated terrorist organization since 1997. Eight years of intercepted wire conversations and faxes demonstrate the defendants' active involvement in the worldwide operations of PIJ. Charges filed included, among others, conspiracy to provide material support to terrorism.

James Ujaama: On August 28, 2002, in Seattle, WA, U.S. citizen and Muslim convert James Ujaama was indicted for conspiracy to provide material support or resources to terrorism, and using, carrying, possessing, and discharging firearms during a crime of violence. Ujaama attempted to set up a jihad training camp at a farm in Bly, Oregon, and operated websites for the former Imam of the Finsbury Park Mosque in London, England. On April 14, 2003, Ujaama pled guilty to conspiracy to violate IEEPA. He admitted to conspiring with others to provide support, including money, computer software, technology, and services, to the Taliban and to persons in the territory of Afghanistan controlled by the Taliban. He agreed to cooperate with the government's ongoing terrorism investigations. Pursuant to the plea agreement, Ujaama will be sentenced to 24 months in prison.

Portland Jihad Case: The charges arise out of an alleged attempt in late 2001 and early 2002 by six of the seven defendants (Jeffrey Leon Battle, Patrice Lumamba Ford, Ahmed Bilal, Muhmmad Bilal, Habis Abdulla al Saoub and Mike Hawash) to enter Afghanistan through China and Pakistan to aid and assist the Taliban against the United States and coalition forces stationed there. The seventh defendant, October Lewis, Battle's ex-wife, served as a conduit for money sent to him during his trip, including his later travel to Korea and then to Bangladesh to join Tablighi Jamatt, an evangelical Islamic group, as a way of entering Pakistan and ultimately Afghanistan. On October 3, 2002, all defendants, but one, were indicted on charges of conspiring to levy war against the U.S., conspiring to violate the IEEPA and provide material support and resources to terrorism, and possession of firearms in furtherance of crimes of violence. The last defendant was charged by criminal complaint on April 28, 2003 and ultimately added as a defendant by superseding indictment on May 2, 2003. Trial is scheduled for October 1, 2003. In a related matter, on March 3, 2003, Mohammed Kariye, the Iman of the Portland mosque, pled guilty to social security fraud.

North Carolina Hizballah Cell: This criminal investigation began when a North Carolina sheriff noticed a group of Lebanese men buying large volumes of cigarettes. An FBI Joint Terrorism Task Force investigation uncovered a cigarette smuggling enterprise involving two dozen people, some of whom had connections to Hizballah operatives in Lebanon. On March 28, 2001, the defendants were indicted on RICO charges, based on the cigarette smuggling, and tax evasion. Later, they were charged with conspiring to provide material support to Hizballah in violation of 18 U.S.C. § 2339B. The latter charges rested on funds sent to Hizballah, and a military procurement program in which operatives in Beirut tasked North America-based adherents to purchase and ship a variety of dual-use items purchased in the United States and Canada.

Primary defendants Mohamed Hammoud and Chawki Hammoud were tried and convicted in June 2002 in

the first 18 U.S.C. § 2339B jury trial in American history. On February 28, 2003, Mohammed Hammoud was sentenced to 155 years imprisonment (based on the terrorism sentencing enhancement) and his brother Chawki Hammoud received 51 months imprisonment and was ordered to report to Immigration and Naturalization Service (INS) for deportation proceedings immediately after serving his sentence.

Al Qaida Drugs-for-Weapons Plot: On September 17, 2002, Syed Mustajab Shah, Muhammed Abid Afridi and Ilyas Ali were charged with conspiring to import and distribute drugs and conspiring to provide material support to Al Qaida. Between April and September 2002, they allegedly negotiated with undercover law enforcement agents for the sale of 600 kilograms of heroin and five metric tons of hashish. The defendants also negotiated with undercover law enforcement agents for the purchase of four "Stinger" anti-aircraft missiles, which they indicated they were going to sell to members of Al Qaida in Afghanistan. Those negotiations took place in, among other places, San Diego and Hong Kong. The defendants were arrested in Hong Kong on September 20, 2002 by local law enforcement authorities, at the request of the United States government. On March 6, 2003, they were extradited thereafter arraigned in San Diego.

AUC Drugs-for-Weapons Plot: On November 1, 2002, federal prosecutors in Houston filed a criminal complaint charging Uwe Jensen and his boss, Carlos Ali Romero Varela, both of Houston as well as Cesar Lopez (A.K.A. "Commandant Napo"), and an individual identified as "Commandant Emilio," both high ranking members of Autodefensas Unidas de Colombia (AUC/United Self Defense Forces of Colombia), the Colombian right-wing designated terrorist organization, with drug conspiracy and conspiracy to provide material support or resources to AUC. The complaint provided the authority for Costa Rican law enforcement officials, in conjunction with the FBI and DEA, to arrest three of the defendants on November 5, 2002 in San Jose, Costa Rica. Jensen was arrested that same day in Houston. These arrests resulted from an undercover sting in a drugs-for-weapons deal that would have delivered $25 million worth of weaponry to AUC, in exchange for cash and cocaine. The weapons that the defendants believed they were purchasing included 9,000 assault rifles, including AK-47's, submachine guns, and sniper rifles; 300 pistols; rocket propelled grenade launchers; almost 300,000 grenades; shoulder fired anti-aircraft missiles; and approximately 60 million rounds of various types of ammunition. The grand jury returned an indictment on December 4, 2002. On April 23, 2003, Varela pled guilty to the § 2339B charge and the drug conspiracy charges. Jensen pled guilty on June 24, 2003. Emilio and Napo are both in Costa Rican custody awaiting extradition

INFOCOM/Marzook Illegal Export & Asset Concealment Case: In December 2002, the Attorney General announced the indictment of a closely-held computer company in Dallas known as INFOCOM and several of its officers. The indictment charges the defendants' alleged conduct of concealing a continuing profit interest held in the company by Mousa Abu Marzook, a senior Hamas leader who was listed as a Specially Designated Terrorist in a 1995 Executive Order issued pursuant to the IEEPA. Marzook and his wife, Nadia Elashi, who allegedly participated in the scheme, were also named as defendants. Under IEEPA and the related designation process, United States-based persons can be charged with the crime of failing to freeze the assets of specially designated terrorists.

Appendix B

Comprehensive List of Joint Designations of Individuals and Entities as Terrorists or Terrorist Supporters

U.S.-Saudi Joint Designations —On March 11, 2002, the United States participated in its first joint designation of a terrorist supporter. Acting with Saudi Arabia, we jointly designated the Somalia and Bosnia-Herzegovina offices of Al Haramain, a Saudi-based NGO linked to al Qaida, and jointly forwarded the names of these organizations to the UN Sanctions Committee for inclusion under the UNSCR 1333/1390 list. On September 9, 2002, the United States and Saudi Arabia jointly referred to the Sanctions Committee Wa'el Hamza Julaidan, an associate of Usama bin Laden and al Qaida supporter.

G7 Joint Designation – On April 19, 2002, the United States and the other G7 members jointly designated nine individuals and one organization. Most of these groups were European-based al Qaida organizers and terrorism financiers. Because of their al Qaida links, all ten names were forwarded to the UN Sanctions Committee for inclusion under the UNSCR 1333/1390 list.

U.S.-Italy Joint Designation – On August 29, 2002, the United States and Italy jointly designated 11 individuals linked to the Salafist Group for Call and Combat designated in the original U.S. Annex to E.O. 13224, and 14 entities that are part of the Nada/Nasreddin financial network run by two terrorist financiers designated on earlier E.O. 13224 lists.

U.S.-Central Asia Joint Designation – On September 6, 2002, the United States; Afghanistan; Kyrgyzstan; and China jointly referred to the UN Sanctions Committee the Eastern Turkistan Islamic Movement, an al Qaida-linked organization that operates in these and other countries in Central Asia.

Designation of Jemaa Islamiyya – On October 23, 2002, the United States designated the Southeast Asian terrorist group, Jemaa Islamiyya, responsible for the bombing of a nightclub in Bali on October 12, 2002 – the deadliest terrorist attack in the world since September 11, 2001. Subsequently, in the most widespread show of support of any terrorist designation to date, the United States joined Australia, Indonesia; Singapore; and 46 other countries, including all the members of ASEAN and the EU, in requesting the United Nations to also designate Jemaa Islamiyya for its ties to al Qaida.

Jemaa Islamiyya Leaders – On January 24, 2003 the US designated two key individuals, Mohamad Iqbal Abdurrahman (aka "abu Jibril") and Nurjaman Riduan Isamuddin (aka "Hambali"), related to the SE Asian group Jemaa Islamiyah. Australia joined the United States in requesting that both names be added to the UN list and Singapore joined in requesting the addition of one of the names (Hambali).

Three Chechen Groups – On February 28, 2003, the United States designated three Chechnya-based terrorists groups responsible for the Moscow theater siege. Thereafter, UN Security Council members France; Russia; China; the UK; Spain; and Germany joined the United States in asking the United Nations to also designate these groups for their ties to al Qaida.

Appendix C

Progress with Non-Cooperative Countries and Territories (NCCTs)

The 2002 NMLS included a comprehensive report on the status of each of the 23 countries that were placed on the FATF Non-Cooperative Countries (NCCT) list during 2000 and 2001. The 2002 NMLS also reported that, as of June 2002, a total of eight countries had been removed from the NCCT list and described their progress. The NCCT review process continues to stimulate efforts by many of the governments to improve their systems. This report reflects the significant developments of the remaining NCCT countries that have either been removed from the list since June 2002, have enacted significant legislative reforms to avoid countermeasures by the FATF, or have made further legislative changes to address deficiencies in their AML regime.

While a number of countries who remain on the NCCT list have developed their AML regime since June 2002, there are some jurisdictions in which substantial reforms have not yet been made and recognized by the FATF. No updates will therefore be included on Burma, and Indonesia.

Countries Removed From NCCT list

Russia

As a result of the implementation of significant reforms to its anti-money laundering system, Russia was removed from the NCCT list in October 2002. Since being placed on the NCCT list in June 2000, Russia has actively sought to address the deficiencies identified by the FATF. Since the effective date of its anti-money laundering legislation, Russia has made notable progress in implementing its anti-money laundering regime. The Russian FIU has accomplished much in a short period of time. Its leadership and staff are dedicated to implementing the requirements of the law. As a result of a positive FATF mutual evaluation report, the Russian Federation was admitted to full FATF membership in June, 2003.

Dominica

As a result of the implementation of significant reforms to its anti-money laundering system, Dominica was removed from the NCCT list in October 2002. Since being placed on the NCCT list in June 2000, Dominica has actively sought to address the deficiencies identified by the FATF. The government of Dominica has attempted to meet resource needs by allocating staff and funds to the appropriate bodies to implement the new anti-money laundering regime. There is a high level of awareness of the new anti-money laundering requirements throughout the financial sector, both on and offshore, and full engagement in the effective implementation of those requirements. The enhancement of Dominica's anti-money laundering regime and strengthening of its regulatory and supervisory oversight of the financial services sector has had a major impact on the offshore sector, which has diminished substantially.

Grenada

As a result of the implementation of significant reforms to its anti-money laundering system, Grenada was removed from the NCCT list in February 2003. Since being placed on the NCCT list in September 2001, Grenada has actively sought to address the deficiencies identified by the FATF. Substantial legislation has been enacted strengthening Grenada's anti-money laundering regime and establishing an effective supervisory and regulatory regime for the offshore sector, resulting in a drastic reduction in the number of offshore banks operating in the jurisdiction. Previous impediments to information exchange have been eliminated. International cooperation has improved substantially. Grenada's FIU has actively investigated several money laundering cases, with another case proceeding in court.

Marshall Islands

As a result of the implementation of significant reforms to its anti-money laundering system, the Marshall Islands was removed from the NCCT list in October 2002. Since being placed on the NCCT list in June 2000, the Marshall Islands has actively sought to address the deficiencies identified by the FATF. In June 2000, no such framework was in place and the Marshall Islands fully met many of the NCCT criteria. The anti-money laundering system in the Marshall Islands is in its infancy and is developing rapidly. While being a very tiny jurisdiction, the Marshall Islands authorities have established an effective bank examination program and a functioning financial intelligence unit that handles reports of suspicious transactions. In addition, there are no offshore banks that are licensed in the Marshall Islands. The offshore sector primarily consists of maritime-related Non Resident Companies (NRCs). The Marshall Islands authorities ensure that necessary information regarding legal and business entities is recorded, maintained and accessible to provide to relevant authorities. It was determined that these NRCs pose limited money laundering risks.

Niue

As a result of the implementation of significant reforms to its anti-money laundering system, Niue was removed from the NCCT list in October 2002. Since being placed on the NCCT list in June 2000, Niue has taken a number of drastic steps to reform its offshore sector. The International Banking Repeal Act, which was brought into force on June 5, 2002, brings to an end Niue's status as an offshore banking center. In practice, Niue no longer has a financial sector that is exposed to the threat of money laundering.

St. Vincent and the Grenadines

As a result of the implementation of significant reforms to its anti-money laundering system, St. Vincent and the Grenadines was removed from the NCCT list in June 2003. Since being placed on the NCCT list in June 2000, St. Vincent and the Grenadines has actively sought to address the deficiencies identified by the FATF. The government of St. Vincent and the Grenadines has enacted significant legislative reforms establishing an FIU, mandating suspicious transaction reporting, enabling exchange of information, facilitating international cooperation, and strengthening the supervisory and regulatory regime for its offshore sector. The size of the offshore sector has been significantly reduced as a result of implementation of the enhanced regime. The FIU is fully operational, active and has responded promptly and fully to numerous foreign requests for assistance.

Countries That Have Made Legal Reforms to Avoid Countermeasures

The Philippines

On September 29, 2001, the Philippines passed the Anti-Money Laundering Act of 2001. However, there were a number of key legal deficiencies with this law. The FATF therefore recommended the application of additional countermeasures as of March 15, 2003 if the Philippines failed to enact adequate legal reforms. On March 13, 2003, the FATF decided not to apply any countermeasures against the Philippines as a result of the enactment of the March 7, 2003 Republic Act No. 9194 which amends the Philippine Anti-Money Laundering Act of 2001. This new legislation addresses the main legal deficiencies in the Philippine anti-money laundering regime previously identified by the FATF. On the basis on this progress, the FATF has invited the Philippines to submit an implementation plan. However, the Philippines will still remain on the NCCT list until it has effectively implemented its new anti-money laundering legislation.

Ukraine

On December 7, 2002, Ukraine enacted the "Law of Ukraine on Prevention and Counteraction of the Legalization (Laundering) of the Proceeds from Crime." This legislation, however, contained serious deficiencies identified by the FATF. As a result of Ukraine's failure to enact anti-money laundering legislation meeting international standards, the FATF applied countermeasures against the Ukraine on December 20, 2002. On February 14, 2003, the FATF withdrew its recommendation for the imposition of countermeasures against Ukraine as a result of the enactment by Ukraine of several legislative amend-

ments addressing key deficiencies in the legislative framework. Ukraine will, however, remain on the NCCT list until it has effectively implemented its new anti-money laundering legislation.

Nigeria

After being placed on the NCCT list, Nigeria did not take action to address the deficiencies in its anti-money laundering regime and did not adequately engage with FATF. On October 31, 2002, the FATF therefore recommended the application of additional countermeasures if Nigeria failed to enact adequate legal reforms by December 15, 2002. The FATF decided not to apply additional countermeasures to Nigeria due to Nigeria's enactment of the "Money Laundering Act (Amendment) 2002" on December 14, 2002. This legislation significantly enhances the scope of Nigeria's 1995 anti-money laundering law. In December 2002, Nigeria also enacted the Economic and Financial Crimes Commission Act to establish a financial intelligence unit as well as competent investigative and enforcement authorities against money laundering. In May 2003, Nigeria enacted the Money Laundering Act 2003 to consolidate and improve previous anti-money laundering legislation. However, Nigeria must continue to strengthen and harmonize its legislative and regulatory framework and must begin operating its anti-money laundering regime. Nigeria will remain on the NCCT list as it works towards these goals.

Countries That Have Enacted Additional Legislation

Egypt

In 2003, Egypt continued to improve its anti-money laundering legislative and regulatory framework. On June 9, 2003, Egypt enacted Law No. 78-2003 to expand the scope of predicate offenses and to remove a pre-existing overbroad exemption from imprisonment for money laundering activity. In addition, on June 10, 2003, Egypt enacted Prime Minister Decree No. 951-2003 to detail requirements for financial institutions regarding suspicious activity reporting and customer identification procedures. The Decree also elaborated on the functions of the Egyptian financial intelligence unit (MCLU), the supervision of entities for compliance with anti-money laundering obligations, and international cooperation. Egypt is now working towards implementing its anti-money laundering regime.

Cook Islands

On May 7, 2003, nine new Acts were passed by the Cook Islands Parliament with the intention of creating an effective anti-money laundering framework, and introducing regulation and supervision of the financial sector consistent with international standards. The FATF is assessing this legislation, and had identified a number of issues requiring clarification. At its Plenary meeting in June 2003, the FATF acknowledged the substantial progress which the Cook Islands has made in addressing the concerns of the international community through the enacted of this legislative package. The FATF noted that the necessary regulations have yet to be enacted. The Cook Islands will remain of the NCCT list until it is demonstrated that this legislation have been fully implemented and has eliminated all shell banks.

Guatemala

In June 2002, Guatemala enacted a Banks and Financial Groups Law that will place offshore banks under the oversight of the Superintendency of Banks following a transition period and once authorization to operate is granted. The Superintendency of Banks has conducted on-site inspections of 13 offshore banks operating in Guatemala, 12 of which have applied for authorization to operate within a financial group. Additionally, on May 21, 2003, Guatemala's Monetary Board issued Resolution FM-68-2003 eliminating all coded accounts within three months. As a result of the significant progress made by Guatemala in addressing deficiencies identified by the FATF, Guatemala has been invited to submit an implementation plan to the FATF, representing a positive step forward in the process toward removal from the NCCT list.

Nauru

On March 27, 2003, Nauru's Parliament passed two pieces of legislation which are intended to address the concerns of the FATF. The Corporation (Amendment) Act of 2003 is intended to abolish the offshore banking sector which consists primarily of shell banks. The second act is intended to update and consolidate the

Anti-Money Laundering Act of 2001. At its Plenary meeting in June 2003, the FATF welcomed Nauru's recent legislative efforts to eliminate offshore shell banks. However, before the FATF can consider the removal of counter-measures, it believes that Nauru must take additional steps to ensure that the shell banks cease to operate and are no longer conducting any banking activity. Once Nauru establishes that it is cooperating fully with the international community, and has taken all available steps to ensure that the offshore banks that it had previously licensed are no longer operating, the FATF will consider the removal of counter-measures.

APPENDIX D

Trade-Based Money Laundering and Terrorist Financing

Trade-Based Value Transfer

Criminally-minded individuals and organizations have long misused international trade mechanisms to avoid taxes, tariffs, and customs duties. As both the formal international financial system and informal value transfer systems become increasingly regulated, scrutinized, and transparent, the risk of criminal money launderers and terrorist financiers attempting to use fraudulent trade-based practices in international commerce to launder, move, and use funds also increases.

Trade-based value transfer schemes use commerce in licit or illicit goods to transfer value. For example, under-invoicing a shipment of trade goods from country A to country B provides a simple and effective way to launder the proceeds of criminal activity. Over-invoicing a shipment of goods gives criminal organizations a paper rationale to send payment abroad and/or launder money. Thus, if a container of electronics is worth U.S. $ 50,000, but is over-invoiced for U.S. $ 100,000, the subsequent payment of U.S. $ 100,000 will cover both the legitimate cost of the merchandise (U.S. $ 50,000) and allow an extra U.S. $ 50,000 to be remitted or laundered abroad. The business transaction and documentation disguise the illicit transfer of $50,000, and wash the money clean. Informal Value Transfer Systems (IVTS) frequently make use of invoice manipulation as part of a scheme to transfer value between IVTS operators.[24]

There are a number of other types of invoice fraud and trade techniques. For instance, export incentives often encourage and disguise fraud. In this scheme, governments pay company cash incentives to export products, and the company uses the same export to launder money. In some countries, traders report to exchange control authorities that imports cost more, or exports less, than the actual value. The excess foreign exchange generated can be used to purchase additional foreign trade items. In some areas of the world, trade goods (including narcotics) are simply bartered for other commodities of value.

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

Trade-based money laundering can also be viewed as a component of other types of alternative remittance systems, such as *hawala*, the Black Market Peso Exchange,[25] and the use of precious metals, gems, and other commodities. Alternative remittance systems, sometimes referred to as IVTS, can be problematic because they use parallel banking, or underground banking and move money or transfer value without necessarily using the regulated financial industry. In all of these alternative systems, trade is most often the vehicle that provides "counter valuation" or a method of "balancing the books."

Trade-based value transfer is prevalent in many parts of the world that harbor terrorist groups and that are vulnerable to terrorist financing because of loose financial regulation and lax import/export laws and regulations. At present, it is difficult for law enforcement to interdict suspect transactions in this underworld of trade. At times, however, trade-based systems intersect with banks and other traditional financial institutions in order for the terrorist financiers or non-terrorist money launderers to obtain currency needed

[24] U.S. v. Shakeel Ahmad, 231 F.3d 805 (2000) (cert. denied Nov. 27, 2000.)

[25] The Black Market Peso Exchange is extensively discussed in Goal 1, see fn. 8.

to purchase goods for further fund transfer, or because the financial institutions serve as links in a clearing process that involves wire transfers.[26] Where trade-based money laundering/terrorist financing intersects with financial institutions, law enforcement may be able to identify the brokers or their representatives. Moreover, at that point, financial institutions may be able to review the trade-related financial transactions for indications of unusual activity, which may be reported to authorities in suspicious activity reports.

In this regard, it is important for law enforcement officials to assert a much more aggressive role in recognizing and investigating how trade can be used in money laundering and in the financing of terrorism. It is also essential that government authorities take active measures to make financial institutions aware of the ways IVTS operations may intersect with their institutions, so that they can better monitor and report on these activities.[27]

Recent money laundering cases involving International Emergency Economic Powers Act (IEEPA) violations demonstrate the use of commodities or goods to facilitate the transfer of value to OFAC-blocked countries.[28] In these cases, IVTS operators accept cash from expatriates in the U.S. and, using informal alternative remittance system mechanisms, transfer the funds abroad where the money is used to purchase miscellaneous goods, (medicine, food, etc.) for family members and friends located in the OFAC-blocked country. In many of these cases, funds are transferred through third parties outside the OFAC-blocked country, who further transfer the funds/value to the OFAC-blocked country, in the form of local currency or goods.

Trade Diversion Schemes

Trade diversion schemes create hard-to-detect value transfers that not only launder dirty money, but also themselves provide quick illegal profits. For example, a foreign front company may purchase legal goods from a legitimate U.S. company at a significant discount (up to 50%);[29] pay through a letter of credit, send the goods via an intermediary in a third country, and divert (i.e. return) the goods back to the United States, where they are sold to wholesalers at a higher price, but at an amount that still represents a discount (e.g., 20%) for the new buyer. The seller in this latter transaction (e.g., an intermediary front company associated with a criminal operation) then receives the proceeds of a legal sale. If a front company purchases $1 million worth of goods at a $500,000 discount and re-sells them for $800,000 a few weeks later through a trade diversion scheme, the mechanism can generate a $300,000 profit in apparently clean funds that anyone can use.

Gold, Gems, Diamonds, and Trade

Trade in gold, diamonds, and other precious metals and gems have long been associated with money laundering. Terrorist organizations around the world have also used gold and the trade of precious commodities to launder money or transfer value. Since our success in establishing international anti-money laundering/counter-terrorist financing standards is bringing about an increase worldwide in financial transparency, the underworld of gold and other precious metals and gems may increasingly be used as an alternative method of laundering illicit proceeds or moving terrorist-related funds.

---

[26] A recent Congressionally- mandated study conducted by Treasury/FinCEN on ARS revealed that some domestic-based ARS operators maintain bank accounts for various purposes, including managing ancillary businesses; conducting aggregate wire transfers; and acquiring monetary instruments for bulk shipment overseas to settle payments with counterpart ARS operators. The study cites an example in which a domestic-based ARS operator wired money to an overseas account, after which the funds were withdrawn to purchase commodities that were shipped to another overseas location, where they were sold. Proceeds from those sales were put into a bank account maintained by an overseas ARS operator, and used to pay the ultimate beneficiaries.

[27] See FinCEN Advisory on Informal Value Transfer Systems, Issue 33, March 2003.

[28] U.S. v. Hussein Alshafei, et al.

[29] A U.S. company may be willing to sell goods to a foreign company at a discount in order to open up a particular market for the U.S. company overseas. The foreign company purchasing the discounted goods may, unknown to the U.S. company, be a front for a criminal operation seeking to launder funds, as well as to gain a profit through a trade diversion scheme.

There are many reasons that gold is popular with money launderers. It has been a universal repository of wealth since antiquity; is a readily acceptable medium of exchange around the world; enjoys relatively constant value; offers easy anonymity; is portable; its form can be readily altered; trade in gold is easily manipulated; cultural reasons ensure a constant demand for gold; and, depending on the form of the gold, it can act as either a commodity or a *de facto* bearer instrument. Gold is used in all stages of money laundering—placement, layering, and integration. It is an alternative remittance system by itself, and is also an integral part of other alternative remittance systems, such as *hawala* and the black market peso exchange Although almost any trade item can be used to launder money,[30] gold is particularly attractive to money launderers because it has less bulk than many other commodities, and a relatively constant high dollar value.

Because of gold's unique properties, it is also a well established vehicle to help finance terrorist operations. For example, the right-wing Posse Comitatus in the United States, the Aum Shinri Kyo cult in Japan, and Colombian narco-traffickers have all used gold.

Gold is also emerging as a base for Internet digital currency transactions. One Internet business is using gold-backed currency, making it the world's first hundred percent precious metal-backed Internet (digital) currency businesses.

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

The extra-legal trade of diamonds in Africa often involves money laundering for criminal and political purposes, and provides a means to purchase arms and influence the political arena. "Blood diamonds" is the term used to describe the diamond trade that has helped finance African civil wars in Angola, Sierra Leone, Liberia, and other countries.

There have been press and other media reports[31] that the diamond trade is also being used for terrorist financing operations. The diamond trade in Africa is susceptible to terrorist financing exploitation through cross-border trade that uses established diamond trade routes, secondary level traders and agents, and suspect buyers. Diamond traders in Africa are often non-African. Operating from secured compounds, expatriate buyers, including those with terrorist links, often purchase rough diamonds via local currency. (Although purchases occur in local currency, the diamond trade utilizes U.S. dollars at all levels of commerce including the payment to buyers). Subsequent exports by the diamond buyers to the major diamond trading centers are often under-valued. Diamonds are also used to provide counter valuation in *hawala* transactions. Many of the diamond buyers involved with illicit diamond dealing in West and Central Africa pay protection money to groups identified as terrorist organizations.

[30] Many other commodities with universal value (e.g., medical equipment; alcohol; tobacco; construction material; etc.) are just as vulnerable to being used for money laundering and value transfer. Terrorist financiers, for example, can raise funds to support terrorism by exporting any kind of commodity or good that has value and use in the receiving country. Such transactions can be ad hoc, as opposed to repeated and regular, and mixed in with other trade transactions, making the activity even harder to detect.

[31] Associated Press, *Group That Tracks Financing of Terrorists to Double in Size,* LA Times, Jan.10, 2003 at A20.

Appendix E

Recent Significant Money Laundering Cases

"Operation Capstone": This BICE case focused on major money laundering mechanisms and systems that were responsible for the international movement of over $80 million by Colombian narcotics traffickers. The investigation demonstrated that the traffickers used, among other things, international life insurance policies, financial professionals, and international markets. Operated out of Miami, this complex investigation involved law enforcement cooperation among United States, Colombia, the United Kingdom, the Isle of Man, and Panama. To date, Capstone has resulted in seizures of approximately $9.5 million in the UNITED STATES, as well as $20 million worth of insurance policies in Colombia, and $1.2 million in Panamanian bank accounts.

"Operation Wire Cutter": In this case, BICE, in conjunction with DEA and Colombia's Departamento Administrativo de Seguridad, completed a 2 Ω year undercover investigation of Colombian peso brokers and their money laundering organizations. The investigation culminated in the January 2002 arrest of 37 individuals, accused of laundering millions of dollars for several cartels. Investigators seized over $8 million in cash, 400 kilos of cocaine, 100 kilos of marijuana, 6.5 kilos of heroin, nine firearms, and six vehicles. The arrests were made possible by undercover BICE agents working with Colombian peso brokers who directed them to illicit funds nationwide that were wired back to Colombia, often in the name of Colombian companies and banks, and subsequently withdrawn as pesos. Operation Wire Cutter an important example of the cooperation between UNITED STATES and Colombian law enforcement.

Broadway National Bank: In November 2002, Broadway National Bank — which has three branches in New York City — pled guilty to failing to report $123 million in suspicious deposits, failing to maintain an anti-money-laundering program and allowing criminal groups to structure their deposits so they wouldn't have to report $76 million in cash to the federal government. From 1996 to 1998, prosecutors said, Broadway was a bank of choice for several major drug gangs and money laundering syndicates, which placed and moved $123 million through more than 100 accounts. The bank was ordered to pay a $4 million fine. The bank has been under close supervision by the Office of the Comptroller of the Currency since 1998.

Bank officer investigation: In June 2002, the U.S. Attorney for the District of New Jersey and BICE announced charges against Maria Carolina Nolasco, a banker from Jersey City, N.J., and Turist-Cambio Viagens e Turismo, Ltda, a Brazilian currency exchange business, in connection with a money laundering scheme that moved more than half a billion dollars in eight months through various bank accounts and an illegal money transmitting business.
Nolasco, an assistant vice president for international banking at the Valley National Bank branch in New York City, was charged in an eight-count criminal complaint with money laundering, illegally "structuring" cash deposits, operating a money transmitting business without a license, and tax evasion. BICE agents, with substantial support from DEA and IRS-CI, also served warrants on 39 bank accounts at Valley National Bank resulting in the seizure of approximately $15.8 million. Valley National Bank was not charged with any wrongdoing and has cooperated fully with the government's case.

Lehman Brothers Account Representative: An indictment unsealed in June 2002 charged Consuelo Marquez, a former Lehman Brothers account representative, with facilitating the laundering of millions in drug money belonging to Villanueva Madrid, the mid-1990s Governor of the Mexican State of Quintana Roo. Madrid and his son, Luis Ernesto Villanueva Tenorio, were also charged in the conspiracy.

Madrid is alleged to have received payments, totaling an estimated $30 million, from Mexico's Southeast Cartel for shipments of cocaine that went through Quintana Roo en route to the United States in ex-

change for protection and transport of the shipments, which included the use of state owned facilities. Since 1995, Madrid and Tenorio allegedly deposited large amounts of narcotics proceeds into foreign and U.S. bank and brokerage accounts. They then enlisted Marquez to conceal ownership and avoid detection of the funds. Marquez utilized her positions at Serfin Securities (a Mexican investment firm with offices in New York) and later with Lehman Brothers to establish offshore corporations structured to conceal the proceeds and their ownership. The seizure and forfeiture of the accounts, estimated at approximately $45 million, are being sought.

After becoming a fugitive in 1999, days before his term as Governor and its immunity from prosecution under the Mexican constitution was to expire, Madrid was finally arrested in May 2001. The case was the result of a joint investigation between the U.S. Department of Justice (United States Attorney's Office for the Southern District of New York) and the Mexican Attorney General's Office, and involved the coordinated efforts of Drug Enforcement Administration agents in New York, Phoenix and Mexico.

Operation Southern Approach: In December 2002, following arrests in Miami, New York, Texas and Colombia, seven money laundering indictments were unsealed in the District of New Jersey following an international money laundering investigation. The indictments - the result of an investigation by the FBI, IRS and U.S. Attorney's Office - charge 26 individuals with conspiracy to launder drug proceeds and/or money laundering. Of the 26 defendants charged, 11 individuals were arrested in the United States and four were arrested in Colombia.

The indictments describe a hierarchy of individuals involved in conspiracies to direct the movement of drug money in the United States as well as conceal the nature, source, and ownership of the money. Defendants gathered cash from the sale of drugs, directed the movement of cash, acted as money couriers, or controlled bank accounts through which the drug money was moved. After the money arrived in New Jersey, it is alleged that some of the cash was retrieved by couriers and moved to other locations, including Florida. Other monies were deposited into bank accounts and then transferred to accounts controlled by members of the money laundering conspiracies. One indictment charged Salomon Camacho Mora, the leader of a Colombian cocaine-exporting organization, and eight others, with laundering approximately $1.6 million through this scheme.

The indictments were the culmination of a five-year OCDETF undercover operation. The FBI and IRS were assisted by DEA as well as by agents in the Special Support Unit of the Departamento Administrativo de Seguridad (DAS) in Colombia. The U. S. plans to seek extradition of the South American based defendants pursuant to the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.

Banco Popular de Puerto Rico: On January 16, 2003, the United States and Banco Popular de Puerto Rico (BPPR) entered an agreement wherein the United States agreed to defer prosecution of BPPR on charges the that bank failed to file Suspicious Activity Reports (SARs) and currency transaction reports in a timely and complete manner in violation of Title 31, USC, Sections 5318(g)(1), 5322(b), 5324(a)(2) and 5324(d)(2). The bank agreed to forfeit $21.6 million involved in the unreported transactions.

The charges arose out of a BICE investigation conducted between June 1995 and June 2000. During this time, more than $33 million was laundered through the bank in suspicious cash transactions conducted by two of its customers and millions more in suspicious transactions were moved through the accounts of eleven money service businesses located in the Dominican Republic that were customers of the bank. Regular deposits of cash, totaling as much as $500,000 in a single day and totaling over $32 million in a three year period, were deposited and immediately wire transferred out. BPPR failed to properly monitor and investigate these accounts, thereby allowing millions of dollars of illegal drug proceeds to move through the bank without being detected and reported to law enforcement. When SARs were filed by BPPR, they failed to accurately report periods and amounts of suspicious activity.

Money Laundering Through Jewelers: In June 2003, U.S. Attorney's Office for the Southern District of New York announced the unsealing of criminal complaints

charging 11 individuals at seven different retail or wholesale jewelers in New York City with money laundering by accepting cash in exchange for gold items they believed were being smuggled to Colombia.

As part of the undercover operation, undercover law enforcement agents, more than $1 million in cash was delivered to different wholesale and retail jewelry businesses which had been identified as having participated previously in this laundering method. When delivering these funds, undercover agents or cooperating witnesses represented that the cash was the proceeds of narcotics trafficking. In return for the cash, undercover agents received more than 100 kilograms of gold, which they told the defendants would be smuggled to South America.

The charges were the result of an investigation conducted by the El Dorado Task Force, which specializes in investigating money laundering violations, and comprises agents of BICE, and IRS-CI, as well as members of the New York City Police Department and other state and local law enforcement agencies. The investigation was conducted in cooperation with the Organized Crime Drug Enforcement Task Force ("OCDETF") program in New York.

Appendix F

Financial Crime-Free Communities (C-FIC) Support Program Grants

Significant C-FIC Grants

Attorney General, State of Arizona-Money Transmitter Project
Total Funding $599,519

This project was designed to support investigations and prosecutions targeting the use of money transmitters by money launderers and other financial criminals. The primary approach is to examine financial records then follow up through six interrelated initiatives: (1) removal and exclusion of money transmitters engaging in illicit transactions from legitimate commerce; (2) prosecution of pick-up operators (those who use multiple fake ID to deal directly with money transmitters on behalf of those who need to move illicit funds); (3) seizure of funds in transit; (4) leveraging the effects of related investigations; (5) coordination with related investigations outside the region; and (6) training and education of industry personnel. The project coordinates its activities with the South West Border Region HIFCA. Importantly, as a result of activities undertaken through this project, the legislature of Arizona has adopted a new money transmitter regulator statute based on recommendations made by the Attorney General of Arizona.

Attorney General, State of Texas — Bulk Currency Project
Total Funding $514,071

This project's proposal involved the problem of bulk currency smuggling across the United States/Mexico border. This effort specifically targeted, for the first time, the vehicular movement of bulk currency across the Southwest Border. This effort reflected bulk currency movement concerns articulated in the National Money Laundering Strategy for 2000 and subsequent Strategies. The Texas Attorney General's Office reports that, under this initiative, it has opened some 40 cases, and obtained 25 indictments.

State Police, State of Illinois—HIFCA SAR Review
Total Funding $491,022

The State Police's original application under C-FIC placed the emphasis on financial analysis, especially targeting through SAR review and analysis. As a result of this grant, the Illinois State Police also is able to perform financial analysis for the Chicago HIFCA. As a result of the analysis effort funded by this grant, multiple seizures have occurred including one totaling $624,691 generated through a single arrest. The project now has become the repository for financial intelligence data that is available to all members of the Chicago HIFCA- related agencies. To date, the intelligence gathered through this project has resulted in more than 23 instances where the financial intelligence gathered was used in opening and advancing cases.

APPENDIX G

Summary of the Anti-Money Laundering Provisions of the USA PATRIOT Act and the Steps Taken to Implement Them

Section	Description	Status
§ 311	Provides the Secretary of the Treasury with authority to require U.S. financial institutions to apply graduated, proportionate counter measures against a foreign jurisdiction, a foreign financial institution, a type of international transaction or a type of account that the Secretary finds to be a "primary money laundering concern."	• Designated Ukraine and Nauru on December 26, 2002. • Proposed rule that would impose countermeasures against Nauru and a notice revoking designation for Ukraine issued on April 17, 2003.
§ 312	Requires U.S. financial institutions that establish, maintain, administer, or manage a "private banking account" or a correspondent account for a non-U.S. person (including a foreign bank) to apply due diligence, and in some cases enhanced due diligence, procedures and controls to detect and report instances of money laundering through those accounts.	• Proposed rule issued May 30, 2002. • Interim rule issued July 23, 2002.
§ 313	Prohibits U.S. banks and securities brokers and dealers from maintaining correspondent accounts for foreign shell banks, that is, unregulated banks with no physical presence in any jurisdiction. Also requires financial institutions to take reasonable steps to ensure that foreign banks with correspondent accounts do not themselves permit access to such accounts by foreign shell banks.	• Interim guidance issued November 27, 2001. • Proposed rule issued December 27, 2001. • Final rule issued September 18, 2002.
§ 314	Encourages cooperation and the sharing of information relating to money laundering and terrorism among law enforcement authorities, regulatory authorities, and financial institutions. (314 (a)) Upon notice to the Secretary of the Treasury, permits the sharing among financial institutions of information relating to individuals, entities, organizations, and countries suspected of possible terrorist or money laundering activities. (314 (b))	• Proposed rule issued March 4, 2002. • Final rule issued September 18, 2002.

Section	Description	Status
§ 319(b)	Authorizes the Secretary of the Treasury or the Attorney General to issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States requesting records relating to that correspondent account. Requires U.S. financial institutions that maintain a correspondent account for a foreign bank to keep records identifying (1) the owners of the foreign bank; and (2) the name and address of a person in the United States who is authorized to accept service of legal process for records related to the correspondent account.	• Interim guidance issued November 27, 2001. • Proposed rule issued December 27, 2001. • Final rule issued September 18, 2002.
§ 324	Requires the Secretary of the Treasury, in consultation with the Attorney General and the federal functional regulators, to evaluate the operations of Title III and submit recommendations for legislative amendments that may be necessary.	• Due in April of 2004.
§ 325	Authorizes the Secretary of the Treasury to issue regulations governing the use of concentration accounts.	• Reviewing existing controls on such accounts and considering options for regulatory action.
§ 326	Requires the Secretary of the Treasury, jointly with the federal functional regulators, to issue regulations prescribing minimum standards for financial institutions to identify and verify the identity of their customers who open accounts.	• Proposed rules issued July 16, 2002 for banks, savings associations, and credit unions; securities broker-dealers; mutual funds; and futures commission merchants and introducing brokers. • Final rules issued May 9, 2003.
§ 326(b)	Requires the Secretary of the Treasury to submit a report to Congress on ways to improve the ability of financial institutions to identify foreign nationals.	• Report issued in October 2002.
§ 328	Requires the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to take reasonable steps to encourage foreign governments to include originator information in wire transfer instructions.	• Proposed and successfully secured the adoption of a special recommendation of the Financial Action Task Force that originator information be included in wire transfer instructions.

Section	Description	Status
§ 352	Requires all financial institutions to establish anti-money laundering programs.	• Interim final rules applicable to banks, savings associations, and credit unions; securities broker-dealers; futures commission merchants and introducing brokers; casinos; money services businesses; mutual funds; and operators of a credit card system issued April 24, 2002. • Proposed rules (or advance proposed rules) issued for insurance companies; unregistered investment companies; investment advisers; commodity trading advisors; dealers in precious metals, stones or jewels; travel agents; vehicle sellers; and persons involved in real estate closings and settlements. • Statutory compliance deadline for financial institutions extended pending issuance of an applicable final or interim final rule.
§ 356(a)	Directs the Secretary of the Treasury, in consultation with the Securities and Exchange Commission and the Board of Governors of the Federal Reserve, to prescribe regulations requiring securities broker-dealers to file suspicious activity reports to the extent considered necessary and expedient.	• Proposed rule issued December 31, 2001. • Final Rule issued on July 1, 2002.
§ 356(b)	Authorizes the Secretary, in consultation with the Commodity Futures Trading Commission, to prescribe regulations requiring futures commission merchants, commodity trading advisors, and commodity pool operators to file suspicious activity reports.	• Proposed rule requiring futures commission merchants to file suspicious activity reports and to comply with BSA recordkeeping requirements issued May 5, 2003.
§ 356(c)	Requires the Secretary of the Treasury, the Board of Governors of the Federal Reserve, and the Securities and Exchange Commission to submit jointly a report to Congress recommending ways to apply Bank Secrecy Act requirements to investment companies.	• Report issued on December 31, 2002.

Section	Description	Status
§ 357	Requires the Secretary of the Treasury to submit a report to Congress on the role of the Internal Revenue Service in the administration of the Bank Secrecy Act.	• Report issued on April 26, 2002.
§ 359	Requires the Secretary of the Treasury to submit a report on the need for additional legislation relating to ARS.	• Report issued in November 2002.
§ 361	Requires, to the extent considered necessary and expedient, the Secretary of the Treasury to submit a report on improving compliance with the reporting requirements of section 5314 of title 31, United States Code (FBAR reporting requirements).	• Report issued on April 26, 2002.
§ 362	Requires the Secretary of the Treasury to establish a highly secure network within FinCEN for filing of BSA reports.	• System operational.
§ 365	Requires non-financial trades or businesses to file currency transaction reports with FinCEN.	• Interim final rule issued December 31, 2001.
§ 366	Requires, to the extent considered necessary and expedient, the Secretary of the Treasury to report to Congress on whether to expand the existing exemptions to the requirement that financial institutions file currency transaction reports and on methods for improving financial institution utilization of exemptions.	• Report issued on October 25, 2002.

APPENDIX H

Terrorist Financing Online

I. INTRODUCTION

For more than 2,000 years, military strategists have recognized the truism that armed conflict cannot be waged until it has been financed.[32] Accordingly, shortly after the September 11, 2001 terrorist attacks on the United States, President Bush observed that the country's first strike in the war against terrorism would target terrorists' financial support.[33] As former Secretary of the Treasury Paul O'Neill stated in October 2001, "our goal must be nothing less than the disruption and elimination of the financial frameworks that support terrorism and its abhorrent acts."[34]

Since September 11, 2001, the United States has made remarkable strides in disrupting and interdicting the flow of financial resources to terrorists. The United States has twice amended its laws to provide, consistent with the rights and privacy of its citizens, additional tools for preventing, investigating, and prosecuting terrorist financing.[35] We have engaged in capacity-building around the globe, encouraging other countries to establish appropriate money-laundering legislation and effective oversight of their banking and financial systems. We have led initiatives in multilateral fora to develop and implement legal and regulatory controls on alternative means of value transfer, such as *hawala*. We have also coordinated with the private sector and the international community to develop best practices to protect charitable organizations from exploitation by terrorists to raise funds.

In cooperation with other countries and with international bodies, the United States has frozen funds and assets worth more than $136 million. Furthermore, the Secretary of the Treasury has frozen the assets of, and prohibited financial transactions with, 315 individuals and organizations by identifying them as specially designated global terrorists under the International Emergency Economic Powers Act ("IEEPA").[36] Countries around the globe are following our lead – as of August 1, 2002, more than 160 foreign countries had instituted blocking orders affecting accounts worth more than $70 million.[37] There is no telling how many more donations, how many more financial transfers to the operational arms of terrorist organizations, and how many more acts of funded terrorism we have prevented with our amended laws, diplomatic efforts, and increased financial and banking controls.

Indeed, one government official recently observed, "[t]errorists can no longer safely use the international banking system. . . . As formal financial systems are purged of terrorist finance, terrorists naturally are inclined to resort to other, more costly and uncertain, but still serviceable mechanisms for moving resources."[38] Although this observation may be overly optimistic in one respect – terrorists and terrorist organizations still use the international banking system – it correctly emphasizes that as the banking system comes under increasing scrutiny, terrorists may

[32] *See* SUN TZU, THE ART OF WAR 72-73 (Samuel B. Griffith trans., Oxford University Press 1963).

[33] Comments of President George W. Bush, Delivered at the Department of Treasury, November 7, 2001.

[34] Remarks of Secretary of the Treasury Paul O'Neill before the Extraordinary Meeting of the Financial Action Task Force, Oct. 29, 2001, available at http://www.treas.gov/press/releases/po735.htm.

[35] *See generally* USA PATRIOT Act, Pub. L. 107-56 (2001) and Homeland Security Act of 2002, Pub.L. 107-296 (2002).

[36] *See* 50 U.S.C. §§ 1701-1706.

[37] Prepared Statement of Kenneth W. Dam, Deputy Secretary of the Treasury, before the Senate Committee on Banking, Housing, & Urban Affairs' Subcommittee on International Trade & Finance (Aug. 1, 2002).

[38] "The Financial War on Terrorism," Testimony of Undersecretary of State Alan Larson before the Senate Committee on Finance, October 9, 2002.

turn as well to other mechanisms to transfer funds. While maintaining our vigilance over traditional means of value transfer, therefore, we must also focus on alternative means – trading in commodities such as gold, gems, and precious stones and metals; non-bank online remittance systems; and informal value transfer systems such as *hawala*.[39]

This Report addresses the Internet, a technological infrastructure that suffuses both traditional and alternative means of resource and money transfer. The Internet has, in the last ten years, revolutionized global commerce and communications. Its potential benefits – in education, in commerce, in communication, and in spreading the message of freedom and democracy – are almost limitless. But the Internet is a value-neutral scientific advance. With the exception of its inherent openness, nothing fundamental to the Internet's architecture favors education over indoctrination, legitimate commerce over fraud and money laundering, or democratic, egalitarian ideals over extremism and intolerance. The anonymous, largely unregulated, and geographically unbounded nature of the Internet has thus created not only unprecedented opportunities for legitimate commerce; it has created unprecedented opportunities for fraud, money laundering, and the provision of material support to terrorists and terrorist organizations as well.

A. Mission Statement

In the 2002 National Money Laundering Strategy,[40] the Department of the Treasury and the Department of Justice committed to study, in coordination with the intelligence community, how the Internet is used to raise and move funds to terrorist groups. In furtherance of this task, the Department of the Treasury and the Department of Justice have convened a working group (the "Working Group") of experts on Internet crime, money laundering, and terrorism. The Working Group includes representatives of the regulatory community, the law enforcement community, and the intelligence community.[41] This Report is a compilation of these individuals' experience and expertise. It addresses both the manners in which the regulatory, law enforcement, and intelligence communities have observed terrorist organizations using the Internet to raise and transfer funds in the past and some of the manners in which such organizations will likely use the Internet for such purposes in the future.

A comprehensive discussion of how terrorists may use the Internet to collect and transfer resources is an enormous and, to the best of the Working Group's knowledge, heretofore unattempted undertaking. It is appropriate at the outset, therefore, briefly to address the breadth and scope of this project and the limiting definitions that guide the Working Group's work.

1. The Internet

The Internet was conceived in 1961 and delivered into existence in a primordial stage of development by a consortium of government scientists and academics in 1969. During the 1970s, the Internet developed as an open-architecture network that would accommodate diverse network interfaces and architectures and as a decentralized, redundant network to ensure reliability if any of its "nodes" malfunctioned. Applications such as electronic mail and file transfer were invented and a common language, or set of protocols, was agreed upon. In the 1980s, government encouraged the development of private networks and commercial applications. A tripartite symbiotic interaction among government, academia, and private industry accelerated the growth rate and application diversity of the

[39] For ease of reference, this Report adopts the colloquial shorthand of referring to the trust-based informal value transfer system with the term "*hawala*." This system has different names, however, in different geographical regions. It is called *hawala* in the Middle East, Afghanistan, and parts of Pakistan; *hundi* in India and parts of Pakistan; *fei ch'ien* in China; and *phoe kuan* in Thailand.

[40] Available online http://www.treas.gov/offices/enforcement/ml2002.pdf.

[41] The working group includes experts from following agencies and organizations: the Office of Comptroller of the Currency ("OCC"), the Department of the Treasury Terrorism and Violent Crime Section, the Department of the Treasury Financial Crimes Enforcement Network, the Securities and Exchange Commission ("SEC"), the Commodity Futures Trading Commission ("CFTC"), the Internal Revenue Service Criminal Investigation Section, BICE , the Department of Justice Asset Forfeiture & Money Laundering Section, the Department of Justice Computer Crime & Intellectual Property Section, the Department of Justice Counter Terrorism Section, the Federal Bureau of Investigation, the Department of Defense, the Central Intelligence Agency, and the National Security Agency.

Internet. The open, multi-disciplinary community out of which the modern Internet evolved is reflected in a number of its signature characteristics – it remains an open, interoperable, decentralized, and largely unregulated network.

The Internet today is a global network of interconnected communication and information systems.[42] A user at any Internet terminal in the world can communicate, share documents and stored information, and engage in financial or commercial transactions with millions of other users throughout the world, or can access the vast wealth of information available on the World Wide Web.[43] The 2002 CIA World Factbook estimates that worldwide there are more than 10,000 Internet Service Providers ("ISPs") and more than 580 million Internet users.[44]

Several of the Internet's cardinal characteristics are relevant to its use to raise and transfer funds. First, Internet users enjoy a large measure of anonymity. Many Internet interactions are memorialized only by computers' exchange of unique numeric identifiers, called Internet Protocol ("IP") addresses, assigned to them by their respective ISPs. Although it is theoretically possible to determine which user was assigned the IP address involved in a transaction, there are a number of practical obstacles to such a determination. The anonymous nature of the Internet has the desirable effect of protecting Internet users' privacy. As with many characteristics of the Internet, however, anonymity is a double-edged sword. It also makes difficult investigation of Internet users who engage in illegal conduct.

Second, the Internet is, for all intents and purposes, not geographically bounded. An Internet user in Washington, DC can as easily exchange e-mail, engage in "chat," visit a web page, or conduct web-based financial transactions with a user or server in a foreign country anywhere in the world as with another user or server in Washington, DC. Again, although it is theoretically possible to locate an Internet user in geographic space, several practical obstacles make the process of pinpointing a user's geographic location difficult. As a result of the Internet's global nature, regulation and investigation of communications and transactions on the Internet often involve two or more countries, which may or may not be on cooperative terms and may or may not have similar procedural and substantive laws.[45]

---

[42] For the purposes of this Report, the term "Internet" does not include the separate network infrastructures provided for automated teller machine ("ATM"), wire transfer, or debit and credit card networks, although it does include web-based applications through which debit and credit card transactions may be accomplished.

[43] The terms "Internet" and "World Wide Web" are often, but incorrectly, used interchangeably. The Internet describes the network itself – the computers, the physical or virtual connections, and all of the protocols and applications it supports – whereas the World Wide Web describes the resources available on that network through the use of one particular protocol, the hypertext transfer protocol ("HTTP").

[44] *See* http://www.cia.gov/cia/publications/factbook/geos/xx.html.

[45] International differences in regulatory regimes and procedural and substantive laws are mediated to a large degree in the area of terrorist financing by a number of international legal instruments and by the work of several multilateral organizations. The International Convention for the Suppression of the Financing of Terrorism, which was adopted by the United Nations in 1999 and has been ratified by 61 countries, requires countries to establish substantive and procedural laws pursuant to which acts of terrorist financing can be effectively investigated and prosecuted and the proceeds of terrorist financing can be frozen, seized, and forfeited. The United Nations Security Council also passed immediately after the September 11th attacks a resolution requiring all 189 member nations to freeze the financial assets of persons and entities who commit or attempt to commit terrorist acts and to forbear from making funds available to terrorists and their supporters. The 33 members of the Financial Action Task Force on Money Laundering ("FATF") have endorsed eight Special Recommendations on Terrorist Financing, which establish international standards relating to regulations and laws facilitating the prevention, investigation, and prosecution of terrorist financing, and to international cooperation in the enforcement of such regulations and laws. Similarly, on June 3, 2002, the General Assembly of the Organization of American States ("OAS") entered into a comprehensive treaty to prevent, punish, and eliminate terrorism. The Inter-American Convention against Terrorism seeks to prevent the financing of terrorism, strengthen border controls, and increase cooperation among law enforcement authorities in different OAS countries, among other measures. The UN, the G8, the OAS, the Asian Pacific Economic Cooperation ("APEC") group, the Association of Southeast Asian Nations ("ASEAN"), the International Organization of Securities Commissions ("IOSCO"), and other bilateral and multilateral fora continue to explore the ways in which international cooperation can facilitate the prevention, investigation, and prosecution of terrorist financing.

Third, the Internet permits users to communicate and conduct financial transactions more quickly and more surreptitiously than would be the case if they were using traditional phone lines or conducting business through "brick-and-mortar" financial institutions. By using widely-available encryption tools, Internet users can convert a message or document into "ciphertext" for secure transmission. The message or document is unintelligible to anyone except the intended recipient, who possesses the key necessary to decrypt it. Similarly, Internet users can embed messages or documents into image, sound, or other files through a process called "steganography." Steganographic files are indistinguishable from the millions of regular files transiting through or posted on the Internet. Unless one knows that the file has an embedded message and possesses the proper tool to reveal that message, it may well remain undetected. These encoding algorithms have important and legitimate information security and privacy protection applications. But when they are combined with the speed of Internet communications, the ephemeral nature of records of Internet communications and transactions (retention periods vary by ISP, ranging from no retention at all to a period of days to, in rare cases, a period of years), and the largely unregulated nature of the Internet, they also pose obstacles to investigations of Internet communications and transactions.

Finally, the Internet is subject to very little regulation. To a large degree, the only "regulations" imposed on Internet users are those that are essential to the Internet's functioning. Because the Internet developed as an open, interoperable network, such rules are few in number and impose only minimal constraints. Moreover, because the Internet is global and decentralized – there is no single point or even set of points through which all information transiting the Internet must flow – its architecture is not easily susceptible to regulation.

In sum, the Internet poses unique challenges to regulatory bodies and to law enforcement because it is largely anonymous, geographically unbounded, unregulated, and decentralized. These challenges will be a recurring theme in the discussion that follows.

2. Raising Funds

Investigations indicate that terrorists and terrorist organizations can use the Internet in four primary ways to solicit funds and collect resources:

1. They can solicit donations, share information, and recruit supporters directly via web sites, chat rooms, and targeted electronic mailings;

2. They can exploit charitable organizations, solicit funds with the express purpose of clothing, feeding and educating a population but with the covert intent of exploiting contributors' largesse to fund acts of violence;

3. They can perpetrate online crimes such as identity and credit card theft, intellectual property piracy, and fraud and support their mission with the proceeds of such crimes; and

4. They can use the Internet as a means of communication to organize and implement other fund raising activities.

The support sought by, and provided to, terrorist organizations need not always be in the form of currency. Terrorist organizations may also solicit online other fungible goods (gold or gems, for instance),[46] supplies, or adherents and foot soldiers. This Report construes "raising funds" broadly in order to provide a comprehensive discussion of the manner in which terrorist organizations use the Internet to further their cause (with the notable exception of using the Internet as a weapon to attack critical infrastructures). In particular, the Report construes raising funds to be consistent with the United States criminal law prohibiting and punishing material support of a terrorist or terrorist organization:

> the term 'material support or resources' means currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances,

[46] *See* Jeannine Aversa, "Cutting Terror Funds Said Effective," The Associated Press, 2002 WL 26545883 (Sept. 10, 2002) (reporting that Treasury officials had emphasized "money flowing through nontraditional financial channels such as trading in diamonds or gold" as one challenge in interdicting terrorist funding).

explosives, personnel, transportation, and other physical assets, except medicine or religious materials.[47]

In the broadest sense, then, the Report addresses how terrorists use the Internet, directly or indirectly, to accumulate the funds, resources, and other material support necessary to maintain their organizations and commit their violent acts.

3. Moving Funds

This Report also construes the term "moving funds" broadly and as encompassing the relevant criminal law. In the context of terrorist fundraising, "moving funds" includes the conduct proscribed and punished by 18 U.S.C. § 1956(a)(2):

> Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States . . . with the intent to promote the carrying on of specified unlawful activity.

The definition adopted by the Report is broader than this statutory definition, however, in two respects. First, the Report also addresses the transportation, transmission, or transfer of funds *within* the United States with the intent to support terrorists and terrorist organizations. Second, the Report interprets moving funds to include making funds available to terrorists or terrorist organizations by providing them with the means of accessing them, such as a debit or credit card, a PIN number, or a password.[48] Terrorist financing may be an inchoate crime in the sense that it is the intent that a further act be committed, a terrorist act, that makes it illegal. Because the parties' intent is often not visible on the face of their transaction, it may be difficult to distinguish legitimate transfers of value (to support an ailing relative in the sender's native land, for instance) from terrorist financing.

This Report will address two different methods of moving funds via the Internet: online banking services and other online financial services such as ARS, brokerage and securities and futures accounts, and digital currency systems. It will also discuss how Internet communications are used to facilitate fund transfers.

4. Terrorists & Terrorist Organizations

The term "terrorists and terrorist organizations" as used in this Report includes the 36 organizations currently designated as Foreign Terrorist Organizations ("FTOs") by the Secretary of State pursuant to 8 U.S.C. § 1189 and the 281 individuals and organizations designated as Specially Designated Global Terrorists ("SDGTs") pursuant to IEEPA. In addition, it includes any person or organization that intends to carry out or to aid, assist or support, an act of domestic or foreign terrorism as those terms are defined by 18 U.S.C. §§ 2331(1) and (5).[49]

There is a temptation to treat terrorist financing just as one would any other form of money laundering or financial fraud, but terrorist financing often has some distinguishing characteristics. First, terrorists and terrorist organizations are not profit motivated. Their goal is not to amass wealth; it is rather to inflict harm and instill terror. Although the maintenance of a terrorist organization may cost tens of millions of dollars annually, terrorist operations such as the September 11, 2001 attacks can often be carried out on relatively low budgets.[50] Accordingly, the funding of terrorist operations may involve fund transfers that are too small to arouse suspicion or trigger regulatory scrutiny. The financing operation of a terrorist cell may be much more modest, and therefore much more

[47] 18 U.S.C. § 2339A.

[48] The Department of Justice asserts that such conduct is proscribed by 18 U.S.C. § 1956(a)(2), although there is no judicial precedent definitively resolving this issue.

[49] *See also* 22 U.S.C. § 2656f(d) ("The term 'terrorism' means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience.").

[50] The FBI estimates the budget required to perpetrate the September 11th attacks at between $300,000 and $500,000. *See* Matthew A. Levitt, *The Political Economy of Middle East Terrorism*, Middle East Review of International Affairs Journal, Vol. 6, No. 4 (Dec. 2002).

difficult to detect than, for instance, the money laundering operation for a drug cartel.

Second, whereas money laundering generally involves financial transactions designed to conceal the illicit origin of funds, the funds used to finance terrorism are often not derived from an illicit source or generated by illicit activity. Law enforcement may uncover money laundering during the investigation of the predicate crime that produced the funds to be laundered – for instance, in the investigation of a drug cartel. Sometimes terrorist financing is linked with other crimes, such as fraud or narcotics trafficking, and may be reported by the victims or otherwise discovered during the investigation of those crimes. In other instances, however, the funds used to finance terrorism derive not from other criminal conduct, but from donations or business proceeds. These facially legitimate fund raising mechanisms are not associated with separate criminal conduct that might arouse law enforcement suspicion. Moreover, in such cases, there may be no "victim" to report the fundraising activity.

The most important distinction between terrorist financing and money laundering, however, is this: terrorist financing supports acts of untold atrocity and violence against innocent victims. Any discussion of terrorist financing must be informed by the stark reality that what leaves our shores as currency or material resources today may later return or appear elsewhere as bullets, bombs, or other means of mass destruction. Understanding and interdicting terrorist financing thus accomplishes more than frustrating a particular type of criminality or recovering criminal proceeds. It presents an opportunity to deprive terrorist organizations of the funding on which their existence depends, to unearth their networks and identify their members before they can act, and to disrupt or destroy them before they take or injure more innocent lives.[51]

B. Methodology

This Report explores the ways in which terrorists and terrorist organizations are using or might use the Internet to raise and move funds, resources, and material support. The Report first discusses the online methods terrorist organizations may use to raise and move funds. It then discusses the challenges posed by these methods in three areas: the prevention of that particular method, whether by regulation, security measures, or deterrence; the investigation of that method to stop the flow of resources and identify the parties responsible; and the prosecution of those parties under United States law.[52] These discussions are meant to raise, but do not purport to resolve, these issues, which may involve choices affecting regulation of the Internet; individual privacy; the rules applicable to banks, other financial institutions, ARS, and tax exempt organizations; and other broad policy concerns.

This Report is both a first step and a work in progress. It is a first step in the sense that it provides a foundation of understanding for further action, such as developing a strategy for preventing, investigating, and prosecuting online terrorist financing. It is a work in progress in that the Internet is an evolving technology. Many of the web sites referred to in the Report, for instance, have long since disappeared, only to be replaced by others. Similarly, as new Internet financial applications and new Internet communication technologies are developed, new challenges may be raised and new issues may be posed.

II. TERRORIST USE OF THE INTERNET TO RAISE FUNDS

Terrorists use the Internet in four different ways to raise funds, collect resources, and recruit adherents. First, terrorists use the Internet as a vehicle for direct

[51] Former FBI Director Louis Freeh, testifying before Congress in 1999, indicated that the 1993 attack on the World Trade Centers could have been much more devastating, but the perpetrators lacked sufficient funds to build a bomb as big as they intended. He also attributed a strong investigative lead in the case to the perpetrators' lack of adequate funding – they were identified in part by their attempt to recover the deposit fee on the rental truck used to transport the bomb. *See* Statement of Louis J. Freeh, Senate Committee on Appropriations, Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies (Feb. 4, 1999).

[52] The Report does not discuss other potential avenues for stopping the flow of resources to terrorist organizations, such as encouraging prosecution by foreign powers or conducting targeted military or intelligence operations against terrorists or terrorist organizations.

solicitation, publishing web sites that openly request money and resources to support their campaign of violence. Second, terrorists infiltrate charitable organizations, soliciting funds from donors who may or may not be aware of the ends to which their donations are being dedicated. Third, terrorists engage in online fraud, identify theft, and other Internet crimes and use the proceeds of these crimes to support their mission. Finally, terrorists use the Internet as a pervasive, inexpensive, anonymous means of communication through which they can plan and orchestrate fund raising activities. Each of these uses is addressed below.

A. Direct Solicitation

Terrorist organizations use web sites, chat rooms, and targeted mass e-mailings to solicit funds directly from their supporters. Several terrorist organizations maintain web sites, accessible to any Internet user that celebrate past acts of terrorism, exhort adherents to further violence, and request donations in support of their causes. A prominent example was the site www.azzam.com, a site named after Abdullah Azzam, Usama bin Laden's mentor who conceived and implemented the idea of establishing international terrorist training camps in Afghanistan.[53] The site sold Islamic extremist publications, including a book by Omar Abdel Rahman, the mastermind behind the 1993 World Trade Center bombings. The site also included a page entitled "What Can I Do to Help Jihad and the Mujahideen?" which read, in pertinent part:

> *Around the Muslim world, the Jihad is being entirely funded by donations from individuals. . . . Jihad is a profitable investment that pays handsome dividends. For someone who is not able to fight at this moment in time due to a valid excuse they can start by the collection and donation of funds . . . Azzam Publications is able to accept all kinds of Zakat and Sadaqah donations and pass them on where they are most needed. The Jihad . . . consists of . . . the one who organizes the weapons and ammunition [and] . . . the one overseas who raises the money . . .*

Several other terrorist organizations have solicited funds and material resources directly from supporters by way of the Internet. A recent article in a Pakistani newspaper reported that five Pakistani jihad organizations currently maintain web sites, some of which receive up to 300 visitors each day.[31] The following examples are illustrative of the direct solicitation sites that have been on the Internet since September 11, 2001:

- $ HAMAS' military wing, the Izz al-Din al-Qassam Brigades, posted communications on a web site recruiting suicide bombers and encouraging supporters "to donate . . . what you can to assist the cause of Jihad and resistance until the occupation is eliminated and every span of the Muslim Palestine is liberated."

- $ Hizballah's television station Al-Manar maintained a web site that urges contributions "for the sustenance of the Intifadah," listing bank accounts in Lebanon to which donations should be made.

- $ The Global Jihad Fund published a web site urging donations "to facilitate the growth of various Jihad Movements around the World by supplying them with sufficient funds to purchase weapons and train their individuals." The site listed bank accounts in Pakistan and featured links to web sites supporting terrorist organizations, including the Taliban, Lasker Taiba, Hamas, and Hizballah.

---

[53] Most of the examples cited in this Report involve terrorist organizations based in the Middle East and founded upon a militant, extreme, anti-American form of Islamic ideology because these organizations currently pose the gravest and most immediate threat to the United States. The Report does not intend to impugn the countries of the Middle East or the vast majority of Islamic sects and communities, many of whom have been among the United States closest allies in waging the war against terrorism since the September 11th attacks. The discussion and conclusions contained in the Report are equally applicable to all terrorists and terrorist organizations, regardless of where they come from, whether they are foreign or domestic, or what their underlying motive or objective may be.

[54] *See* Amir Rana, *Jihad Online*, LAHORE DAILY TIMES, Apr. 20, 2003.

- $ A message carried on at least four jihadist web sites offered greetings from Usama bin Laden, other al-Qaeda leaders, and Mullah Muhammad Omar urged men to donate money and women to donate jewelry to the cause of jihad.

In addition to such web sites, terrorist organizations request donations through bulletin boards, chat rooms, and targeted mass e-mailings. One message posted to an Arabic language Internet forum exhorted its readers to send "assistance to the families of the Guantanamo captives, for the families of the martyrs of the American invasion of Afghanistan, and for the families of those innocent arrestees detained on account of terrorism."[55]

1. Prevention

It is difficult, if not impossible, to prevent such solicitations from occurring through web sites, bulletin boards and chat rooms. Regulation and deterrence fail effectively to prevent such sites from appearing for essentially four reasons. First, the Internet is global. Among the more than 10,000 Internet service providers worldwide are several in countries that have large populations sympathetic to Islamic extremism or antagonistic to the United States. According to the 2002 CIA World Fact Book, the seven nations currently listed by the State Department as "state sponsors of terrorism" maintain 19 ISPs.[56] Website hosts in these countries are not subject to United States regulatory jurisdiction, nor may these countries be eager to assist the United States in preventing terrorist organizations from soliciting funds on the Internet.

Second, the Internet is inexpensive. Many ISPs, including several in the United States, allow subscribers to register online for free web hosting services. These ISPs provide their services to subscribers free of charge and therefore have no incentive to identify accurately their subscribers. Nor do their subscribers have any disincentive to register a web site that will be closed down after a short period of time – it costs them nothing, and they can simply open another one. Indeed, www.azzam.com used to inform its visitors: "We expect our web-site to be opened and closed continuously. Therefore, we urgently recommend any Muslims that are interested in our material to copy all the articles from our site and disseminate them through their own web-sites, discussion boards and e-mail lists."[57]

Third, the Internet may be used anonymously. Users can access the Internet from a public library or a cyber café without providing any identifying information. A user can even register such a web site from his home computer without identifying himself by first visiting a site, called an anonymizer, that replaces the IP address for the user's home computer with another IP address that cannot be traced back to the user (because anonymizers generally do not maintain logs). Internet investigative techniques in such cases will determine that the web site was registered from a public library, a cyber café, or an anonymizer, but will be unable to take the next step and identify the person in the library or café, or the user who visited the anonymizer. *See* Figure 1.

Fourth, the Internet is largely unregulated. In most countries, there is no central government authority that reviews the content of web sites before they are hosted online. Moreover, most ISPs have neither the resources nor the desire to monitor the content of their customers' web sites. Large ISPs have literally millions of customers; small ISPs generally have limited budgets and small staffs. Although law enforcement may search the Internet for public sites soliciting donations to terrorist organizations, they, too, lack the resources to maintain constant vigilance over the vastness of the Internet.

Recent events suggest that terrorist organizations are aware of these and other features of the Internet. The capture of terrorist officials or infiltration of terrorist compounds is now often accompanied by the discovery of computers that have accessed the Internet.[58] In addition, many of the individuals and organizations in the United States under investigation or facing pros-

[55] Available at www.arabforum.net (October 18, 2002).

[56] The nations currently on the State Department list are Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.

[57] Jihad Online: Islamic Terrorists and the Internet, available at http://www.adl.org/internet/jihad_online.pdf (April 22, 2003).

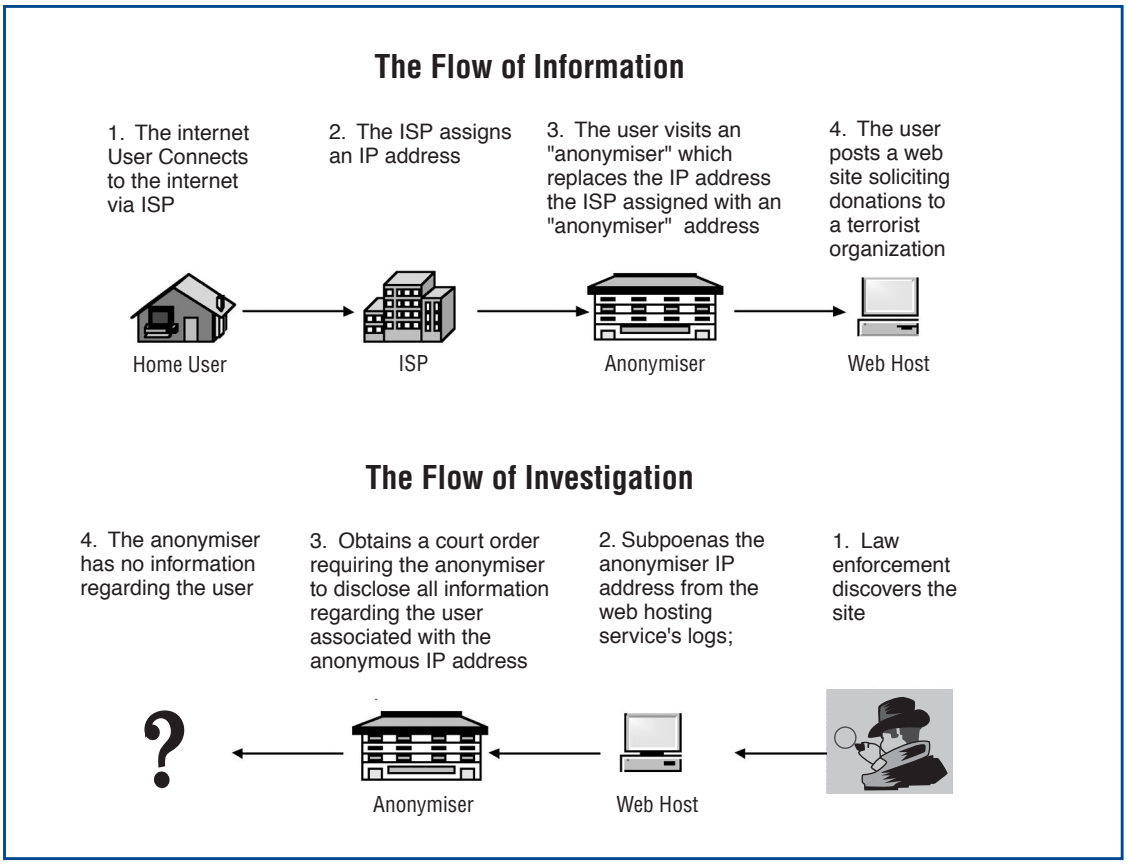


Figure 1

ecution for terrorist-related activities are highly trained in computer networks and communication systems.[59] Cybersecurity specialists also maintain that terrorists have probed the networked operation and security systems for several US critical infrastructures, possibly in preparation for an attack on those systems.[60] Terrorist organizations are becoming increasingly adept at taking advantage of these features of the Internet.

2. Investigation

Investigation of terrorist organizations' direct solicitation of funds over the Internet faces many of the same difficulties as prevention of such conduct. Even assuming that a terrorist web site is hosted in the United States – and in the post September 11, 2001 atmosphere of strict counter-terrorism practices, that is an assumption that would rarely be met – investigating the people responsible for web site, bulletin board, or chat room solicitations may be difficult. If the perpetrator is Internet savvy, he can mask his online identity even as he hosts a public site on the Internet. An example may be helpful in trying to understand how this is possible:

Consider an al-Qaeda operative living in New York City. He receives, by regular mail, a diskette from

[58] *See, e.g.,* Kamran Khan, *Alleged September 11 Planner Captured in Pakistan*, The Washington Post, March 2, 2003, at A1 (reporting that computer equipment was seized from the house in which Khalid Sheik Mohammed was captured); Alan Cullison & Andrew Higgins, *Suicide Watch: Al Qaeda Acolyte, One of Many, Vows to Die for Cause*, The Wall Street Journal, Dec. 30, 2002 (reporting on the contents of a computer seized from a Taliban compound in Afghanistan).

[59] *See, e.g.,* Susan Schmidt, *5 Tied To Islamic Charity Indicated in N.Y., Idaho*, The Washington Post, Feb. 27, 2003, at A2; John Mintz, *5 in Texas Jailed in Hamas Probe*, The Washington Post, Dec. 19, 2002, at A3.

[60] *See* Barton Gellman, *Cyber-Attacks by Al-Qaeda Feared*, The Washington Post, June 27, 2002, at A1.

Pakistan containing the content of a web site praising the September 11, 2001 "martyrs" and encouraging supporters to send funds to three bank accounts in Karachi to support future attacks against the "infidels." The sympathizer accesses the Internet from a New York public library and registers online using false identification information with a free web-hosting provider (there are dozens, at least, in the United States). Law enforcement does not discover the web site for several weeks. They compel the ISP to provide any information it has regarding the subscriber account, a process that may take additional time, and discover that the information is almost certainly false: the site was registered from a public library computer by John Doe at 315 Nameless Avenue, New York, NY, telephone 123-456-7890. Because the ISP keeps virtually no logs (records of activity on the site) – its business plan calls for low overhead, the ISP's representative explains, and logging and data storage cost money – law enforcement obtains, at most, IP addresses for the visits to the site over the last several days. The logs are not detailed enough to distinguish between someone who visited the site accidentally, leaving immediately when he discovered its content, and someone who printed out donation instructions or submitted a donation via credit card while on the site. *See* Figure 2.

With one exception, investigation of the individuals who donate through such sites is subject to the same obstacles – use of public computer terminals or anonymizers, Internet accounts registered using false subscriber information, and failure of the web hosting ISP to retain logs of who visited the site and what they did there. Donors are susceptible to an undercover investigative technique – law enforcement, posing as an online solicitor, can host such a site itself. Sites hosted by law enforcement for the purpose of attracting and gathering information on criminals are called "honey pots." Such a site would appear identical to the one above (law enforcement could even re-open the site on a computer it administered). It would differ from the site above, however, in that it would record everything a visitor did while on the site. If a donor read a home page describing the site's purpose (i.e., to support a terrorist organization) and then filled out and submitted an electronic donation form, law enforcement would have good evidence that the visitor intended to donate money to support a terrorist organization.

3. Prosecution

The United States criminal code contains strict prohi-

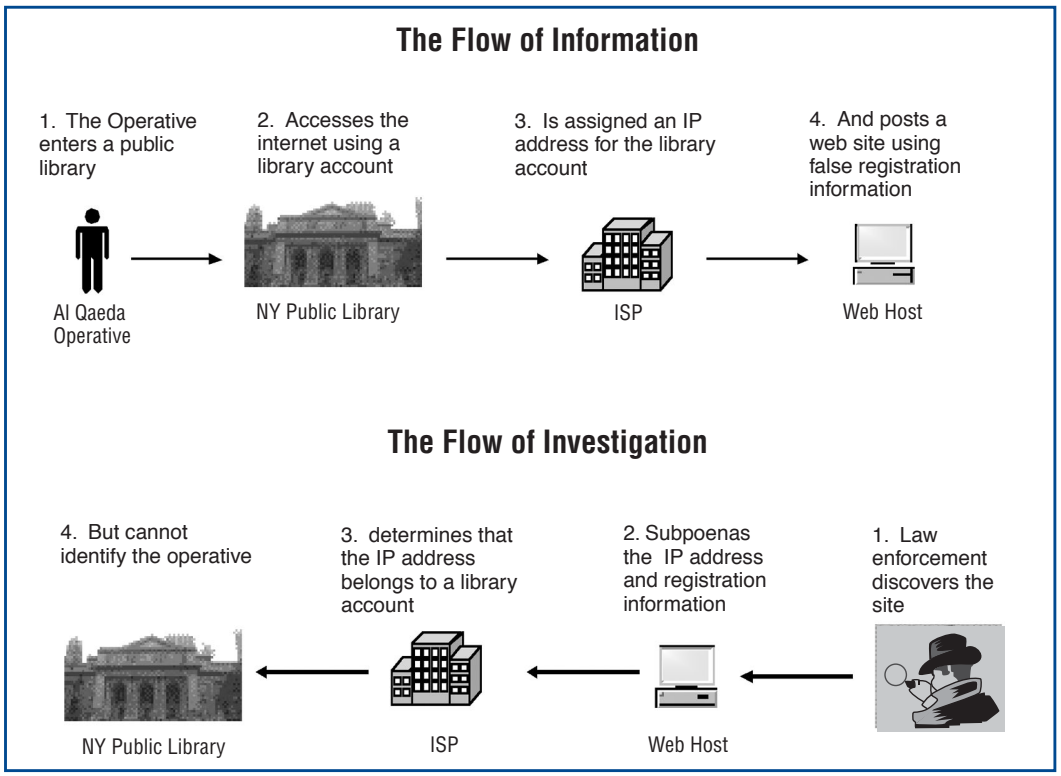


Figure 2

bitions against providing material support or resources, knowing that material support or resources will be used to commit terrorist acts,[61] or that they will knowingly provided to a Foreign Terrorist Organization.[62] The code also prohibits conspiring within the jurisdiction of the United States to kill, kidnap, or maim any individual outside the United States or to damage any property in a foreign country with which the United States is at peace, a prohibition that may apply to a perpetrator who solicits or donates funds in the United States knowing that they will be used to commit a specific act of terrorist violence abroad.[63] Moreover, the money laundering statutes[64] apply to any individual other than the original donor who handles such a donation knowing that it will be used to support a terrorist organization, because each such individual conducts a transaction knowing that it involves the proceeds of illegal conduct (the donation) with intent to promote or continue the conduct. These criminal statutes impose substantial penalties for violations and, in conjunction with other statutes, enable the government to seize and forfeit the proceeds of illegal fund raising activities.

As the United States' global effort to crack down on terrorist fundraising gains the support of countries around the world, the regimes under which terrorist organizations are allowed to flourish are decreasing. As a result, direct solicitation is becoming less prevalent, and terrorist organizations are exploiting other, more surreptitious means of raising funds.

B. Exploitation of Charities & E-Commerce

Terrorist organizations have frequently and successfully exploited charities as vehicles for surreptitious fundraising. In some cases, as with Wafa al-Igatha al-Islamiya, Rabita Trust, Rashid Trust, Global Relief Fund, Benevolence International Foundation, and Ummar Tamir-e-Nau, terrorist organizations have established a charity with an ostensibly humanitarian purpose. These charities have advertised in sympathetic communities' press and on web sites and chat rooms with common themes.[65]

For example, Al-Rashid Trust, a Pakistan-based, al-Qaeda affiliated charity describes itself as "[a] prestigious welfare organization whose comprehensive services are benefiting all the Muslims of the world."[66] The Trust's web site, which is still available in English as of the writing of this Report, solicits donors with an impressive list of humanitarian accomplishments and a promise that "[m]ore attention shall be given to the departments of health, food, education, and employment."[67] Just days after the September 11, 2001 attacks, however, President Bush signed an executive order identifying the Trust as a financial conduit for the Taliban and al-Qaeda and freezing its U.S. assets.[68]

The Benevolence International Fund ("BIF") provides another excellent example of how terrorists can simultaneously raise funds and avoid scrutiny by cloaking themselves as a charitable organization. In

---

[61] *See* 18 U.S.C. § 2339A.

[62] *See* 18 U.S.C. § 2339B.

[63] *See* 18 U.S.C. § 956.

[64] 18 U.S.C. § 1956.

[65] The Qur'an requires Muslims to give a portion of their money to charity. The Quran divides alms giving into the obligatory ("zakat") and the voluntary ("sadaqa"). Devout Muslims may give contributions directly to Islamic organizations or needy individuals. In some Islamic countries, however, the collection and distribution of charitable funds is managed by the government. For example, the Islamic affairs councils of various states in Malaysia collect and disburse contributions, while Pakistan imposes a 2.5% annual income tax upon its Sunni Muslim residents. Unfortunately, terrorist organizations exploit this admirable Islamic practice to support their mission of violence.

[66] *See* www.ummah.net.pk/dharb/services.htm (April 22, 2003).

[67] *Id.*

1993, the IRS granted BIF tax-exempt status under 26 U.S.C. § 501(c)(3).[69] BIF raised millions of dollars each year during the 1990s, in part by accepting donations on its web site. Authorities have uncovered evidence that BIF supported al-Qaeda and other terrorist organizations. The Department of Treasury has listed BIF as a financier of terrorism.[70] In October 2002, BIF's leader, Enaam Arnaout, was indicted for, among other things, providing material support to terrorist organizations, including al-Qaeda.[71] In 2003, Arnaout pled guilty to charges involving diversion of charitable contributions to armed militant groups in Bosnia and Chechnya.[72]

In other cases, terrorists have infiltrated branches of an existing charity to raise funds surreptitiously. Many such organizations provide the humanitarian services advertised: they feed and clothe the poor, educate the illiterate, provide medical care for the sick and the suffering – and it is important not to presume that charitable organizations have terrorist affiliations simply because they serve regions or religious or ideological communities with which terrorism may be associated. Some such organizations, however, in addition to pursuing their public mission of providing humanitarian aid, pursue a clandestine agenda of providing material support to the militant groups that seek violently to "liberate" their particular region or expand the influence of their particular religion or ideology. These organizations' propaganda may or may not provide hints as to their darker, more secret purpose.

Terrorist-affiliated entities and individuals have also established Internet-related front businesses as a simultaneous means of facilitating communications among terrorist cells and raising money to support their mission. For example, InfoCom, a Texas-based ISP, was indicted along with its individual corporate officers in December 2002 on thirty-three counts relating to its provision of communication services, in-kind support, and funds to terrorist organizations such as HAMAS and the Holy Land Foundation for Relief and Development.[73] According to the Indictment, InfoCom also exported advanced computer technologies to Libya and Syria, designated state sponsors of terrorism, in violation of IEEPA.[74] Incorporated in Texas in 1992, InfoCom's initial capital was donated primarily by Nadia Elashi Marzook, wife of HAMAS figurehead and specially-designated terrorist Mousa Abu Marzook.[75]

1. Prevention

Charities continue to be an attractive vehicle to terrorist groups seeking to raise and move funds. Such organizations are often hard to distinguish from the scores of legitimate charities providing humanitarian aid, a task rendered more difficult by the fact that often organizations that bankroll terrorist groups also finance legitimate charitable projects. The Internet exacerbates this problem in two respects. First, a charity may locate itself anywhere in the world – in a state that sponsors terrorism, for instance, or a country that does not regulate charitable organizations – and, through the Internet, obtain access to donors worldwide. Second, a charity that exists primarily online

---

[68] Exec. Order No. 13224, 66 Fed. Reg. 49079 (Sept. 23, 2001).

[69] *See* Indictment, United States v. Arnaout, No. 02-CR-892 (N.D. Ill. Nov. 1, 2002), available at http://news.findlaw.com/hdocs/docs/terrorism/usarnaout10902ind.pdf.

[70] *See* Indictment, United States v. Arnaout, *supra* note 43.

[71] *Id.*

[72] *See* Plea Agreement, United States v. Arnaout, , No. 02-CR-892 (N.D. Ill. Nov. 1, 2002), available at http://news.findlaw.com/hdocs/docs/bif/usarnaout203plea.pdf.

[73] *See* Indictment, United States v. Elashi, Cr. No. 3:02-CR-052R (N.D.Tex.) Dec. 17, 2002), available at http://news.findlaw.com/hdocs/docs/infocom/uselashi121702sind.pdf.

[74] *Id.*

[75] *Id.*

(the Working Group is not currently aware of any that exist *only* online) is not generally subject to the scrutiny of donors or regulators in the way that predominantly brick-and-mortar charities are. Donors do not, for the most part, visit the charity's offices or speak to one of its representatives.

The United States' effort to prevent terrorist groups from raising and moving money through charities focuses largely on international cooperation and domestic regulation. With regard to charities that are located overseas, the United States relies heavily on the host country's help in preventing abuse. To this end, the Special Recommendations on Terrorist Financing adopted by the FATF in October 2001 exhorted member countries to review their laws and regulations governing charitable organizations and ensure that such organizations are not subject to misuse.[76] In addition, the United States has actively availed itself of bilateral meetings and multilateral *fora* to encourage other countries to strengthen regulatory control over charities within their borders.[77]

To obtain charitable status in the United States an organization must file an Application for Recognition of Exemption (Form 1023) with the IRS.[78] The Application requires the organization to list its name, address, phone number, and web site and general information about its formation or incorporation and its activities and operations. The organization must also provide information regarding its financial support and its fundraising program, its officers or directors, and the basis upon which it qualifies for exempt status.

Once the IRS grants an organization tax-exempt status, the organization must file annually a Form 990 containing its name, address, web site and phone number; its contributions and other forms of income or revenue; its operational expenses; its charitable activities and accomplishments; its officers and directors; and a list of its contributors who donated more than $5,000 during that year.

The Internal Revenue Code specifies the procedures that the IRS must follow to revoke the exempt status of any organization.[79] The Code also provides the organization with the right to contest a determination that its tax exempt status should be revoked in the United States Tax Court, and appeal an adverse decision from the Tax Court to the appropriate United States Court of Appeals.[80] To revoke an organization's tax exempt status, the Commissioner of Internal Revenue must: (1) conduct an examination of the organization; (2) issue a letter to the organization proposing revocation; and (3) allow the organization to challenge that determination in administrative proceedings.[81] The actual letter of revocation may be issued only at the conclusion of that administrative process. During any subsequent Tax Court proceeding or appeal to the Court of Appeals, the organization continues to enjoy tax exempt status. This process may take years to complete. As a result, an organization that has had its assets frozen pursuant to a Presidential order may continue to remain tax exempt under the code for years. To address this situation, the Senate is currently considering a bill that would suspend an organization's status as soon as it is identified as a terrorist organization.[82]

Greater awareness and caution on the part of donors may also help curb online terrorist fund raising. In this respect, the Internet provides some of the means to cure its own ills. Donors may be educated both by waging a proactive media campaign to raise awareness of online charities associated with terrorist organiza-

[76] *See* Special Recommendations, *supra* note 17.

[77] *See* Prepared Statement of Kenneth Dam, *supra* note 6.

[78] If the organization seeks the exemption for any subsection other than 501(c)(3), they provide similar information on a Form 1024 instead.

[79] *See* 26 U.S.C. § 7428.

[80] *See id.*

[81] *See id.*

[82] *See* The Care Act of 2003, S.272.

tions and by encouraging donors to take advantage of the vast resources on the Internet regarding charitable organizations. For instance, the site www.guidestar.org provides information on every charitable organization recognized by the IRS. Donors may also take advantage of the web sites of organizations such as InterAction, the Better Business Bureau Wise Giving Alliance, and the National Association of State Charities Officials, which provide reports on charities, promote standards of accountability for charities, and alert donors to current charity frauds.[83] The Treasury Department, too, has promulgated guidelines encouraging charities to operate with appropriate transparency and accountability in order to discourage criminals and terrorists from exploiting charitable organizations.[84] By publicizing terrorists' use of charity web sites to raise funds and by encouraging donors to learn about a charity before contributing to it, the amount of unwitting donations made to terrorist groups can be reduced.

2. Investigation

Investigation of a charitable organization with an online presence generally begins with discovery of that organization's affiliation with a terrorist organization. In a rare case, it may be possible to demonstrate the affiliation by online investigation. For instance, if a charitable organization's web site includes a hyperlink to a terrorist propaganda page or vice versa, this may form the basis for further investigation. The information provided regarding a particular charity by online information services, such as www.guidestar.org, may also provide grounds to suspect that a charitable organization has terrorist connections. More often than not, however, the affiliation will be discovered through offline investigative techniques.

Once the affiliation is identified, there will be several sources of information online. The ISP that hosts the charity's web site may have logs that indicate who created the site, who has visited it, and what they have done there. In addition, such organizations may keep electronic records of their donors, so that they can contact them again for future donations. Records regarding the accounts associated with the organization may be subpoenaed, and affiliated electronic mail accounts can be searched for communications with members of terrorist organizations or regarding terrorist activities. In addition to these online sources, law enforcement may obtain a charitable organization's Form 1023 or 1024 and its Form 990s.[85] *See* Figure 3.

3. Prosecution

Once investigation demonstrates the affiliation between a charity and a terrorist group, the case against the charity or individuals associated with the charity may be made. Law enforcement still has an important decision to make, however, before prosecuting such a charity and/or its donors. A charity that provides funds and resources to a terrorist organization may be a valuable source of information regarding that organization. If the ISP that provides web hosting service to the charity is located within the United States, law enforcement can obtain logs showing the IP addresses from which the site was accessed, the donations submitted online, and the electronic communications of the web site operators (assuming that they provide their own electronic mail service through the web site), which may identify individuals involved in the terrorist organization or reveal details about imminent terrorist operations. Law enforcement must assess in each investigation whether the benefit to be gained by prosecuting the individuals who are abusing the charitable organization outweighs the benefit to be gained by monitoring them as they continue to act.

If law enforcement does prosecute such a case, as discussed above, providing money or material support to a terrorist organization may violate 18 U.S.C. § 2339A, § 2339B (if the organization has been designated a FTO), or § 956. Soliciting donations over the Internet from donors who believe their money is being

[83] *See* http://www.interaction.org; http://www.give.org/donors/index.asp; http://nasconet.org.

[84] *See* U.S. Department of the Treasury Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S. Based Charities, available at http://www.treas.gov/press/releases/docs/tocc.pdf.

[85] As a result of amendments to the tax laws passed in the Victims of Terrorism Tax Relief Act of 2001, Pub. L. No. 107-134, 115 Stat. 2427 (Jan. 23, 2002), law enforcement now has expanded authority to obtain tax returns and return information for the purpose of preventing or investigating terrorist incidents, threats, or activities. *See* 26 U.S.C. § 6103.

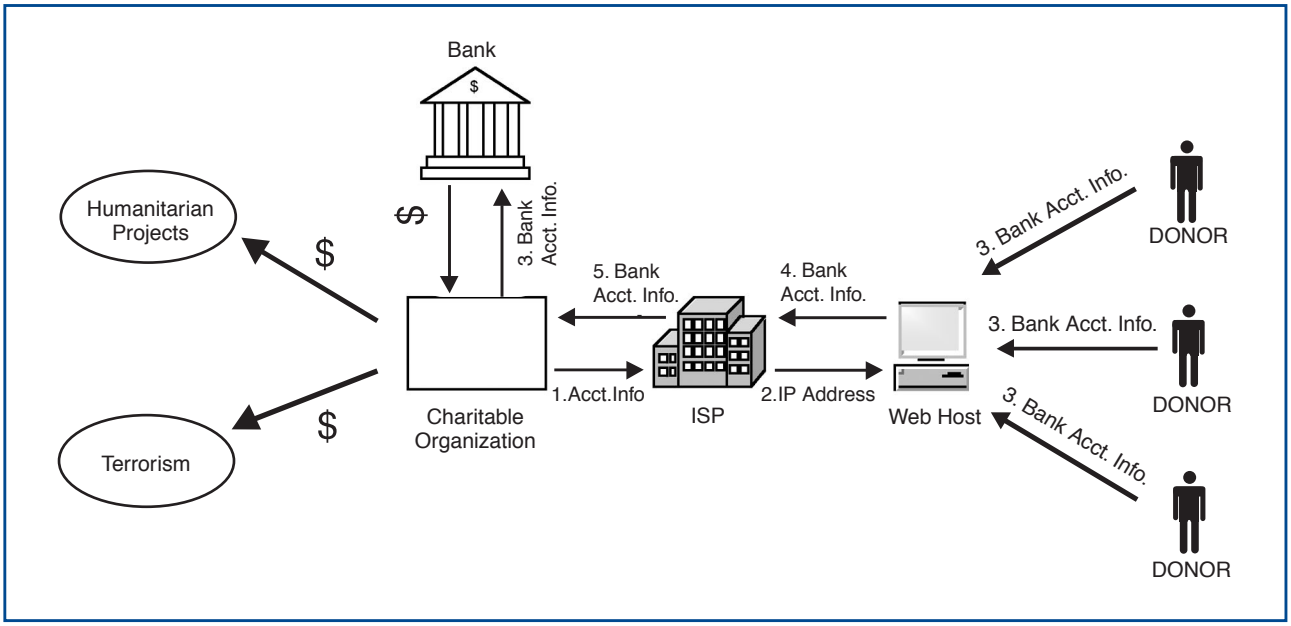


Figure 3

used for humanitarian purposes, when in fact it is being used to support violent extremism and militancy, may violate the wire fraud statute.[86] Transferring funds received by a charity to another organization to further such unlawful activity may violate the money laundering statute, § 1956. In all likelihood, too, the organization will have submitted false tax documents, a violation of 26 U.S.C. § 7206(1).

Prosecution of contributors to such organizations would, in most instances, not follow because such contributors intended to contribute to a humanitarian organization, not to a terrorist front. Generally, a contributor must know that a charity is affiliated with a terrorist organization to be prosecuted for a violation of sections 956, 1956, or 2339A. If an organization has been designated a FTO, however, the prosecutorial burden is somewhat lighter – under section 2339B, the government must prove only that the contributor had knowledge concerning the status of the recipient FTO; it need not prove that the contributor knew the funds would be used to support terrorist activities.

C. Proceeds of Online Crimes

In addition to soliciting funds, either directly or through charitable or e-commerce front organizations, terrorist groups use the Internet to raise funds by perpetrating online crimes. The same qualities that protect individual privacy on the Internet make it particularly susceptible to fraud and deception. The anonymity users enjoy online also allows the perpetrator of a fraud to pose easily as someone else – an identity theft victim or a fictitious person. Terrorists have used identities they have stolen through online fraud schemes to obtain cover employment within the United States, access to bank and credit card accounts, and even entry into secure locations.[87]

It requires very little technical expertise to change the "from" information on an e-mail so that it appears to come from an ISP's billing department, a credit card company, or a bank. Just slightly more skill allows a user to design a fraudulent web page that purports to be an ISP's, the credit card company's, or the bank's customer service center. The ease and efficiency with which an Internet user can communicate with hundreds or thousands of other users, regardless of

[86] 18 U.S.C. § 1343.

[87] *See* Dennis M. Lormel, Statement on Technology, Terrorism and Government Information before the Senate Judiciary Subcommittee (July 9, 2002).

geographic location, makes the Internet an environment particularly conducive to vast fraud schemes with numerous victims.

Online auction fraud is another common e-crime gambit – the perpetrator offers to sell a valuable item, such as a piece of jewelry, through an online auction service, receives payment, and never sends the item. The purchaser attempts to obtain recourse from the seller, only to find out that he has provided fraudulent contact information. Online securities frauds, such as "pump and dump" schemes in which an investor publishes fraudulent information about a security online to inflate its value and then sells large quantities of the security at the inflated price, might also provide a source of funding for terrorist organizations.[88] Finally, commentators have recently suggested that the proceeds of intellectual property piracy may also be supporting terrorist organizations.[89]

1. Prevention

Regulation of ISPs and of Internet users themselves would prevent some online crimes. If electronic communications services, remote computing services, web hosting services, and other ISPs were required to obtain and verify valid contact information for each of their subscribers, for instance, the number of investigations that would dead end at false registration information would diminish significantly. Similarly, if ISPs were required to retain logs regarding the use of their services, more information would be available to law enforcement investigating online crimes. The United States does not require by law or regulation, however, that ISPs retain such information, in part because regulatory approaches to the prevention of online crime are viewed as at odds with the free and open ethic of the Internet.[90] ISPs are understandably reluctant to have business practices that facilitate law enforcement investigations, rather than profit generation, imposed upon them. Internet users are understandably protective of their privacy and anonymity.

For these reasons, the problem of Internet crime may be better prevented by encouraging increased security by ISPs and online businesses and by educating Internet users regarding the danger of fraud online. ISPs and online businesses can significantly reduce Internet crime by many means, some as simple as actively notifying their subscribers of current scams and swindles. Similarly, Internet users can abate online fraud by following simple rules such as "never provide your credit card number over the Internet except over a secure connection with a merchant you trust." As such measures reduce Internet crime in general, they will also reduce the amount of money flowing to terrorist organizations.

Deterrence, also, may play an important role in diminishing terrorists' ability to capitalize on online crimes. In both the USA PATRIOT Act and the Homeland Security Act, Congress strengthened the statutory penalties for some computer crimes.[91] The Homeland Security Act also directed the United States Sentencing Commission to amend the United States Sentencing Guidelines to reflect adequately the prevalence and seriousness of computer crimes.[92] In addition, federal, state and local investigative and

---

[88] For a thorough discussion of online securities frauds, *see* John Reed Stark, *Enforcement Redux: A Retrospective of the SEC's Internet Program Four Years after Its Genesis*, 57 Bus. Law. 105 (2001).

[89] *See* Matthew A. Levitt, *The Political Economy of Middle East Terrorism*, Middle East Review of International Affairs (MERIA) Journal, Vol. 6, Issue 4 (2002).

[90] Most European countries have also shied away from requiring ISPs to retain information. "[T]o ensure . . . protection of . . . the right to privacy, with respect to the processing of personal data in the electronic communication sector," the European Union obligates its 15 member countries to pass laws requiring ISPs to delete information regarding electronic communications if it is no longer being used to ensure the integrity of the communication service or for billing purposes. European Union Directive on Privacy and Electronic Communications, 2002/58/EC (July 31, 2002). Several European countries, including France, Spain, Ireland, and Denmark, have, however, taken advantage of an exception to the "data protection" requirement that permits countries to adopt legislation requiring ISPs to retain data "for a limited period . . . to safeguard national security, . . . defence, public security , and the prevention, investigation, detection and prosecution of criminal offenses." *See id.*, at Art. 15(1).

[91] *See* USA PATRIOT Act, Pub.L. 107-56, Title VIII, § 814 (2001); the Homeland Security Act, Pub.L. 107-296, Title II, § 225 (2002).

[92] *See* the Homeland Security Act, Pub.L. 107-296, Title II, § 225 (2002).

prosecutorial agencies have improved their ability to respond to such crimes. As these steps make punishment for online crimes more likely and more severe, the Internet will become a less appealing environment for criminal activity.

2. Investigation

United States law enforcement's capacity to investigate and prosecute computer crimes has increased over the last several years. This is due, in part, to amendments in the USA PATRIOT Act and the Homeland Security Act to the procedural laws applicable to investigations of online activity.[93] These two Acts amended the laws that prescribe the procedures by which law enforcement may obtain information regarding online communications,[94] effectively streamlining these procedures while protecting the autonomy of ISPs and the privacy of Internet users. The Acts also amended the substantive laws applicable to computer crimes,[95] explicitly taking new strains of Internet criminality into account and strengthening penalties for many online crimes.

Law enforcement's increasing effectiveness in investigating and prosecuting computer crimes is also due, in part, to the dedication of increased resources to this area and to federal, state, and local law enforcement entities' concomitant development of expertise in the area of computer crimes. Many such entities now have cybercrime squads that are trained to investigate crime committed via the Internet.

The investigation of computer crimes has also been a fertile ground for international cooperation over the past seven years, resulting in a greater ability to track computer crimes that cross international borders. The G8 Roma & Lyon Groups, established to combat, respectively, transnational terrorism and transnational organized crime, for example, maintain a group of international computer crime experts, the G8 Subgroup on High-Tech Crime, that has promulgated principles and best practices regarding the prevention, investigation, and prosecution of computer crimes. The Subgroup also maintains a network of computer crime experts from 31 countries that are available 24-hours-a-day, 7-days-a-week to respond to computer crime emergencies. In addition, in November 2001, the Council of Europe completed negotiation of the Convention on Cybercrime, which commits its 35 signatories to pass procedural and substantive computer crime laws and to provide assistance to other signatory countries investigating cybercrimes.[96] Such cooperation and capacity-building in the international community is essential if the United States is to investigate effectively a mode of criminality that often transcends international borders.

It is worth noting that the measures for effectively preventing Internet crime and those for effectively investigating it are complementary. Adequately secured ISPs, well-educated users, strong, comprehensive procedural and substantive laws, and enhanced law enforcement capacity all support effective prevention and investigation of online crimes and deprive terrorists of the proceeds of such crimes as a source of funding.

3. Prosecution

As mentioned above, the procedural and substantive laws pertaining to computer crimes have been amended twice since September 2001, aiding both investigators and prosecutors while maintaining a healthy respect for Internet privacy. Federal, state, and local prosecutorial teams have also developed specific expertise in the area of computer crimes. The United States Department of Justice, for instance, maintains

---

[93] *See supra* note 4. Some of the amendments in the USA PATRIOT Act are subject to a sunset provision which will remove them from the code, unless they are affirmatively renewed, on December 31, 2005. *See* Pub.L. 107-56, Title II, § 224 (2001). If these provisions are permitted to sunset, it will be a tremendous setback to law enforcement's ability to investigate and prosecute online crimes.

[94] Generally speaking, these laws are the Wire Tap Act, 18 U.S.C. §§ 2510, et seq., the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701, et seq., and the Pen Register/Trap & Trace statute, 18 U.S.C. §§ 3121 et seq. *See also* the Department of Justice's manual, "Searching and Seizing Computers and Electronic Evidence," available at http://www.cybercrime.gov/s&smanual2002.pdf.

[95] The primary substantive law applicable to computer crimes is the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

[96] *See* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

the Computer Crime & Intellectual Property Section, a team of approximately 40 attorneys with expertise in the prevention, investigation, and prosecution of computer crimes.[97] This team forms the nucleus of a network of federal computer crime experts that includes at least one Computer & Telecommunications Coordinator ("CTC") in each of the United States' 94 federal law enforcement districts and Computer Hacking and Intellectual Property ("CHIP") units in several of the larger districts. These experts complement traditional investigative techniques with Internet investigative techniques (such as legally obtaining information from ISPs and using publicly available online resources) and computer forensics.

Although one should not expect fraud or unauthorized intrusions to be eradicated from the Internet any more than fraud or burglary have been eradicated from the brick-and-mortar world, as network security, user education, and investigative and prosecutorial capabilities all continue to improve, Internet crime may well decrease, and with it the proceeds terrorist organizations derive from Internet crime.

III. TERRORIST USE OF THE INTERNET TO MOVE FUNDS

Terrorists and terrorist organizations may use the Internet to transfer funds in three primary ways. First, they can use Internet banks and online banking and other financial services.[98] Second, they can use Internet-based alternatives to the banking system, such as Internet payment services and e-cash. Finally, terrorists can communicate over the Internet regarding the movement of funds. Each of these topics is taken up below.

A. Internet Banks, Online Banking, & Other Online Financial Services

Brick-and-mortar banks and other financial institutions increasingly offer their customers online financial services.[99] A recent article estimated that whereas in 1994 only .3% of United States households used online banking, currently 26% (a total of 21 million United States households) use such services.[100] The article projected that this figure would increase to 45% by 2010. Similarly, an April 2002 report on Internet banking by Harvard University's Program on Information Resources Policy indicated that all the largest United States banks now offer Internet banking.[101]

As demand for the convenience of online services increases, Internet-only banks are also entering the market. There were only nine separately chartered virtual banks at the beginning of 2000.[102] For instance, First-e, the virtual bank of online finance company Enba, attracted 71,000 customers in its first six months of business. Online banking is equally popular abroad, with financial entities such as EGG and ING populating foreign financial services markets.

The Internet infrastructure underlying online banking and other financial services allows customers more easily to take advantage of the global nature of the financial system. With a few clicks of the mouse, a customer in one country can set up accounts in several other countries. With a few more clicks, the customer can transfer money between these accounts. The

---

[97] To learn more about the Department of Justice's efforts to combat computer crime and intellectual property violations, visit http://www.cybercrime.gov.

[98] Terrorists and terrorist organizations may move funds through a variety of formal financial institutions, including securities and futures brokerages, mutual fund companies, and investment companies. These institutions are included within the definition of "financial institution" set forth in the anti-money laundering provisions of the Bank Secrecy Act and, pursuant to the USA PATRIOT Act, they must establish anti-money laundering programs reasonably designed to prevent their use for money laundering or terrorist financing. *See* 31 U.S.C. §§ 5313(a)(2) and 5318(h).

[99] Although this Report focuses primarily on the banking system, much of the discussion in Section III.A applies equally to non-banking financial services and to non-depository financial institutions.

[100] *The Rise in Online Banking*, The Philadelphia Inquirer, February 10, 2003.

[101] Karen Furst, William W. Lang, and Daniel E. Nolle, Internet Banking: Developments and Prospects (April 2002), available at www.pirp.harvard.edu.

[102] *Id.*

efficiency of the Internet also makes it easier to "layer" transactions and fund transfers, routing money through a number of accounts using a number of different instruments and transfer mechanisms within a short period of time. *See* Figure 4. If any of the accounts used by the customer is in a country that does not require financial institutions to maintain information regarding such transactions or in a country that does not share such information, the ability to trace such transfers is severely hindered.

Terrorist use of online banking services is facilitated in part by banks that have terrorist ties. For instance, Al-Taqwa Bank, founded by the Muslim Brotherhood in the Bahamas in 1988, maintained branches in Algeria, Liechtenstein, Italy, Malta, Panama, and Switzerland, and provided banking services to al-Qaeda and HAMAS until it was shut down by sanctions in the wake of September 11, 2001.[103] Similarly, HAMAS established Al-Aqsa Bank in 1997.[104]

The convenience, speed, and fluidity of online financial services are tremendous assets to customers and to the global economy. These same features, however, make online financial services a potential vehicle for terrorists and terrorist organizations seeking to move funds.

1. Prevention

Regulation of the financial services industry is the primary tool for preventing terrorists from moving funds through the United States banking system. Banks often act as the gateway to the world of financial and fund transfer services. The first step in financial security is identifying a customer as she opens an account and verifying her identity.[105] In this arena, the Internet poses some unique challenges.[106] For traditional brick-and-mortar banking, this process often involves meeting the customer, obtaining identifying documents that have photographs or list physical characteristics that match the customer's characteristics, and observing the customer's behavior. In an Internet banking context, none of these traditional techniques is possible.[107] Banks can, and do, ameliorate the risks inherent in online banking by requiring new customers to provide identifying information such as their social security number, driver's license number, address, and phone number and by indepen-

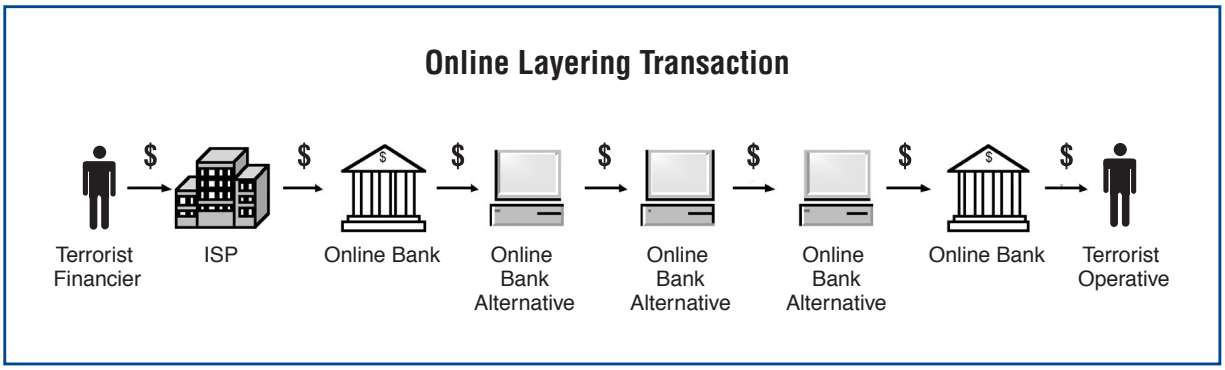


Figure 4

[103] *See* Testimony of Steven Emerson, *supra* note 49.

[104] *Id.*

[105] *See* Internet Banking: Comptroller's Handbook (Oct. 1999), available at http://www.occ.treas.gov/handbook/intbank.pdf. Banks may also offer transferable monetary instruments such as money orders and value transfer services such as wire transfers without requiring a customer to open an account. Monetary instruments are subject to identification rules promulgated by FinCEN if they are purchased with more than $3,000 in cash. *See* 31 C.F.R. § 103.29. Likewise, money transfer services that involve more than $10,000 in cash are subject to FinCEN's currency transaction reporting rule. *See* 31 C.F.R. § 103.30. In addition, the purchase of money orders and the use of value transfer services are subject to the suspicious activity reporting requirements discussed *infra*.

[106] *See* OCC Bulletin: ACH Transactions Involving the Internet (Jan. 14, 2002), available at http://www.occ.treas.gov/ftp/bulletin/soos-2.txt.

[107] *See* Authentication in an Electronic Banking Environment (Aug. 8, 2001), available at http://www.ffiec.gov/PDF/pr080801.pdf.

dently confirming that the information provided is valid.[108]

The USA PATRIOT Act normalized the process of identification and verification, directing the Secretary of the Treasury to promulgate regulations requiring financial institutions[109] to establish reasonable procedures to verify to the extent reasonable and practicable the identity of any customer seeking to open an account, to maintain records of the information used to verify the customer's identity, and to determine whether the customer appears on any list of known or suspected terrorists or terrorist organizations maintained by any government agency. [110]

On April 30, 2003, the Secretary of the Treasury, in conjunction with the Federal banking agencies, the SEC, and the CFTC, released for final publication a series of regulations promulgated under the authority of Section 326 of the USA PATRIOT Act, which requires banks, broker-dealers, mutual fund managers, futures commission merchants, and introducing commodities brokers to adopt a written Customer Identification Program ("CIP") setting forth procedures pursuant to which it will: (1) identify customers as they open accounts by obtaining certain required information such as the customers' name, address, date of birth, and taxpayer identification number; (2) exercise reasonable efforts to verify the customer's identity; (3) maintain records of information obtained during the identification and verification processes; and (4) consult lists identified by the Department of the Treasury of individuals and organizations whose assets have been blocked or frozen. The financial institution's CIP must enable it to form a reasonable belief that it knows the true identity of each customer. These regulations apply equally to online financial services. Financial institutions must comply with the new regulations by October 1, 2003.

Financial institutions' role in ensuring the security and integrity of the United States' financial system does not end once a customer has opened an account. United States banks and securities brokers are also required to report to an appropriate federal law enforcement agency and to the Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") any transaction exceeding $5,000 that attracts suspicion, either because it serves no evident business purpose or because it is unusual for that particular customer.[111] The United States, through participation in multilateral bodies, has encouraged other countries to adopt similar regulations.[112]

As these regulations indicate, much of the burden of securing online financial services against abuse by terrorist organizations must be borne by financial institutions. Both within the United States and internationally, oversight and regulatory bodies have offered guidance to financial institutions seeking to expand into the electronic market without becoming vulnerable to misuse by terrorist organizations and other criminals. For instance, in 2001 the Federal Financial Institutions Examination Council ("FFIEC") issued a report entitled Authentication in an Electronic Banking Environment that advises banks regarding how successfully to verify the identity of new customers who open accounts online and authenticate the identity of existing customers who initiate fund transfers or other transactions online.[113] The OCC

---

[108] *See* Ivan Schneider, *Banks Crack Down on Terror Funds*, Apr. 8, 2002, available at www.banktech.com/story/whatsNews/BNK20020408S0002 (noting that "in the ongoing war on terrorism, banks and their technology providers can best serve the government by acting as a tripwire for criminals attempting to infiltrate the world financial systems").

[109] The statutory definition of "financial institutions" includes banks, credit unions, securities brokers and brokerage houses, currency exchanges, and several other, less formal entities offering financial services. *See* 31 U.S.C. § 5312.

[110] *See* USA PATRIOT Act, Pub.L. 107-56, Title III, § 326 (2001).

[111] *See* 12 C.F.R. § 21.11; 31 C.F.R. §§ 103.18 and 103.19.

[112] For instance, the Special Recommendations on Terrorist Financing adopted by the FATF exhort countries to require of financial institutions and other business entities prompt reporting of suspicious transactions that may be related to terrorism. *See supra*, note 17.

[113] *See* Authentication in an Electronic Banking Environment, *supra* note 85; *see also* OCC Bulletin: ACH Transactions Involving the Internet, *supra* note 84.

and the Federal Reserve Bank of Chicago also offer guidance regarding secure electronic banking and fraud and intrusion prevention.[114] On the international front, in May 2001 the Basel Committee on Banking Supervision, published its seminal document, "Risk Management Principles for Electronic Banking."[115] These documents encourage banks in the United States and abroad to consider the risks involved in offering electronic banking services and develop a strategy to manage those risks; install and maintain adequate security to ensure that electronic banking services are not vulnerable to fraud or attack, either by an insider or an Internet user; actively supervise electronic banking services outsourced to third-party providers; establish adequate identifying and authenticating protocols for electronic bank service customers, preferably involving multiple, complementary methods; and effectuate measures to ascertain the accuracy, completeness, and reliability of banking information exchanged over public electronic networks.

Regulation and security do not provide a foolproof prevention system, in large part because, from the perspective of a financial institution, a transfer of funds to a terrorist organization through a contact in Pakistan, for instance, may look exactly like a legitimate transfer by a Pakistani immigrant sending support home to his family.

2. Investigation

Investigation of terrorist use of online financial services to transfer funds generally begins with information provided pursuant to the banking regulations and security measures discussed above. FinCEN analyzes Suspicious Activity Reports ("SARs") filed by financial institutions, searching for trends and patterns, and assists law enforcement in tracing complex series of financial transactions back to criminal suspects. Law enforcement also investigate reports of electronic banking fraud, attacks on electronic banking systems, and intrusions into electronic banking computers. Such investigations rely heavily on the records maintained by the victim bank, but because they involve online conduct, law enforcement may rely on an additional source of information.

A perpetrator's abuse of an electronic financial service leaves an electronic trail. If the conduct simply involves accessing e-banking services to transfer funds to a terrorist suspect, the perpetrator leaves behind an IP address when he accesses the services. If the ISP through which he connected to the Internet is in the United States, or a cooperating foreign country, law enforcement can obtain the customer information associated with that user, pinpointing the computer from which the account was accessed (although there may still be significant obstacles to identifying the perpetrator if he used an Internet café, public library terminal, or anonymizer). If the conduct involves fraud, the perpetrator leaves behind an IP address and a cache of electronic messages to and from the defrauded financial institution or individual. The financial institution very likely logs both the IP address from which the customer accessed the web site and the customer's activity while on the web site. Whereas an ISP may have little business incentive to maintain logs of its subscribers' communications for extended periods of time, a financial institution has every incentive to maintain thorough and accurate logs of customer and account activities. Not only is reliable verification of account activities central to the financial institution's business, it is required by regulation.[116] Moreover, for an online bank transfer to work, the customer must provide valid destination information. Investigation of online bank transfers therefore poses only one challenge – as suggested by the example of the Pakistani immigrant, it is often difficult to determine which transfers are worthy of investigation.

3. Prosecution

A bank transfer to a recipient that the transferor knows is a terrorist or terrorist organization may be prosecuted under any of several criminal statutory

[114] *See* Internet Banking: Comptroller's Handbook (Oct. 1999), available at http://www.occ.treas.gov/handbook/intbank.pdf; An Internet Banking Primer, available at http://www.chicagofed.org/bankinforeg/bankregulation/Ibankingbooklet.pdf.

[115] *See* Risk Management Principles for Electronic Banking (May 2001), available at http://www.occ.treas.gov/ftp/release/2001-42a.pdf.

[116] The regulations promulgated by the Department of Treasury under the Bank Secrecy Act requiring banks, other financial institutions, and individuals and businesses engaged in certain transactions to maintain records may be found at 31 C.F.R. §§ 103.11-103.39.

provisions. If such a transfer is international, it may constitute money laundering[117] and probably, in addition, constitutes material support.[118] If the transfer can be traced to a conspiracy to commit particular terrorist acts, the transferor and the recipient may also be prosecuted for conspiracy to kidnap, maim, or kill a person or destroy property on foreign territory.[119] Finally, if the transfer is to an individual or entity that has been designated a terrorist or terrorist organization, it may violate the IEEPA[120] and section 2339B. Any intermediary involved in the transfer that possesses the requisite mental state – knowledge that the money is to provide material support for terrorists under section 2339B and knowledge that the money is being given to a designated FTO has also violated those sections. If the conduct involved fraudulent access to financial accounts or services or fraudulent use of customer information, the perpetrator may be tried under the criminal provision prohibiting wire fraud,[121] and potentially also the provisions prohibiting violating the privacy of a financial institution's customer information[122] and perpetrating fraud in connection with an access device such as an account number, PIN number or password.[123] If the conduct involved an intrusion or attack on an electronic banking system, the perpetrator may be tried under the Computer Fraud and Abuse Act.[124] In addition to prosecuting the perpetrator, the government may seek forfeiture of the funds and assets involved.[125]

B. Internet-Based Banking Alternatives

The Internet provides several new financial services and means of transferring value. Internet users can avail themselves of online non-bank payment systems such as AnonymousGold, PayPal, and StormPay; electronic currencies such as E-Bullion, E-Dinar, E-Gold, and Evocash; electronic checks such as those offered by PayNow and BankServ; and electronic debit cards such as "smartcards." Dollar-based electronic currencies such as Evocash and electronic checks are dependent on the banking system. Transactions involving these value transfer mechanisms must eventually pass value into or out of the traditional banking system, subjecting these transactions, at least second-hand, to the record-keeping and reporting requirements imposed on the banking industry.

Many of the online payment systems, gold-backed e-currencies, and smartcard applications, however, are not dependent on the banking industry.[126] For instance, the online payment system StormPay requires only an e-mail address to open an account.[127] Customers can fund their accounts, StormPay states, by credit

[117] 18 U.S.C. § 1956.

[118] 18 U.S.C. § 2339B if the recipient is a designated FTO; potentially 18 U.S.C. § 2339A if the transferor knows that the recipient intends to carry out any of a number of enumerated violent crimes.

[119] 18 U.S.C. § 956.

[120] 50 U.S.C. §§ 1701-1706.

[121] 18 U.S.C. § 1343.

[122] 15 U.S.C. § 6823.

[123] 18 U.S.C. § 1029.

[124] 18 U.S.C. § 1030.

[125] 18 U.S.C. § 981. The USA PATRIOT Act broadened the scope of funds and assets subject to forfeiture actions, bringing within the ambit of Section 981 funds in a United States interbank account, funds that are the proceeds of certain foreign crimes, funds and monetary instruments involved in currency smuggling, funds transferred without complying with currency reporting requirements, and funds that are the assets of terrorist organizations. *See* USA PATRIOT Act, Pub.L. 107-56, Titles III and VIII, §§ 319, 320, 371, 372, and 806 (2001).

[126] While these applications are developing largely independent of the banking system, some of them have implemented security, fraud prevention, and recording practices similar to those imposed on banks. PayPal, for instance, has established an aggressive fraud prevention strategy, cooperated routinely with law enforcement investigations, and reported voluntarily suspicious use of its services that may implicate money laundering, other criminal conduct, or misuse by terrorist organizations.

[127] *See* http://www.stormpay.com/stormpay/.

card, check, electronic currency, another online payment system "and much more!"[128] StormPay even advertises its services as "MLM [multi-level marketing] friendly."[129]

Similarly, AnonymousGold converts funds into or out of a gold-backed electronic currency.[130] To buy a quantity of the e-currency, a customer merely sets up an e-gold account, sends to AnonymousGold, by mail, cash and an order ticket that discloses only the customer's e-gold account number, and notifies AnonymousGold by encrypted e-mail to expect the purchase order.[131] *See* Figure 5. Likewise, to convert a quantity of the e-currency into cash, a customer simply transfers the e-currency into AnonymousGold's account, and then sends an encrypted e-mail to AnonymousGold notifying it of the address to which AnonymousGold should send cash or a blank money order by regular mail.[132] AnonymousGold states that it "do[es] not deal with banks" and that it "destroy[s] all of [its] transaction records upon completion of [a customer's] order."[133] Applications such as StormPay and AnonymousGold effectively protect the privacy of their customers. Without doubt, a vast majority of their customers use their services for legitimate business purposes and private transfers. But because they effectively mask the identity of their customers and destroy or refuse to disclose the records of monetary transactions, such services are also susceptible to abuse by terrorist organizations.

Electronic currency accounts with companies such as e-gold (backed by gold)[134] and e-dinar (backed by the

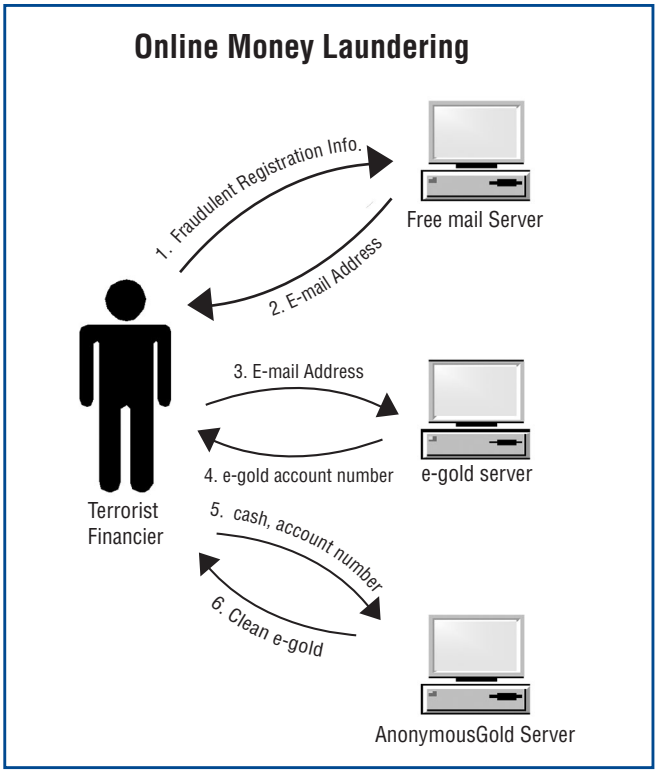


Figure 5

Islamic dinar, a specific weight of gold minted according to Islamic law) may also be opened with only a valid e-mail address (both companies request contact information, but the information does not appear to be verified or essential to the initiation of an account or the provision of services).[135] E-gold can then be converted into any of eight different currencies or transferred instantaneously to any other e-gold account anywhere in the world.[136] Such accounts may be opened with the information of identity theft

[128] *Id.*

[129] *Id.* The term "multi-level marketing" is sometimes used to conceal fraudulent "ponzi" or "pyramid" schemes. *See, e.g.*, "FutureNet Defendant Settles FTC Charges," available at http://www.ftc.gov/opa/1998/11/huff.htm.

[130] *See* http://www.securitygold.com/buy.htm.

[131] *Id.*

[132] *See* http://www.securitygold.com/sell.htm.

[133] *See* http://www.securitygold.com/.

[134] Gold-based e-currencies back accountholders' value by physical reserves of gold or other precious metals. The gold remains in a central, secured vault. Customers pay each other by transferring electronically ownership of a quantity of that gold (GoldMoney, for instance, quantizes its transactions in units of value called GoldGrams). Accountholders can withdraw value from these companies by ordering a check or by ATM or debit card.

[135] *See* https://www.e-gold.com/newacct/; https://www.e-dinar.com/en/index_1.html.

[136] *See* http://www.e-gold.com/unsecure/qanda.html.

victims, funded with their credit cards, and then used to transfer money into the account of a perpetrator.

Magnetic stripe applications and smartcards are another stored value alternative that can interface with the Internet to transfer funds to users around the world. Magnetic stripe stored value applications, such as traditional credit and debit cards, utilize existing financial networks. Smartcards are microcomputers the shape and size of a credit card that contain small electronic data storage chips from which information can be read or to which information can be written with appropriate hardware. Smartcards have a number of useful applications, one of which is serving as a bearer-authenticated form of stored value – whoever holds the card can access the value stored on it. A customer can log on to a website, create a username and PIN number, and fund the card using a check, money order, cashier's check, credit card number, or direct draw from a bank account. The card can then be sent to anyone in the world, and used as though it were cash. The information contained on the card is protected by strong authentication protocols and encryption and cannot be accessed without the appropriate key, PIN, or biometric identifier. If the smartcard or e-cash application relies on securities or brokerage accounts to hold its reserves, these transactions are invisible to the regulatory regime that scrutinizes traditional banking transactions – they appear to be normal, legitimate transactions.

It is not difficult to imagine how these new alternative payment processes might be used, either singly or in series, to transfer funds for terrorists. The relative anonymity afforded by these processes, their ability to circumvent banking regulations, and their increasing use around the world render them vulnerable to exploitation by terrorists and terrorist organizations.

1. Prevention

Abuse of alternative payment processes might be prevented, or at least diminished, by regulating vendors and requiring them to collect more information from their customers. Although the regulatory landscape with regard to new technologies such as alternative payment systems, e-currencies, and smartcard applications is not clearly defined by statute or case law, these systems seem to fall within the broad definition of "financial institution" set forth in 31 U.S.C. § 5312.[137] Still, a balance must be struck in regulating these new technologies.

One might argue that these services, which essentially perform the functions of a bank, should be subject to the same oversight and regulation. The counter-argument is twofold: (1) most of these systems interface with the banking system at some point, so there is no need for onerous record keeping by alternative payment companies; and (2) these companies thrive on low overhead and the administrative burden of, for instance, reviewing transactions and filing SARs would impose an additional transaction cost on vendors.

Similarly, one might argue that customers of such services should be required to provide the same information that banking customers provide – at least names, social security numbers, driver's license numbers, valid addresses and phone numbers. There is an obvious trade-off with this measure, too. Customers use these services in part because of the privacy and anonymity that they provide.

Nor would an appropriate regulatory regime be a panacea for misuse of such new technologies. The borderless fluidity of the Internet poses unique challenges for such regulations. Customers can easily conduct online transactions that cross international borders or access foreign financial services from an

[137] The statutory definition of "financial institution" appears to extend the Secretary of the Treasury's anti-money laundering and anti-terrorist financing regulatory authority to these new technologies. It includes both specific categories ("a dealer in precious metals, stones or jewels," § 5312(a)(2)(N); "a licensed sender of money or any other person who engages as a business in the transmission of funds," § 5312(a)(2)(R)) and catch-all provisions ("any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage," § 5312(a)(2)(Y); "any other business designated by the Secretary whose cash transactions havea high degree of usefulness in criminal, tax, or regulatory matters," § 5312(a)(2)(Z)). The definition also includes money services businesses, which FinCEN has defined to include providers of alternative payment and stored value services if those providers conduct more than $1,000 worth of transactions per day. *See* 31 C.F.R. § 103.11(uu). Although FinCEN's regulations require issuers, sellers, and redeemers of stored value to have anti-money laundering programs, they are not currently subject to other Bank Secrecy Act requirements.

Internet terminal located in the United States. Particularly when transactions span two or more regulatory jurisdictions, it can be difficult to differentiate legitimate from illegitimate transactions.

2. Investigation

To the extent that these new technologies interface with the Internet, opening accounts with them and using their services requires visiting a web site. If the company logs traffic on its web site and retains those logs (although in rare cases, such as those discussed above, companies proactively destroy business records to protect their customers' privacy, most of them retain logs so that they can investigate customers' claims of fraud or theft), it should, at the very least, have a record of the date, time, and IP address from which the account was accessed for every transaction. Law enforcement can obtain this information for both accounts that are party to a transaction, i.e., the payor and the payee. From this information law enforcement can in theory determine who accessed each account and participated in the transfer of value.[138]

3. Prosecution

The potential statutes under which a transfer of funds to a terrorist or terrorist organization may be prosecuted are the same regardless of the means used to transfer the funds. *See* Section III.A.3, above. If a suspect provides false registration information when opening an account, that individual might also be prosecuted under the wire fraud statute.[139]

IV. ELECTRONIC COMMUNICATIONS

Terrorists' use of the Internet to communicate with one another constitutes perhaps the most prevalent use of the Internet to facilitate the raising and moving of funds. Communication, of course, is protected in the United States by the First Amendment unless it is in furtherance of some criminal conduct. Thus, for instance, the First Amendment protects an individual who transmits, without doing more, the message, "I believe that the only way to curb the spread of American capitalism, and the spiritual vacuum that accompanies it, is by waging war against the United States." Communications are often more, however, than a passive ideological statement. They may be an incitement to imminent unlawful action or a threat, neither of which is protected by the First Amendment.[140] A conspiracy to commit unlawful acts may also be punished, even if communications are the strongest indicators that a conspiracy exists.[141] Similarly, communications regarding criminal conduct may constitute information essential to the prevention of, or evidence valuable to the investigation and prosecution of, such conduct and may be obtained with appropriate legal process.[142]

Terrorist organizations have established web sites to communicate regarding fund transfers. The most straightforward example of such communication is the listing on sympathetic web sites of accounts to which funds for various terrorist organizations can be transferred. For instance, the site http://www.ummah.net/jihad/support provided account numbers for the Al Rashid Trust at Habib Bank Limited, for Harkat ul Mujahideen at the Allied Bank

---

[138] In practice, this will depend on how long the ISP through which the customer accessed the Internet maintains information and whether it requires and confirms valid registration information.

[139] *See* 18 U.S.C. § 1343.

[140] *See* Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (holding that "the constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to produce such action."); *Planned Parenthood of the Columbia/Williamette, Inc. v. American Coalition of Life Activists*, 290 F.3d 1058, 1072 (9th Cir. 2002) (en banc) ("[W]hile advocating violence is protected, threatening a person with violence is not.").

[141] *See* Wisconsin v. Mitchell, 508 U.S. 476, 489 (1993) (noting that "[t]he First Amendment . . . does not prohibit the evidentiary use of speech to establish the elements of a crime or to prove motive or intent.").

[142] *See supra* note 72.

of Pakistan, and for Lashker Taiba at Faisal Bank Limited.

Many of the terrorists and terrorist organizations indicted or designated by the United States have communicated via e-mail. For instance, the indictment of four members of the Islamic Group alleges that computers were used "to transmit, pass and disseminate messages, communications and information between and among IG leaders and members in the United States and elsewhere around the world."[143] Similarly, six individuals indicted in 2002 in Oregon allegedly communicated via e-mail regarding their efforts to travel to Afghanistan to aid al-Qaeda and the Taliban in their fight against the United States.[144] Mukhtar al-Bakri, indicted in 2002 for training with al-Qaeda to wage war against the United States, allegedly e-mailed with co-conspirators to discuss and plan acts of terrorism.[145] Finally, four members of a Colombian terrorist organization indicted in November 2002, allegedly used e-mail to broker a guns-for-drugs deal.[146]

Terrorists may also pass PIN numbers, account passwords, or transfer instructions by e-mail, secure web sites, or chat rooms. Increasingly, value transfer through *hawala*, the traditional alternative remittance system that has provided value transfer to the people of the Middle and Far East for centuries, relies on e-mail communications between *hawaladars* around the world.[147] Although the vast majority of *hawala* transfers are legitimate (it is estimated that there are tens of millions of dollars transferred through *hawala* annually), experts believe that much of al Qaeda's funds for September 11, 2001 transferred through *hawalas* in Dubai and that terrorist organizations continue to use *hawala* to transfer funds.[148] *Hawala* provides a cheap, efficient, less well regulated means of moving money, particularly in and out of countries in the Far and Middle East.[149] The advent of e-mail as a preferred means of communication between *hawaladars* has at least one benefit – for the first time in the centuries-long history of this alternative remittance system, e-mail creates a record of transactions that law enforcement can obtain (or even intercept) to aid in an investigation.

Terrorists may be using sophisticated means of electronic communication to conceal their efforts to raise and move funds and to plan acts of violence. One common method is to provide the username and password of an e-mail account to all the members of a conspiracy. One member drafts, but does not send, an e-mail message. He then logs off (exits the e-mail account). His co-conspirators can log on from anywhere in the world, read the draft, and then delete it. Because the draft was never sent, the ISP does not retain a copy of it and there is no record of it travers-

---

[143] *See* Indictment, United States v. Sattar, No. 02-CRIM-395 (S.D.N.Y Apr. 9, 2002), available at http://news.findlaw.com/hdocs/docs/terrorism/ussattar040902ind.pdf.

[144] *See* Indictment, United States v. Battle, No. CR 02-399 HA (D.Or.) Oct. 2, 2002), available at http://news.findlaw.com/hdocs/docs/terrorism/usbattle100302ind.pdf.

[145] *See* Criminal Complaint, United States v. Al-Bakri, No. 02-M-108 (W.D.N.Y. Sept. 13, 2002), available at http://news.findlaw.com/hdocs/docs/terrorism/usal-bakri091302cmp.pdf.

[146] *See* Criminal Complaint, United States v. Varela, No. H-02-1008M (S.D.Tex.) Nov. 1, 2002), available at http://news.findlaw.com/hdocs/docs/terrorism/usromero110102cmp.pdf.

[147] *See* Patrick M. Jost & Harjit Singh Sandhu, *The Hawala Alternative Remittance System and its Role in Money Laundering* (noting that for communication between *hawaladars* "e-mail is becoming more and more common"); Christopher Blevins, U.S. Dep't of Treasury, *Hawala: Issues & Policy Implications* (2002) (same).

[148] *See* Karen DeYoung & Douglas Farah, *Infighting Slows Hunt for Hidden Al Qaida Assets; Funds Put in Untraceable Commodities*, WASH. POST, June 18, 2002, at A1.

[149] The USA PATRIOT Act amended the definition of "financial institution" to include informal value transfer systems such as *hawala*. *See* 31 U.S.C. § 5312(2)(R). As a result, *hawalas* operating in the United States must now establish an anti-money laundering program, register with FinCEN, and comply with record keeping and reporting requirements. Several foreign countries, such as United Arab Emirates and Saudi Arabia, now regulate *hawala* transactions, while other countries, such as India and Pakistan, have banned the practice of *hawala* altogether.

ing the Internet – it never went anywhere, its recipients came to it.

Another common method involves providing basic electronic mail services in conjunction with a terrorist-sympathizer web site. Imagine a secure web site www.jihad.com The web site supports basic e-mail services. An e-mail can be sent from one of its e-mail accounts (e.g., johndoe@jihad.com) to another (e.g., janedoe@jihad.com) without ever leaving jihad.com's servers. It cannot, therefore, be intercepted or tracked. In fact, United States intelligence and law enforcement will never know about it unless they obtain access to jihad.com's servers or records. In addition, terrorists may use encryption and steganography to conceal the content of electronic communications regarding raising and moving funds.

1. Prevention

One can no more prevent terrorists from communicating via the Internet than one can prevent them from communicating via telephone or regular mail. A regulation requiring ISPs to obtain and confirm valid subscriber information would discourage some such communications (and much of the other illicit conduct discussed in this Report). Such a measure would, however, deprive Internet users of a certain degree of privacy and anonymity and impose significant business costs upon ISPs. As a result of the delicate balance between law enforcement's need for valid identifying information and computer users' right to privacy, no consensus for such regulation has developed in the international community. Even if the United States established such a regulatory regime, therefore, terrorists could simply use mail servers based in other countries. Moreover, as noted above, a terrorist group could easily establish basic mail service capabilities on its own web site. In short, such regulation would limit the Internet's use as a global communication media, a forum for international commerce, and an educational resource without effectively preventing terrorists from communicating over the Internet.

2. Investigation

As noted in Section II.C.2, above, capacity to investigate terrorist communications over the Internet has increased appreciably over the last several years. Amendments to procedural and substantive laws, increased cooperation and capacity-building in the international community, and the development by federal, state, and local law enforcement of computer crime expertise, all have combined to enhance our efforts to investigate the use of the Internet by terrorists.

3. Prosecution

Before pursuing prosecution, law enforcement must again decide whether the benefit of prosecution outweighs the benefit of the information that might be gathered if prosecution is delayed and the terrorists are allowed to continue communicating so that law enforcement can continue to gather information. Once the decision has been made to prosecute individuals engaged in electronic communications as a means of soliciting material support for terrorist organizations, the individuals or organizations engaged in the communications may be prosecuted under the statutes prohibiting such solicitations, discussed in Section II.A.3, above.

IV. CONCLUSION

The Internet is undeniably one of the most significant technological advances of our era. Its prevalence and accessibility have revolutionized the ability of individuals and organizations all over the world to communicate, share and access information, and conduct transactions virtually instantaneously. It has created an efficient, borderless marketplace for the exchange of communications and ideas and for the transacting of business and financial affairs. This marketplace has been fertile ground for innovation, providing an infrastructure within which existing businesses can offer services with greater efficiency and convenience and new businesses can capitalize on the remarkable attributes of this new global network.

With this technological advance and these new opportunities, however, come new challenges. The very attributes that make the Internet an invaluable communication, educational, and business resource make it susceptible to abuse by criminals and terrorists. The challenge, then, for legislators and for regulatory and law enforcement agencies, is to preserve the attributes that make the Internet such a remarkable innovation –

the anonymity and privacy it offers users, the liberation from geographic boundaries, the speed-of-light efficiency, and the rarity of regulatory constraints – while at the same time making it less susceptible to criminal abuse.

The full weight of this challenge is implicated in the effort to curtail terrorist use of the Internet to raise and move funds. Terrorists and terrorist organizations take advantage of all of the Internet's uses (for communicating, for accessing and sharing information, and for transacting business) and avail themselves of all of its cardinal attributes (the anonymity achieved through false identifiers and through communications protected by encryption and steganography, the disregard of geopolitical boundaries, the speed of transactions and communications, and the paucity of regulations). They raise funds on the Internet by direct solicitation, by exploiting facially legitimate online charities and e-commerce companies, and by garnering the proceeds of online criminality. They move these funds through any of the panoply of traditional and alternative banking and other financial services offered online. And they use the Internet's communication applications to facilitate the raising and moving of funds. As Internet communication and business technologies evolve, so too will terrorists' use of the Internet to raise and move funds.

Several future steps in addressing the threat of online terrorist financing suggest themselves. Technological, investigative, and legal experts drawn from the regulatory, law enforcement, and intelligence communities should continue to take up legal and policy issues associated with terrorist abuse of the Internet to raise and move funds; coordinate efforts to prevent, investigate, and prosecute such abuse; and address new technological challenges as they arise. Acting in concert, such experts might also develop a uniform strategy to address existing problems, such as direct solicitation sites and the abuse of charity sites, and continue to encourage international outreach, in conjunction with existing bilateral cooperation and multilateral bodies, to our foreign partners in the effort to curb online terrorist fund raising and transfer. And they should continue to work with industry representatives to foster public-private cooperation in effectively preventing, investigating, and prosecuting terrorist use of the Internet to raise and move funds.

Appendix I

Money Laundering Defendants Sentenced in FY 2001 - Highlights

In FY 2001, there were 951 defendants convicted of money laundering as the primary guideline of conviction[150] representing nearly 1.6% of all defendants sentenced in the United States. Another 243 defendants also were convicted of money laundering offenses on other counts, totaling 1,194 defendants who were convicted of money laundering under any guideline of conviction.[151] For these additional defendants, other offenses, mostly drug trafficking and fraud offenses, yielded the highest sentence.

In 2001, 615 or 65% of all money laundering defendants were convicted of laundering monetary instruments (2S1.1); 121 (13%) were convicted of engaging in monetary transactions with property derived from specified unlawful activity (2S1.2); and 215 (22%) were convicted of structuring transactions to evade reporting requirements, failure to report cash or monetary transactions, failure to file currency and monetary instrument report, or knowingly filing false reports (2S1.3).

For the purpose of analyzing sentencing factors, this analysis focuses on the 736 defendants who were sentenced under 2S1.1 (laundering monetary instruments) and 2S1.2 (engaging in monetary transactions with property derived from specified unlawful activity) as primary guidelines of conviction. The attached tables present summaries for defendants sentenced under each of the three money laundering guidelines separately, as well as for the sum of defendants sentenced under the two main money laundering guidelines (2S1.1 and 2S1.2).

Characteristics and District Distribution (2S1.1 and 2S1.2)

About 46% (340) of money laundering defendants sentenced in FY 2001 were White, 30% (220) were Hispanic and 19% (141) were Black. The majority, 78% or 571 defendants, were U.S. citizens, 62% (455) were over 35 years of age, 76% (558) were high school or college graduates, and 80% (591) were male.

The five districts with the greatest number of money laundering defendants sentenced in FY 2001 collectively accounted for nearly a third of all money laundering defendants sentenced that year. These districts were: Florida Southern (55), New York Southern (47), California Central (46), Puerto Rico (40), and Florida Northern (37).

Sentencing (2S1.1 and 2S1.2)

In FY 2001, 90% (660) of all money laundering defendants pleaded guilty, and about 89% (653) received prison sentences – 89% of defendants sentenced under 2S1.1, 90% of 2S1.2, and 41% of 2S1.3. The greatest number, 442 or 60%, of money laundering defendants received one to less than five years of imprisonment and about 21% (151) received five to less than ten years of imprisonment. The majority, (59%) of defendants sentenced under 2S1.1 and 68% of those sentenced under 2S1.2 received one to less than five years of imprisonment.

The average length of imprisonment in FY 2001 was 52 months for defendants who received imprisonment, up from 50 months in 1997, and 46 months for all money laundering defendants. Substantial differences in the average length of imprisonment exist between defendants who received imprisonment under the three money laundering guidelines. On average, defendants sentenced under 2S1.1 received 54 months of imprisonment, defendants sentenced under 2S1.2 received 41 months, and defendants sentenced under 2S1.3 received 10 months.

[150] Defendants for whom money laundering convictions yielded the highest sentence under 2S1.1, 2S1.2, and 2S1.3.

[151] Defendants for whom money laundering convictions contributed to the sentence.

Approximately 56% (369) of all money laundering defendants were sentenced within the recommended sentencing guideline range, 33% (216) received downward departures for providing substantial assistance to the government, and 11% (70) received downward departures for other reasons. The most frequently cited reasons for departures were: the existence of general aggravating or mitigating circumstances, criminal history level over-represents the defendant's involvement, and family ties and responsibilities. The majority of money laundering defendants were sentenced at the minimum guideline range.

Aggravating/Mitigating Factors (2S1.1 and 2S1.2)

About 33% (204) of defendants sentenced under 2S1.1 were convicted of laundering $100,000 or less, 43% (266) of over $100,000 to $1 million, 19% (116) of over $1 million to $10 million, and 5% (29) of offenses exceeding $10 million.

About 28% (34) of defendants sentenced under 2S1.2 were convicted of transactions involving $100,000 or less, 42% (51) of over $100,000 to $1 million, 20% (24) of over $1 million to $10 million, and 10% (12) of transactions involving over $10 million.

About 42% (90) of defendants sentenced under 2S1.3 were convicted of offenses involving $70,000 or less, 46% (99) of over $70,000 to $350,000, 8% (18) of over $350,000 to $1.5 million, and 4% (8) of over $1.5 million.

The majority of defendants sentenced under 2S1.1, 47% or 288 defendants, and 17% or 21 defendants sentenced under 2S1.2 knew or believed that the funds were the proceeds of an unlawful activity involving the manufacturing, importation, or distribution of narcotics or other controlled substances. About 41% (87) of defendants sentenced under 2S1.3 and 74% (89) of defendants sentenced under 2S1.2 knew or believed that the funds were proceeds of unlawful activity or were intended to promote unlawful activity.

About 20% (125) of defendants sentenced under 2S1.1, 17% (21) under 2S1.2, and 5% (10) under 2S1.3 received aggravating role adjustments for their participation in the offense. About 58 (9%) defendants sentenced under 2S1.1, 9 under 2S1.2, and 2 under 2S1.3 received four additional sentencing levels for being a leader or organizer of five or more participants. About 29 (5%) defendants sentenced under 2S1.1, 5 under 2S1.2, and 2 under 2S1.3 received three additional sentencing levels for being a manager of five or more participants. About 38 (6%) defendants sentenced under 2S1.1, 7 under 2S1.2, and 6 under 2S1.3 received two additional sentencing levels for being a leader, organizer, manager, or supervisor.

Small percentages of money laundering defendants (4% under 2S1.1, 13% under 2S1.2, and 1% under 2S1.3) received two additional sentencing levels for abusing a position of trust, while 28 defendants had additional criminal history points applied for committing the offense less than two years after their release from prison.

About 75% (550) of all money laundering defendants sentenced in 2001 had criminal history category I. The majority (83% or 609) of all money laundering defendants received reductions for acceptance of responsibility – 79% (579) received a three-level reduction and 4% (30) received a two-level reduction. About 16% (116) of all money laundering defendants sentenced in 2001 received reductions ranging from two to four levels for their minor/minimal participation the offense.

Appendix J

International Asset Forfeiture Sharing
Payments To Other Countries

COUNTRY	JUSTICE FY89 - FY99 AS OF 4/30/99	TREASURY FY90 - FY99 AS OF 9/30/99	TOTAL SHARING FY89-9/99
Argentina	$162,852	$0	$162,852
Aruba	$0	$161,702	$161,702
Bahamas	$165,833	$342,000	$507,833
British Virgin Islands	$2,437,886	$0	$2,437,886
Canada	$2,402,844	$2,277,745	$4,680,589
Cayman Islands	$1,686,326	$682,980	$2,369,326
Colombia	$2,473,385	$0	$2,473,385
Costa Rica	$733,019	$0	$733,019
Ecuador	$4,264,700	$0	$4,264,700
Egypt	$51,240	$999,187	$1,050,427
France	$0	$2,000,000	$2,000,000
Guatemala	$816,176	$0	$816,176
Guernsey	$297,713	$145,045	$442,758
Honduras	$0	$139,720	$139,720
Hungary	$8,415	$0	$8,415
Isle of Man	$335,862	$0	$335,862
Israel	$69,725	$0	$69,725
Jersey	$0	$1,049,991	$1,049,991
Liechtenstein	$20,500	$0	$20,500
Luxembourg	$19,104,348	$0	$19,104,348
Mexico	$0	$6,030,750	$6,030,750
Netherlands Antilles	$22,500	$0	$22,500
Nicaragua	$0	$58,586	$58,586
Panama	$0	$39,971	$39,971
Paraguay	$70,000	$0	$70,000

Treasury Forfeiture Fund
Equitable Sharing To Foreign Countries

Fiscal Years 1990-1994

Country	FY 1990	FY 1991	FY 1992	FY 1993	FY 1994	TOTALS
Aruba	$0	$0	$0	$92,702	$0	$92,702
Canada	$1,500,000	$141,063	$186,177	$56,566	$116,658	$2,000,464
France	$0	$2,000,000	$0	$0	$0	$2,000,000
Mexico	$750	$0	$0	$0	$0	$750
Netherlands	$0	$0	$0	$0	$0	0
Nicaragua	$0	$0	$0	$0	$58,586	$58,586
Panama	$0	$0	$0	$0	$39,971	$39,971
Trinidad	$0	$0	$40,330	$0	$0	$40,330
United Kingdom	$0	$3,000,000	$0	$0	$0	$3,000,000
TOTALS	**$1,500,750**	**$5,141,063**	**$226,506**	**$149,269**	**$215,216**	**$7,232,803**

Treasury Forfeiture Fund
Equitable Sharing To Foreign Countries

Fiscal Years 1995-2003

Country	FY 1995	FY 1996	FY 1997	FY 1998	FY 1999	FY 2000	FY 2001	FY 2002	FY 2003	Totals
Aruba	$36,450	$0	$32,550	$0	$0	$0	$0	$0		$69,000
Australia									$44,958	$44,958
Bahamas	$342,000	$0	$0	$0	$0	$0	$0	$0		$342,000
Cayman Islands	$0	$0	$0	$682,980	$0	$2,680,803	$14,324	$9,061		$3,387,168
Canada	$67,260	$21,725	$130,525	$8,394	$42,119	$241,446	$640,778	$686,863	$706,909	$2,662,678
China	$0	$0	$0	$0	$0	$0	$0	$216,555		$216,555
Dominican Republic	$0	$0	$0	$0	$0	$63,885	$0	$0		$63,885
Egypt	$0	$0	$0	$0	$999,187	$0	$0	$0		$999,187
Guernsey	$0	$0	$145,045	$0	$0	$0	$0	$0		$145,045
Honduras	$0	$0	$0	$0	$139,720	$0	$0	$0		$139,720
Isle of Man	$0	$0	$0	$0	$0	$0	$0	$300,802		$300,802
Jersey	$0	$0	$1,049,991	$0	$0	$0	$0	$0		$1,049,991
Mexico	$6,030,000	$0	$0	$0	$0	$0	$0	$843,388		$6,873,388
Netherlands	$0	$0	$0	$0	$0	$1,717,213	$144,220	$64,407		$1,925,840
Nicaragua	$0	$0	$0	$0	$0	$0	$0	$0		$58,587
Panama	$0	$0	$0	$0	$0	$0	$0	$0		$39,971
Portugal	$0	$0	$0	$0	$0	$85,840	$0	$0		$85,840
Qater	$60,000	$0	$0	$0	$0	$0	$0	$0		$60,000
Switzerland	$79,992	$335,408	$0	$37,669	$938,576	$903,934	$0	$0		$2,295,579
United Kingdom	$670,049	$145,754	$17,784	$449,567	$739,225	$1,019,499	$279,443	$0		$3,321,321
TOTALS	**$7,285,751**	**$502,887**	**$1,375,895**	**$1,178,610**	**$2,858,827**	**$6,712,620**	**$1,078,765**	**$2,121,077**	**$751,867**	**$24,081,515**

Department of Justice Transfers to Foreign Countries
Summary of International Asset Sharing

Name of Case or Investigation	Recipient Country	Amount of Transfer	Transfer Date
Operation Polar Cap (S.D. Florida) DEA 21 U.S.C. 881	Canada Switzerland	$1,000,000.00 $1,000,000.00	01-Aug-89 01-Aug-89
In re Isle of Man (S.D. Florida) 21 U.S.C. 881	United Kingdom	$2,486,637.63	04-Dec-91
US v. $2,421,327.43 (N.D. Florida) 21 U.S.C. 881	Canada	$807,109.00	11-Dec-91
In re Isle of Man (S.D. Florida) DEA (D. Massachusetts)	B.V.I. B.V.I.	$640,730.45 $1,797,155.18	20-Dec-91 03-Apr-92
Transfer of $1,173,229 to the Cayman Islands W.D. La., S.D. Tex. M.D. Pa., S.D. Ind. D. Me., DEA - E.D.N.C. 21 U.S.C. 881	Cayman Islands	$1,173,229.00	13-Mar-92
Jose Rodriguez Gacha (M.D. Florida) 21 U.S.C. 881 (91-646-Ci v-J-10) Res'd for Colo. $12,279,348 (originally $18,104,348.00)	Switzerland Colombia Colombia Switzerland Isle of Man Luxembourg Colombia	$2,485,673.00 $900,000.00 $1,573,385.28 $1,421,667.20 $335,862.39 $18,104,348.00 $5,825,000.00	24-Mar-92 25-Feb-92 13-Nov-92 20-Nov-96 01-Jun-96 23-May-97 16-Dec-99
US v. $ 43 Million (D. of Puerto Rico) 21 U.S.C. 881	Venezuela	$1,384,845.00	24-Mar-92
US v. Taboada (D. South Carolina) FBI 21 U.S.C. 881	Switzerland	$93,751.00	10-Apr-92

Name of Case or Investigation	Recipient Country	Amount of Transfer	Transfer Date
In re Seizure of $100,000 (S.D. Texas) DEA 21 U.S.C. 881	**Paraguay**	$70,000.00	25-Jun-92
SDNY and 12 DEA Admin Cases DEA 1 - C.D. Cal. DEA 3 - E.D.N.Y. DEA 8 - E.D. La. 21 U.S.C. 881	**Guatemala**	$227,147.94	23-Jul-92
US v. $279,895 **US v. $733,988** (M.D. Florida) 21 U.S.C. 881	**Guatemala** **Guatemala**	$139,947.50 $146,797.60	23-Jul-92 23-Jul-92
Vessel named "Aguja" (S.D. Florida) DEA 21 U.S.C. 881	**Costa Rica**	$120,000.00	17-Aug-92
US v. $1,007,611 (W.D. Texas) 21 U.S.C. 881	**Guatemala**	$302,283.00	08-Oct-92
US v. $53,964 in Canadian Currency (W.D. New York) 21 U.S.C. 881(a)(1)(6)	**Canada**	$16,445.88	27-Aug-92
In re Seizure of $325,703, DEA No. 101156 (S.D. Florida) DEA	**Argentina**	$162,851.50	26-May-93
In re Seizure of $39,480 and $63,000 DEA Seizure Nos. 103598, 103599	**Egypt**	$51,240.00	check mailed 10-Aug-93
US v. Luytjes (M.D. Pennsylvania) 21 U.S.C. 881	**Switzerland**	$1,087,344.50	09-Sep-93

Name of Case or Investigation	Recipient Country	Amount of Transfer	Transfer Date
US v. Newton/Datz and Bloomfield (E.D. New York) 21 U.S.C. 881	Switzerland Switzerland	$8,183,626.10 $2,958,492.50	01-Oct-93 23-Nov-93
In re Seizures Nos. 120458 and 120461 (S.D. Florida) DEA 21 U.S.C. 881	Bahamas	$109,510.00	08-Oct-93
In re Seizure of $11,220 DEA Case No. GZ 90-0048 (US v Bacha, E.D. Va.) 21 U.S.C. 881	Hungary	$8,415.40	24-Feb-94
US v. Fernandez (M.D. Florida) 21 U.S.C. 881	Switzerland	$606,254.90	07-Mar-94
US v. McCarthy (N.D. Indiana) 21 U.S.C. 881	Canada	$64,324.96	15-Mar-94
US v. Michael LeBoss (W.D. Washington) 21 U.S.C. 881	Liechtenstein	$20,500.00	01-Apr-97 Check re-issued
US v. Kubosh (N.D. Texas) 21 U.S.C. 881	Cayman Islands	$422,387.87	19-Apr-94
In re $47,500 (Roizis) (S.D. N.Y.) DEA	Romania	$23,700.00	15-Jul-94
U.S. v. Hugo Reyes Torres Funds 21 U.S.C. 881 18 U.S.C. 981	Switzerland Ecuador Ecuador	$3,833,092.02 $3,833,092.02 $330,316.96	19-Sep-94 13-Oct-95 27-Jun-94

Name of Case or Investigation	Recipient Country	Amount of Transfer	Transfer Date
US v. Hickey (N.D. Indiana) S CR-86-91 (01)	Guernsey	$297,713.00	25-Oct-94
Fair Rose of Sharon DEA Case No. I991X019	Netherlands Antilles	$22,500.00	01-Nov-94
Seizure of $150,120 from Darrell Chambers DEA Case No. I7930033 (E.D. Michigan)	Bahamas	$56,323.00	14-Nov-94
US v. $2,146,084.56 (M.D. Florida) 21 U.S.C. 881	Switzerland	$1,073,042.00	23-Dec-94
Operation Softshoe Administrative Forfeitures FBI - N.D.Cal.	Canada Canada Canada	$27,907.77 $19,878.66 $10,150.60	21-Jun-95 17-Jun-96 30-May-97
David Shmuel (D. Mass., N.D. N.Y.)	Israel	$34,769.55	27-Jun-95
Ancaleto Case DEA Case No. MK84Z004 (D. Col.)	Canada	$13,509.94	26-Oct-95
Alarcon Mengual Case (N.D. Florida)	Switzerland Canada Switzerland Canada	$679,696.62 $135,919.12 $1,365,409.82 $136,526.58	26-Oct-95 24-Jan-96 18-Nov-96 28-May-98
US v. Herberto Rodriguez (N.D. Florida)	Switzerland Canada	$1,417,786.26 $51,302.11	30-Nov-95 05-Jun-96
The Ayala Brothers DEA case No G1-93-0356 S.D. Fla.	Ecuador	$51,345.00	10-May-96
Santa Cruz Londono (E.D. N.Y.)	United Kingdom Luxembourg	$523,392.44 $1,000,000.00	15-Dec-95 08-Mar-96

Name of Case or Investigation	Recipient Country	Amount of Transfer	Transfer Date
U.S. v. Michael J.P. Green S.D. Fla., C.D. Cal.	**United Kingdom**	$529,507.96	17-Jul-96
U.S. v. Real Property Five Civil Forfeiture cases (M.D. Fla.) Derrick Walpole	**United Kingdom**	$463,596.76	17-Jul-96
U.S. v. Midvale Development Corp. et al. (W.D. Wa.) 18 U.S.C. 981	**Cayman Islands**	$12,470.87	31-Oct-96
U.S. v. $33,967.00 in United States Currency (C.D. Cal.) USPS case	**United Kingdom**	$8,940.81	03-Dec-96
In re Seizure of $460,000 from Narko Tettegah DEA Case #C1-95-0113 S.D. N.Y.	**United Kingdom**	$68,922.15	06-May-97
U.S. v. All monies, etc. in Swiss Bank Corp. London (E.D. Texas) Martinez	**United Kingdom** **Cayman Islands**	$175,316.22 $58,438.74	29-Sep-97 13-May-98
US v 220 NW 132 Ave. Miami Tellechea, S.D. Fla.	**Canada**	$74,518.04	16-Dec-97
Jose Roberto Martinez DEA Administrative case (S.D. Fla.)	**Cayman Islands**	$19,800.00	13-May-98
M/V Pegasus DEA Administrative case No. CT 92Z001 (S.D.N.Y.)	**Ecuador**	$49,946.00	06-Apr-98
U.S. v. Montalbo, et al., Case No. 95-0142-Cr. and	**Costa Rica**	$428,920.50	23-Jun-98
U.S. v. Premises and Real Property, etc. (Efraim)	**Israel**	$34,954.52	10-Aug-98

Name of Case or Investigation	Recipient Country	Amount of Transfer	Transfer Date
US v. Stephen Lloyd Chula Cr. Case No. 94-0669-B DEA (S.D. California)	Costa Rica	$184,098.50	14-Oct-98
Jorge Luis Cantieri FBI Admin. forfeiture Case No. 3010-84-F-139	Canada	$14,338.15	03-Dec-98
Ives Charest DEA Admin. forfeiture Case No. C7970084	Canada	$24,887.50	03-Dec-98
US v. Julio Nasser David, et al. Case No. 94-131-CR (SDFL)	Switzerland Switzerland Switzerland Switzerland Switzerland	$89,016,022.00 $4,554,086.00 $245,464.18 $1,499,980.00 $2,379,330.00	18-Dec-98 23-Dec-99 23-Oct-00 18-Apr-02 12-July-02
Daniel Berger DEA Admin. forfeiture Case No. GH960118 (CD. Cal)	Switzerland	$107,161.13	05-Feb-99
Walter Furst Admin. Forfeiture Case No. R1960625 (CD. Cal)	Switzerland	$10,630.43	05-Feb-99
Farina (D.Col.) U.S v. $1,814,807.93 Case No. 97-S-1928	United Kingdom Hong Kong S.A.R.	$181,466.89 $907,403.00	03-Jun-99 21-Jun-00
Operation Dinero (N.D. Ga) U.S. v. $295,375,28 No. 1:94-CV-3340-AC U.S. v. $3,531,149.00 No. 1:95-CV-0153-AC	United Kingdom Anguilla	$229,517.39 $328,528.99	03-Jun-99 24-Aug-99
Luz Mary Durango DEA Admin. Forfeiture Case No. C1960051	Ecuador	$14,327.50	18-May-99

Name of Case or Investigation	Recipient Country	Amount of Transfer	Transfer Date
U.S. v. Midkiff DEA and D of Oregon Drug money laundering case	Switzerland	$226,447.88	24-Jul-00
U.S. v. Haddad DEA and SDTexas Drug trafficking	Canada	$37,809.97	02-Aug-00
U.S. v. Esquivel DEA/Admin Fft and SDFL CS Payment Drug trafficking	Ecuador	$14,850.00	22-Aug-00
Phan Case/ DEA Admin 21 U.S.C 881 ND GA	Thailand	$19,144.00	09-Nov-00
U.S. v. All Funds, Securities, etc., 18 U.S.C. § 981(i) Blair Down USPIS and W.D. Wa.	Barbados	$100,000.00	27-Dec-00
U.S. v. Barnette 18 U.S.C. § 981(a)(1)(A) FBI and USAO MD Fla	United Kingdom	$612,500.00	28-Dec-00
Greenberg / DEA Admin Seattle, WA and LA, CA 21 U.S.C 881 12,500 shared directly with RCMP	Canada	$89,129.62	05-Mar-01
U.S. v. Fuqua Mobile Home (Francine Corbeil-For. Bank Fraud) FBI and USAO SD Fla	Canada	$31,653.89	22-Mar-01
Luis Cano/DEA/SDFLA 21 U.S.C. 881	Dominican Republic	$1,139,399.77	02-Apr-01
US v. $393,892.66 (Op. Green Ice) DEA and SD Cal 881 (e)	Cayman Islands	$146,874.34	11-May-01
US v. Eric Howard Wells (N. Minn.) DEA Seizure Nos. 115499 and 186868	South Africa	$11,044.57	22-May-01
U.S. v. Frederick Taft et al. (E.D. PA)	Canada	$151,794.92	15-June-01

Name of Case or Investigation	Recipient Country	Amount of Transfer	Transfer Date
U.S. v. Jafar Rayhani (CV 95-8694-RMT and CV- 96-1595-RMT) CDCA	**Turkey**	$264,846.42	07-Feb-02
US v. Gammella (CR No. 96-083T) Dist. of RI	**Canada**	$200,377.58	08-Mar-02
US v. Ned K. Schroeder (No. 94-Cr-161) E.D. Wisc.	**Canada**	$7,704.36	08-Mar-02
DEA Case No. I2-95-0080 (Henderson)	**Canada**	$14,334.00	08-Mar-02
U.S. v. M/V Bulk Princess Case No. 00-7459-CIV (SDFL)	**Greece**	$2,267,959.05	03-July-02
Wilhelm Koenig (Criminal No. 95-116 LH) Dist. NM	**Luxembourg**	$686,842.66	**17-Sept-02**
U.S. v. $155,750 in US Currency (Chochana) Civil No. 3:02CV1690 (Dist. Conn.)	**Switzerland**	$155,750.00	12-Sept-02
U.S. v. Richard Spence Case No. 95 Cr.380 (SDNY) - DEA	**Canada**	$323,642.20	27-Dec-02
DEA Case No. C1-97-0289 (Fischer)	**United Kingdom**	$29,761.72	14-Jan-03
US v. Claude Duboc (GCR 94-01009) (N.D. Florida)	**Hong Kong SAR**	$2,898,755.42	11-June-03
DEA Case No. G-5960172 (Melendez)	**Dominican Republic**	$10,000	Aug-03
TOTALS		**$181,727,532.85**	