Global Business & Development Law Journal

Volume 18 | Issue 2 Article 13

1-1-2005

Lost in Implementation: Financial Institutions Face Challenges Complying with Anti-Money Laundering Laws

Alan E. Sorcher
Securities Industry Association in Washington, D.C.

Lost In Implementation: Financial Institutions Face Challenges Complying With Anti-Money Laundering Laws

*Alan E. Sorcher**

TABLE OF CONTENTS

The world has changed greatly in the four years since the September 11th terrorist attacks. Heightened security checks at airports, threat levels, terror alerts in the United States, government watch lists, and terrorist attacks around the world are constant reminders of the new risks we face. Americans have grown more accustomed to the disruption and intrusions into our lives to help protect our safety.

The events of September 11th have particularly affected U.S. financial institutions. The attacks were a direct hit on the heart of New York's financial district and inflicted a terrible toll on the securities industry. Many innocent lives

* Mr. Sorcher is Vice President and Associate General Counsel for the Securities Industry Association in Washington, D.C. The Securities Industry Association ("SIA") brings together the shared interests of nearly 600 securities firms to accomplish common goals. SIA member firms (including investment banks, broker-dealers, and mutual fund companies) are active in all U.S. and foreign markets and in all phases of corporate and public finance.

were lost and operations were thrown into disarray. However, the industry showed remarkable resiliency by reopening bond markets only two days later, and the equity markets the following Monday. In the four years since the attacks, markets have returned to normal and financial institutions have undergone many operational and system changes to conduct business in a post-September 11th world.

The U.S. government has led the global campaign to tighten money laundering restrictions and crack down on terrorist financing. The watershed event in the United States was the passage of the USA Patriot Act of 2001[1] in the weeks after September 11th. The legislation, while aimed at giving the government new powers in the war on terrorism, imposes significant requirements on broker-dealers and other financial institutions well beyond traditional notions of anti-money laundering compliance. The long lasting implication for broker-dealers, banks, and other financial institutions is that they will be required to devote more resources than ever before to anti-money laundering efforts. A recent study reported that spending on anti-money laundering systems for banks increased an average of sixty-one percent in the past three years, and is expected to increase an additional forty percent over the next three years.[2]

International organizations, foreign governments, and foreign financial institutions have also stepped up efforts to combat terrorist financing and money laundering. While the U.S. government has led the effort to make terrorist financing a global priority, the Financial Action Task Force ("FATF"), the leading international organization that sets money laundering policy, has made several important steps. Additionally, the United Nations ("UN") and European Union ("EU") have also implemented several significant counter measures.

Despite the advances made in the past three years, money laundering and terrorist financing continue to be a significant problem. Estimates of the amount of money laundered each year are between two and five percent of the world's gross domestic product ("GDP"), or roughly between $590 billion and $1.5 trillion.[3] Regulators worldwide are now stepping up efforts to enforce money laundering laws. In the United States, much attention has been focused on the compliance failures at Riggs Bank, located in Washington, D.C. Riggs was assessed a $25 million penalty—one of the largest penalties for a violation of the Bank Secrecy Act. U.S. bank regulatory agencies have recently entered into written agreements with ABN Amro Holding N.V., HSBC Bank, and Standard Chartered Plc. for anti-money laundering compliance failures.

---

1. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Patriot) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter Patriot Act].

2. *See* KPMG, GLOBAL ANTI-MONEY LAUNDERING SURVEY 2004: HOW BANKS ARE UP TO THE CHALLENGE 5 (2004) [hereinafter KPMG].

3. Vito Tanzi, *Money Laundering and the International Financial System*, INT. MONETARY FUND (2005), *available at* http://www.imf.org/external/pubs/cat/doctext.cfm?docno=WPIEA0551996.

Enforcement actions have not been limited to the United States. The United Kingdom's ("U.K.") Financial Services Authority, the primary financial regulator, fined the Bank of Ireland $3.5 million for failing to take reasonable steps to detect several high-risk cash transactions. Additionally, in September 2004, Japan's Financial Services Agency ordered Citigroup to terminate its private banking operations for failing to implement procedures to prevent money laundering and other violations of the country's banking laws. More recently, AmSouth Bancorporation was assessed a $10 million penalty for anti-money laundering compliance failures.

Part I of this article will discuss the new requirements under the Patriot Act for U.S. financial institutions. The focus will be on the rules for securities firms, although the requirements for banks are largely the same. Part II will review significant international developments in anti-money laundering requirements. Discussion will center on the primary international groups responsible for money laundering policy. Lastly, Part III offers recommendations to improve anti-money laundering regulation.

I. U.S. ANTI-MONEY LAUNDERING REQUIREMENTS

The Patriot Act provisions are far reaching and will require new levels of compliance by all financial institutions.[4] The Patriot Act amends the Bank Secrecy Act, the principle U.S. statute imposing anti-money laundering compliance obligations on financial institutions. The Patriot Act focuses on expanding due diligence and monitoring requirements, enhanced reporting obligations, and financial intermediaries.[5] The requirements include anti-money laundering compliance programs, suspicious activity reporting, verification of new accounts, certain recordkeeping for "correspondent accounts" with foreign banks, special due diligence for correspondent and private banking accounts, and prohibition of correspondent accounts with foreign shell banks.

Since the passage of the Patriot Act, the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") and the federal financial regulators have drafted extensive implementing regulations. These regulations expand the categories of financial institutions that must possess basic anti-money

4. Prior to the passage of the Patriot Act, broker-dealers were subject to certain provisions of the Bank Secrecy Act that imposed reporting and record keeping requirements. Since 1970, securities firms have been required to report currency transactions in excess of $10,000 on a Currency Transaction Report ("CTR"). Similarly, these firms have been required to file reports relating to the physical transportation of currency or bearer instruments in amounts over $10,000 into or outside of the United States on a Currency or Monetary Instrument Transportation Report ("CMIR"). Since 1986, broker dealers, like other financial institutions, have been subject to the criminal provisions of the Money Laundering Control Act of 1986, Pub. Law No. 99-570 , 100 Stat. 3207 (1986) ("MLCA"). Among other things, the MLCA established two anti-money laundering criminal statutes that for the first time, made money laundering a crime in of itself. *See* 18 U.S.C. §§ 1956-1957 (2000).

5. *See* Written Testimony of David D. Aufhauser, before the Committee on Banking, Housing and Urban Affairs, Unites States Senate (Sept. 25, 2003) *available at* http://www.treas.gov/press/release/js760.htm.

laundering programs and report suspicious activity. Rules requiring anti-money laundering programs are in effect for banks, securities firms, futures commission merchants, introducing brokers in commodities, operators of credit card systems and money services businesses. These rules have also been proposed for investment advisors, commodity trading advisors, insurance companies, and hedge funds. Currently, depository institutions, broker-dealers, mutual funds, futures commission merchants and introducing brokers in commodities, casinos, and money services businesses are required to report suspicious activity. Analogous reporting rules have been proposed for insurance companies. The financial institutions that are required to establish customer identification and verification procedures include banks, savings associations, credit unions, certain non-federally regulated banks, broker-dealers, futures commission merchants and introducing brokers in commodities and mutual funds.

Anti-money laundering compliance will continue to be a focus for financial institutions as they grapple with new regulations and increased scrutiny from regulators. This will be true in the United States and abroad. Resources will flow towards account opening procedures, transaction monitoring, staff training, and external reporting requirements.[6]

A. *Anti-Money Laundering Compliance Programs*

The Patriot Act required broker-dealers to establish comprehensive anti-money laundering programs by April 24, 2002.[7] The National Association of Securities Dealers and the New York Stock Exchange (collectively referred to as SROs) issued rules that set forth the requirements for these programs.[8] The rules require: written internal policies, procedures, and internal controls to achieve compliance with the Bank Secrecy Act; the designation of a compliance officer; an ongoing employee-training program for appropriate personnel; and an independent audit by firm personnel or a qualified outside party to test the programs. These anti-money laundering programs must be approved by a member of senior management. The Securities and Exchange Commission ("SEC") also recognized that anti-money laundering compliance programs "will evolve over time" as firms find "new ways to combat money laundering and to detect suspicious activity." [9] The SROs' anti-money laundering program rules also require firms to establish reasonable procedures and internal controls to identify and report suspicious activity.

---

6. *See* KPMG, *supra* note 2.

7. Patriot Act, *supra* note 1, at § 352.

8. The NYSE (SR-NYSE-2002-10) and NASD (SR-NASD-2002-24) anti-money laundering rules were issued by the SEC on April 22, 2002. Rel. No. 34-4378.

9. *Id.*

B. Suspicious Activity Reporting

Recent press reports regarding money laundering compliance failures at Riggs National Bank brought much attention to the need for financial institutions to file suspicious activity reports ("SARs"). Riggs, a Washington, D.C. based bank that made its name by providing banking services to Washington's foreign embassies, was assessed a $25 million penalty for violations under the Bank Secrecy Act by the U.S. Department of the Treasury's Financial Crimes Enforcement Network.[10] The inquiry into Riggs began after the September 11th terrorist attacks, when government investigators were looking at Saudi Arabian accounts at the bank and discovered that Riggs failed to file numerous SARs.

Suspicious activity reporting is an important part of a firm's anti-money laundering program. The SARs rule for broker-dealers was issued on July 1, 2002 by FinCEN, under section 356 of the Patriot Act.[11] The rule, which took effect on January 1, 2003, applies to any broker or dealer located within the United States, and those firms registered as broker-dealers simply to permit the sale of variable annuities. The rule also applies to activities of futures commission merchants registered as broker-dealers that deal in securities products over which the SEC, or any federal agency other than the Commodity Futures Trading Commission, has authority.

A broker-dealer must report a transaction (of at least $5,000) if it is conducted or attempted by, at, or through the broker-dealer, and the broker-dealer knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions): (1) involves funds derived from illegal activity, or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity; (2) is designed, whether through structuring or other means, to evade the requirements of the Bank Secrecy Act; (3) has no business or apparent lawful purpose, or is not the sort in which the particular customer would be expected to engage, and the broker-dealer knows of no reasonable explanation after examining the available facts; or (4) uses the broker-dealer to facilitate criminal activity.[12] The reporting requirements apply even to transactions that do not involve currency.

Suspicious activity reports must be filed on a "SAR-SF" form with FinCEN. The SAR must be filed within thirty days of the broker-dealer becoming aware of facts that may constitute a basis for filing. If a firm is unable to identify a suspect,

---

10. In the Matter of Riggs Bank, N.A., Matter No. 2004-01(May 13, 2004). Riggs was also assessed a $25 million penalty by the U.S. Office of the Comptroller of the Currency. However, Riggs is only required to make one payment of $25 million to the Department of Treasury. Department of the Treasury Financial Crimes Enforcement Network. *Id.*

11. Prior to the Patriot Act, all broker-dealers that were subsidiaries of bank holding companies were required to file SARs. In addition, many other broker-dealers, particularly the larger firms, filed SARs voluntarily, even though they were under no legal obligation to do so.

12. Financial Crimes Enforcement Network (FinCEN), 66 Fed. Reg. 67,670 (to be codified at 31 C.F.R. pt. 103 (2001)).

filing may be delayed for an additional thirty days in order to identify a suspect. In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, the broker-dealer must immediately notify the appropriate law enforcement agency by telephone in addition to filing a SAR.

The rule requires firms to maintain copies of all SARs filed and the original supporting documentation for five years from the date of the filing. In addition, the supporting documentation must be made available to law enforcement or authorized regulatory agencies and the SROs to ensure compliance with the rule.

Firms that file a SAR are prohibited from notifying any person involved in the transaction of the SAR filing. This prohibition does not apply to requests from law enforcement or regulatory agencies.[13] Lastly, firms are protected from liability for reporting suspicious activity and for failing to disclose such reporting.[14]

C. *Customer Identification and Verification*

The United States Department of the Treasury and the SEC issued final rules on May 9, 2003, requiring broker-dealers to establish procedures to verify the identity of new accountholders, which is one of the most significant Patriot Act provisions.[15] Similar rules were also issued by other federal regulatory agencies for banks, credit unions, mutual funds, futures commission merchants, and introducing brokers.

The rules require a broker-dealer to adopt a written Customer Identification Program ("CIP") appropriate for its size and business, enabling it to form a reasonable belief that it knows the true identity of the customer. The CIP must be part of a firm's overall anti-money laundering compliance program required under section 352 of the Patriot Act. A firm's program should be based on the institution's assessment of the risks presented (e.g., its size, location, customer base, types of accounts and transactions, methods of opening accounts, and types of identifying information available). The CIP must include risk-based procedures for verifying the identity of each customer if reasonable and practicable, as described more fully below.

Firms are required to have procedures for opening an account that specify the identifying information required from each customer. Firms are required, at a minimum, to obtain the following information prior to opening an account: (1) name; (2) date of birth (for individuals); (3) residential or business street address for individuals, or principal place of business, local office or other physical location for persons other than individuals; and (4) identification number – for a

13. 31 U.S.C. § 5318(g)(2) (2005).

14. *Id.* § 5318(g)(3).

15. *See* Patriot Act, *supra* note 1, § 326.

U.S. person, a taxpayer identification number ("TIN"); for a non-U.S. person, a TIN, a passport number and country of issuance, an alien identification card number or the number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard. Firms may have procedures for opening an account for a customer that has applied for, but not received, a taxpayer identification number.

Broker-dealers are required to have procedures for verifying the identity of each customer within a reasonable amount of time before or after the account is opened. The CIP must specify when the institution will verify a customer's identity through documents, including identifying the documents that will be used, and when the firm will verify through non-documentary methods, or a combination of both. Non-documentary methods may include contacting the customer, comparing information from the customer with information from a consumer reporting agency, public database, or other source, and checking references. The CIP must also address situations when the broker-dealer should not open an account, when an account should be closed because the firm is unable to verify the customer, and when a SAR should be filed.

A firm must also have procedures for making and maintaining records of all information obtained in verifying a customer's identity. The records must include all identifying information about the customer and a description of any original document relied upon in verifying identity. The records must also include a description of the methods and results of any measures undertaken to verify the customer's identity, including the resolution of any discrepancies discovered. Identifying customer information must be maintained for five years after the account is closed. In addition, records relating to how a firm verified the identity of a customer must be maintained for five years after the records are made.

The rules also require financial institutions to adopt procedures for determining whether a customer appears on any list of known or suspected terrorists or terrorist organizations issued by any federal government agency and designated as such by the Treasury in consultation with the federal functional regulators. Firms will receive notification regarding the lists that must be consulted for purposes of this provision. Procedures must also ensure that the institution follows all federal Directives issued in connection with such lists. Firms must also have procedures for providing customers with adequate notice that the institution is requesting information to verify their identities. The final rule includes sample language that a firm may follow.

D. Correspondent and Private Account Due Diligence

Of all the rules rolled out by the Treasury, those that perhaps may impose the greatest burden—at least on those firms with substantial international clientele—are the due diligence procedures under section 312 of the Patriot Act to detect

money laundering for private banking accounts and corresponding accounts for aliens and offshore banks.[16] The proposed rule requires "covered financial institutions" to establish: (1) due diligence policies, procedures, and controls to detect money laundering through correspondent accounts with foreign covered financial institutions; (2) enhanced due diligence policies, procedures, and controls for correspondent accounts for certain foreign banks with offshore banking licenses, and for all banks licensed by jurisdictions that have been determined to pose a high risk of money laundering; and (3) due diligence policies, procedures, and controls for accounts for foreign "private banking" clients, including "senior foreign political figures."[17]

The Treasury's proposed rule defines a "correspondent account" and a "foreign financial institution" so broadly that the rule could be interpreted to cover virtually *all* accounts U.S. financial institutions have with foreign financial institutions. For example, correspondent accounts are defined as accounts that "receive deposits from, make payments on behalf of . . . or handle other financial transactions" for a foreign financial institution.[18] Because the broad definitions in the proposed rule cover an array of accounts used to conduct ordinary business transactions with foreign financial institutions, U.S. institutions would thus be expending resources on accounts that do not raise "red flags."

In response to issues raised by the SIA and others in comment letters, the Treasury postponed the issuance of a final rule under section 312. Instead, the Treasury issued an interim rule advising firms of their compliance obligations until the issuance of a final rule. Under the interim rule, broker-dealers are required only to comply with the enhanced due diligence requirements for private banking clients.[19] For private banking accounts that meet this definition, pending the adoption of a final rule, the interim rule provides that firms should focus on those accounts that present a high risk of money laundering. The due diligence for these accounts should be consistent with guidance for private banking issued by the Federal Reserve and the Treasury.

E. Shell Bank Prohibitions

The rule regarding foreign shell banks implements two key provisions (sections 313 and 319(b)) of the Patriot Act. Section 313 prohibits U.S. financial institutions from providing correspondent accounts to foreign shell banks, and requires them to take reasonable steps to ensure that correspondent accounts are

16. 67 Fed. Reg. 37,736 (May 30, 2002) (implementing section 312 of the Patriot Act and proposed on May 30, 2002).

17. 67 Fed. Reg. 37,743 (May 30, 2002).

18. 67 Fed. Reg. 37,742 (May 30, 2002).

19. 67 Fed. Reg. 37,738 (May 30, 2002). A private banking account is defined as an account of at least $1 million, for one or more individuals who have a direct or beneficial interest in the account, and managed by an officer, employee or agent of a financial institution "acting as a liaison between the financial institution and the direct or beneficial owner of the account." *Id.*

not used indirectly for foreign shell banks. Section 319(b) requires financial institutions that provide correspondent accounts to foreign banks to keep records of the foreign banks' owners and agents, who will accept service of legal process in the United States.

The final rule provides that a broker-dealer:

> Shall not establish a correspondent account in the United States for, or on behalf of, a foreign shell bank;
>
> Take reasonable steps to ensure that any correspondent account established by a broker-dealer in the United States for a foreign bank is not being used by the foreign bank to indirectly provide banking services to a foreign shell bank;
>
> Maintain records—for all correspondent accounts in the United States for a foreign bank—that identify the owners of each foreign bank whose shares are not publicly traded and the foreign bank's U.S. agent authorized to accept service of legal process.[20]

Firms are permitted to use a certification form, provided in the rule, to comply with the shell bank prohibition, and the requirement to identify a foreign bank's owners and agent for service of process.[21] The certification must be obtained at least once every three years.[22] Firms have thirty days from when an account is opened to obtain the certification. If a certification is not obtained within the required time, a broker-dealer must close all correspondent accounts with the foreign bank within a commercially reasonable time.

F. Sharing of Information

The Treasury issued a final rule under section 314 of the Patriot Act, which is aimed at encouraging greater cooperation among financial institutions, regulators, and law enforcement in efforts against money laundering and terrorism financing.

Under the rule, FinCEN, acting on behalf of a federal law enforcement agency investigating money laundering or terrorist activity, may require any financial institution to search its records to determine whether the financial institution maintains or has maintained accounts for, or has engaged in transactions with, named individuals, entities, or organizations. Firms must search their records for any current account and any account maintained for a named suspect during the preceding twelve months. A firm is required to search

---

20. 31 C.F.R. § 103.177(a) (2005).
21. *Id.* § 103.177(b).
22. *Id.*

for transactions that are required to be recorded and are conducted during the preceding six months by, or on behalf of, a named suspect.[23] This process has resulted in 607 Grand Jury subpoenas, 129 Administrative subpoenas or summons, 1,285 new counts identified, and eleven search warrants.[24]

The rule also establishes procedures for voluntary information sharing between or among financial institutions. The sharing of information must be for the purpose of identifying and reporting activities that may involve money laundering or terrorist activity. A firm that shares information pursuant to the rule is protected under the Patriot Act from any liability for such sharing, or for any failure to provide notice of such sharing.

A financial institution that intends to share information under the rule must file a notice with FinCEN using the form set forth in the rule. An institution is required to submit a new form to FinCEN each year, and must take reasonable steps to verify that the institution with which it intends to share information has also filed the required notice with FinCEN. FinCEN maintains a list of institutions that have submitted the required notice and are thus qualified to share information.

G. *Office of Foreign Assets Control*

Although not under the Patriot Act, financial institutions are also prohibited under U.S. law from entering into transactions with "Specially Designated Nationals and Blocked Persons." These prohibited transactions come under the jurisdiction of the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC").[25]

OFAC administers and enforces U.S. economic and trade sanctions against targeted foreign countries, terrorism sponsoring organizations, and international narcotics traffickers. At present, OFAC administers comprehensive sanctions and embargo programs involving Cuba, Iran, and Sudan.[26] OFAC also enforces prohibitions against transactions with designated terrorists, Foreign Terrorist Organizations, and named foreign persons who engage in activities related to the proliferation of weapons of mass destruction. OFAC acts by imposing controls on transactions and freezing foreign assets under U.S. jurisdiction. OFAC's actions are authorized pursuant to presidential wartime and national emergency powers and specific legislation.

---

23. U.S. TREASURY DEPARTMENT, FINANCIAL CRIME'S ENFORCEMENT NETWORK, 314(A) FACT SHEET (2004). Through September 2004, 340 (of which 123 related to terrorist financing and 217 related to money laundering) requests have been processed under the Patriot Act § 314(a) by ten different Federal agencies. *Id.* These requests identified 2,402 subjects. In responding, financial institutions had 16,405 positive matches and 797 inconclusive matches. *Id.*

24. *Id.*

25. OFAC is within the Office of Terrorism and Financial Intelligence in the Treasury Department. Information about this agency is *available at* http://www.treas.gov/offices/enforcement/ofac/.

26. OFAC also administers several additional programs of lesser scope or severity than these programs. *Id.*

OFAC regulations apply to all financial institutions in the United States and require the identification of any transaction and property subject to a U.S. sanction. OFAC regulations also apply to all U.S. citizens and permanent resident aliens, wherever they are located, entities and organizations located in the United States, and overseas branches and subsidiaries of U.S. companies. Financial institutions must "block" or "freeze" accounts, assets, and obligations of blocked entities and individuals. Financial institutions must report such blockings within ten days to OFAC and file a comprehensive annual report on blocked property. Securities firms are also prohibited from dealing in securities issued from targeted countries and governments.

OFAC administers a master list of "Specially Designated Nationals and Blocked Persons" that targets members of foreign government regimes and networks of companies or other entities whose activities are inimical to the United States. Financial institutions are prohibited from conducting transactions, providing services, or having other dealings with persons or entities designated as such.

In combating terrorist financing, the Treasury may designate terrorist organizations as Foreign Terrorist Organizations under the President's Executive Order 13224. Those on the terrorist list are known as Specially Designated Global Terrorists or Specially Designated Terrorists. With respect to drug trafficking, the Treasury acts under the authority of the Foreign Narcotics Kingpin Designation Act and the International Emergency Economic Powers Act to administer and enforce the provisions of law relating to the identification and sanctioning of major foreign narcotic traffickers. These persons are known as Specially Designated Narcotics Traffickers.[27]

II. INTERNATIONAL DEVELOPMENTS IN ANTI-MONEY LAUNDERING REQUIREMENTS

A. Financial Action Task Force on Money Laundering

The Financial Action Task Force on Money Laundering is the intergovernmental organization dedicated to developing international money laundering standards. FATF was established in 1989 by the G-7 summit in Paris. FATF's primary purposes develop and promote policies to combat money laundering and the financing of terrorism.

FATF monitors members' progress in implementing anti-money laundering measures, reviews money laundering, terrorist financing techniques and counter measures, and lastly, promotes the adoption and implementation of anti-money laundering measures globally. FATF coordinates with other international bodies

27. The U.S. Department of Treasury identifies targets in cooperation with the Drug Enforcement Administration and the Narcotics and Drug Section of the Department of Justice.

in performing its mission. FATF functions as informal bodies of experts, thus, its policies do not have any directly binding legal force.

The number of FATF member-states has increased since 1990 from the original sixteen members to now include thirty-one countries and territories from North and South America, Europe, and Asia, and two regional organizations (the Commission of the European Union and the Gulf Cooperation Council).[28] There are also several FATF-style regional bodies, which strengthen FATF's approach and spread standards to non-members countries.

As part of a plan to help member countries fight money laundering, in 1990 the FATF issued its Forty Recommendations on Money Laundering ("Forty Recommendations"). The Forty Recommendations represent the international standard for anti-money laundering principles and have been endorsed or adopted by many international bodies.

Although not binding, the Forty Recommendations have been implemented by many nations throughout the world. They include recommendations that countries: criminalize the laundering of illicit proceeds of criminal activity; require financial institutions to develop anti-money laundering programs and report suspicious activity; exchange information with other countries relating to suspicious transactions; encourage cooperative investigations among the various countries; and recognize money laundering as an extraditable offense.

The Forty Recommendations were initially revised in 1996 to reflect changes in money laundering trends. In 2003, FATF completed a thorough revision of the Forty Recommendations after reviewing comments from countries, the financial sector, and other interested parties.[29] The review sought comment on whether changes were needed on customer due diligence, suspicious activity reporting, beneficial ownership, and the application of anti-money laundering obligations to non-financial businesses and professions. FATF has also issued Interpretive Notes that clarify certain of the Forty Recommendations.

In 2000, FATF developed its Non-Cooperative Countries and Territories ("NCCT") program to determine those jurisdictions that undermine the global effort to combat money laundering. The goal of the program is to reduce the vulnerabilities of the international financial system to money laundering by ensuring that all countries adopt and implement systems to counter money

---

28. The Member States of FATF are: Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, European Commission, Finland, France, Germany, Greece, Gulf Co-operation Council, Hong Kong, China, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, Kingdom of the Netherlands, New Zealand, Norway, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, and United States.

29. *See* Letter from SIA, the Futures Industry Association and the Investment Company (Aug. 30, 2002), *available at* http://www.futuresindustry.org/downloads/regulatory/FATFpaper.doc. The Securities Industry Association submitted a comment letter with two other trade groups making a number of suggestions on how the FATF's Forty Recommendations, which are tailored primarily for the banking industry, could be revised for the securities and related industries. One suggestion was to recognize the importance—in appropriate circumstances—of relying on intermediaries to perform due diligence. *Id.*

laundering. In February 2000, FATF published its initial report on NCCTs that established twenty-five criteria for determining NCCTs falling into these four categories: loopholes in financial regulations; obstacles raised by other regulatory requirements; obstacles to international cooperation; and inadequate resources for preventing and detecting money laundering activities. After a review, in June 2000, FATF published its first list naming fifteen jurisdictions as NCCTs.[30]

In determining whether jurisdictions should be removed from the NCCT list, FATF must make a determination that the previously identified deficiencies have been addressed. In general, the jurisdiction must have enacted legislation and regulations, and the regulations must be implemented and enforced. In 2002, eight jurisdictions were removed from the list: Hungary, Israel, Lebanon, St. Kitts and Nevis, Dominica, Marshall Islands, Niue, and Russia. Since then, other jurisdictions have been removed. Today the list includes Mynamar, Nauru and Nigeria.[31]

After the September 11th attacks, the United States and other countries called for an immediate worldwide effort to prevent the use of the international financial system to finance terrorism. At a special plenary session held on October 29-30, 2001, FATF expanded its focus beyond money laundering to include efforts to combat terrorist financing. FATF issued Eight Special Recommendations on Terrorist Financing,[32] which are the new international standards for combating terrorist financing.

The Eight Special Recommendations on Terrorist Financing call on countries to, among other things: implement UN resolutions relating to terrorist financing; criminalize the financing of terrorism, terrorist acts, and terrorist organizations; freeze funds or other assets of terrorists; require financial institutions and other businesses to report any suspicious activity where it appears that funds are connected to terrorist activities; and ensure that entities, especially non-profit organizations and charities, cannot be misused to finance terrorism.[33]

FATF monitors member countries in implementing the FATF recommendations through self-assessments and mutual evaluations. The self-assessment process involves each member providing information each year on a standard questionnaire that is addressed to their level of compliance. FATF then analyses and compiles this information and makes an assessment as to the extent the recommendations have been implemented by individual countries and by FATF as a group. Through the mutual evaluation process, each country is examined by

---

30. The report named the Bahamas, Cayman Islands, Cook Islands, Dominica, Israel, Lebanon, Liechtenstein, Marshall Islands, Nauru, Niue, Panama, Philippines, Russia, St. Kitts and Nevis, and St. Vincent and the Grenadines as having critical deficiencies in their anti-money laundering regimes or a demonstrated unwillingness to cooperate in anti-money laundering efforts.

31. Financial Action Task Force on Money Laundering, *Current List of Non-Cooperative Countries and Territories, available at* http://www.oecd.org/fatf/ncct_en.htm (last visited Sept. 12, 2005).

32. Financial Action Task Force on Money Laundering, *Annual Report, available at* http://www.oecd.org/dataoecd/13/1/34328160.pdf.

33. *Id.* at 8.

the FATF during an on-site visit conducted by a team of experts from other member countries. A report is then prepared assessing the extent to which the country has implemented an effective system to counter money laundering. For those members not in compliance, FATF's policy is to undertake a graduated approach through peer pressure put on member governments aimed at convincing them to tighten their systems.

FATF has also adopted a best practices paper for combating the abuse of non-profit organizations. [34] At its October 2004 session, the FATF is likely to approve international standards on cash couriers who carry money across borders to finance terrorism.[35]

B. *European Union*

The EU's efforts to combat money laundering were launched in 1991. In June of that year, the Commission of the European Community ("Community") published its first Directive (Directive 91/308/EEC) aimed at preventing the use of the financial system for money laundering purposes. The Community's 1991 Directive, which closely followed FATF's Forty Recommendations and the recommendations of other international groups, regarded anti-money laundering regimes principally as a tool to combat illegal narcotics trafficking. The Directive, among other things, obliged financial institutions to identify their customers, keep various records, establish certain policies and procedures, and report to relevant authorities suspicions of money laundering activities. The Directive is binding, and those EU Member States that fail to comply can be compelled through the legal process to bring their systems in line.[36]

Despite the 1991 Directive, concerns surfaced that the problem of money laundering was growing within the EU and that the focus of the 1991 Directive on illegal drug-related activities was too narrow. In 1998, the Commission issued a report recommending an expansion of existing anti-money laundering measures.[37] Reform efforts culminated in the adoption of a new Directive in the fall of 2001, soon after the terrorist attacks on the World Trade Center and the Pentagon.

The 2001 Directive (Directive 2001/97/EC), which amended the 1991 Directive, covered a wider range of predicate or underlying criminal offenses, including organized criminal activities and corruption. This action conformed to recommendations made by the FATF in the late 1990s. The 2001 Directive also

---

34. FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING, COMBATING THE ABUSE OF NON-PROFIT ORGANIZATIONS: INTERNATIONAL BEST PRACTICES (SPECIAL RECOMMENDATION VII) (2002).

35. *FATF Expected to Approve International Standards on Cash Couriers*, BNA, INC. DAILY REPORT FOR EXECUTIVES (October 1, 2004).

36. Directive 91/308/EEC, *available at* http://europa.eu.int/index_en.htm.. The EU Directives provide the EU Member States with a detailed set of mandatory measures to take against money laundering. *Id.*

37. *See* Second Commission Report to the European Parliament and Counsel on the Implementation of the Money Laundering Directive, COM(98)401.

expanded the range of institutions that were subject to due diligence and suspicious activity reporting requirements. The 2001 Directive more clearly covered currency exchange offices and money transmitters than the 1991 Directive, and imposed anti-money laundering obligations on certain non-financial professionals, such as lawyers and accountants, when they engaged in financial and corporate transactions.

The EU also reacted swiftly to the events of September 11th by introducing measures against a terrorist threat. The measures included the Council Recommendation on Cooperation in the Fight Against the Financing of Terrorism (Joint Position of the Council of 27 December 2001). In addition, UN Security Council Resolutions 1267, 1333, and 1373 (against the Taliban and Osama bin Laden and other terrorists) were passed and applied by regulation within the framework of the Common Foreign and Security Policy.

On June 30, 2004 the Commission proposed a new Directive (the "Third Anti-Money Laundering Directive"), designed to supplant and replace the prior two Directives.[38] The new proposed Directive specifically covers terrorist financing and provides for more detailed customer identification and verification procedures. This will involve not only mandatory implementation of the new FATF Forty Recommendations, but will create clearer and more detailed regulations in order to ensure uniform and manageable implementation.[39]

The proposed Directive generally includes measures that are designed to keep EU laws in line with recommendations made in 2003 by the FATF.[40] The proposal contains forty-three separate articles, some of which are summarized below.

Article One defines money laundering specifically to cover terrorist financing. Article Two applies the Directive to a wide range of financial and non-financial intermediaries, including life insurance firms and trust and service companies (which are defined to include entities that provide incorporation, trustee, and other business formation and facilitation services). In addition, this Article makes clear that the Directive covers all persons trading in goods or services who accept cash payments above €15,000.

Article Seven of the proposed Directive sets forth risk-based due diligence procedures that institutions subject to the Directive must follow to "know their customers' and understand their customers" financial and business activities.

---

38. Press Release by European Commission, *Money Laundering: Commission Proposes to Update and Improve Directive*, (June 30, 2004), available at http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/04/832&language=en&guiLanguage=en.

39. *See Adoption of Anti-Money Laundering Directive Will Strike a Blow Against Crime and Terrorism*, (June 7, 2005) *available at* http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/682&format=HTML&aged=0&language=EN&gulLanguage=fr. Subsequent to the writing of this article, the Third Anti-Money Laundering Directive was adopted.

40. *See Proposal for a Directive of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purpose of Money Laundering, including Terrorist Financing*, COM(04)448.

These procedures require, among other things, taking "reasonable measures" to identify underlying beneficial owners and, where trust and other similar arrangements are involved, taking "reasonable measures to understand the ownership and control structures." Article Eight makes clear that due diligence efforts should be undertaken at the outset of the customer relationship and, for existing accounts, "at appropriate times . . . on a risk-sensitive basis."

Article Ten permits individual EU Member States to allow institutions that are covered by the Directive in those Member States to adopt simplified due diligence procedures in situations involving a reduced risk of money laundering. Article eleven requires enhanced due diligence procedures in certain higher risk situations, such as when a customer is not physically present for identification purposes. This article also prohibits correspondent relationships with shell banks.

Articles Twelve through Sixteen contain various provisions that allow institutions covered by the Directive to rely on other parties to carry out their due diligence obligations. In general, reliance is permitted when a customer has been referred by a third party that is subject to either (a) mandatory professional registration requirements, or (b) due diligence and recordkeeping requirements "equivalent to those laid down" by the Directive.

Articles Eighteen through Twenty-Four provide for suspicious activity reporting to appropriate authorities, and Article Twenty-Five prohibits informing customers or third parties when suspicious activities are reported. Articles Twenty-Six through Twenty-Nine generally establish a five-year recordkeeping requirement for documents and information covered by the Directive.

Article Twenty-Seven requires institutions covered by the Directive to apply customer due diligence and recordkeeping measures "at least equivalent" to those required by the Directive to their branches and majority-owned subsidiaries that are located in non-EU countries.

Finally, as to enactment of the proposed new Directive, under the Commission's legislative process, the proposed Directive will be sent to the European Parliament and the Council of Ministers, which scrutinize, amend, and adopt proposed legislation, such as this Directive. The Dutch Presidency of the Council has indicated that it intends to give priority to enacting this proposed Directive.[41]

C. *The United Nations*

Through the United Nations, the international community has made several significant initiatives aimed at money laundering and terrorist financing. The terrorist financing initiatives have occurred largely as a result of the September 11th attacks. A summary of significant United Nations' Convention Resolutions related to money laundering and terrorist financing follows.

---

41. *See supra* note 39.

On December 9, 1999 the UN General Assembly adopted the International Convention for Suppression of Financing of Terrorism.[42] The Convention requires states to criminalize the collection or provision of funds with the knowledge or intent that they be used to conduct certain terrorist activity. Article eighteen of the Convention encourages implementation of a number of FATF's Forty Recommendations on Money Laundering, including prohibiting accounts held by unidentified parties, verifying the identity of real parties to transactions, and obtaining proof of incorporation. Article eighteen also requires parties to cooperate in the efforts against terrorist financing by adapting their home legislation to prevent the commission of certain identified offenses. The Convention also encourages states to require financial institutions to: report complex or large transactions or unusual patterns of transactions that have no apparent lawful purpose; maintain records for five years; monitor the physical cross-border transfer of cash; and supervise money transmission agencies. The Convention also addresses the exchange of information.

The Convention entered into force on April 9, 2002. Sixty-four states had become parties to the Convention as of December 31, 2002 and seventy-five others had signed but not ratified the Convention. The United States became a party on June 26, 2002.

The UN Convention Against Transnational Organized Crime was the first legally binding multilateral treaty specifically aimed at transnational organized crime. The Convention opened for signature on December 12-14, 2000, in Palermo, Italy. The United States and 124 other countries became signatories. Article seven requires each state to establish comprehensive regulatory systems in order to deter and detect money laundering. The Convention also encourages each state to develop a financial intelligence unit to act as the center for the collection and analysis of information relating to money laundering.[43] Also required is cooperation among the parties, including the exchange of information, in the investigation and prosecution of money laundering offenses.

On September 28, 2001, the UN Security Council adopted Resolution 1373 requiring states to take specific action to combat terrorism.[44] The Resolution requires states to: (1) freeze, without delay, funds, financial assets, and other economic resources of any individuals or entities who participate in any way in the commission of terrorist acts; (2) prohibit any person within their territories from making any funds available for the benefit of persons who attempt or commit terrorist acts; (3) ensure that the state's domestic laws treat terrorist acts as serious criminal offenses; and (4) deny safe haven to anyone who participates

---

42. *See* International Convention for Suppression of Financing Terrorism, G.A. Res. 109, U.N. GAOR, 54th Sess., Supp. No. 49, at 408, U.N. Doc. A/54/49 (1999). The Convention was open for signature from January 10, 2000 to December 31, 2001. *Id.*

43. These financial intelligence units would be comparable to FinCEN.

44. S.C. Res. 1373, U.N. SCOR, 4385th Meeting (2001), *available at* http://daccessdds.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement.

in the financing or planning of terrorist acts and to ensure that such persons are brought to justice. Resolution 1373 also ensures that states treat terrorist acts as serious criminal offenses with just punishment to coincide with the seriousness of the crime, as well as, deny safe haven to those who financially facilitate terrorist acts. Member States are called upon to fully cooperate in exchanging information in order to prevent such acts.

The UN Counter-Terrorism Committee was established under Resolution 1373 to monitor implementation of the Resolution and to review reports from states on steps they have taken on implementation. As of the end of 2002, 181 out of 191 Member States had submitted progress reports.

Lastly, under several other UN Security Council Resolutions (UNSCR 1267,1390, and 1455) UN Member States are required to implement measures against all individuals and entities associated with Osama bin Laden, Al Qaida, and the Taliban. Such measures include: asset freezing, travel restrictions, and an arms embargo. Member States are required to impose those measures against the individuals and entities associated with Al Qaida and the Taliban, who are placed on a list maintained by the UN 1267 Sanctions Committee. Limited exceptions to the asset freeze provisions are permitted under certain circumstances.

III. RECOMMENDATIONS TO IMPROVE ANTI-MONEY LAUNDERING REGULATION

Since the Patriot Act was enacted over three years ago, great strides have been made in the battle against money laundering and terrorist financing. New rules have vastly increased the difficulty of laundering illicit funds. A global campaign is well underway to shut down the flow of funds to terrorists. Securities firms, banks, and other financial institutions have implemented new policies, procedures, and systems to detect illegal activities more effectively and to help government officials track down the perpetrators.

As a result, there has been a dramatic increase in the reporting of suspicious activity since September 11th. The U.S. Treasury Department reports that financial institutions filed 2,655 SARs relating to possible terrorist financing in the eighteen months following the terrorist attacks. Although the number of SARs filed relating to terrorism has decreased since then, 459 SARs connected to terrorism were filed by depository institutions in the last six months of 2003.[45] In general, the number of SARs filed by depository institutions in 2003 was 453 percent higher than those filed in 1996.[46] In 2003, broker-dealers filed 4,267 SAR forms.[47]

Other kinds of reporting have also increased. Financial institutions have reported 16,405 possible matches (of which only 878 were inconclusive) in their

45. *The SAR Activity Review*, BY THE NUMBERS, Issue 2 (May 2004).
46. *Id.*
47. *Id.*

records of parties suspected by law enforcement of money laundering or terrorist financing.[48] In addition, law enforcement has designated over 330 terrorists or terrorist supporters. Approximately $200 million has been frozen or seized worldwide.[49]

These statistics demonstrate that much can be achieved when the financial services industry works in concert with law enforcement, but clearly more needs to be done. Only recently, Stuart Levey, Undersecretary of the Treasury for Terrorism and Financial Intelligence, stated that European officials have been slow to take action against entities designated by the United States as funding the terrorist group Hamas.[50] The efforts of the United States and her allies must compliment and support each other and there cannot be any lapses.

Three achievable recommendations that will make financial institutions and regulators more effective in the war on money laundering and terrorist financing are: (A) increased coordination among regulators, both domestically and on an international level; (B) increased reliance on regulated financial intermediaries; and (C) more information sharing by law enforcement with industry to assist in detecting suspicious activity. These three recommendations are discussed below.

A. *Increased Coordination Among Regulators, Both Domestically and On An International Level*

First, we need increased coordination among regulators, both here and internationally. This is necessary to avoid duplication of efforts and to harmonize the various anti-money laundering requirements. A recent Government Accountability Office ("GAO") Report found the government's National Money Laundering Strategy has had mixed results "guiding the coordination of federal law enforcement agencies to combat money laundering."[51] The GAO Report noted that various agencies had different priorities in their efforts addressed at money laundering. Such an approach cannot be successful. Instead, coordination must be improved, and to do that, regulators must cooperate to achieve effective regulation. In addition, each financial regulatory agency should have a designated anti-money laundering and terrorist financing office to centralize its own

---

48. *See* FinCEN, *supra* note 23. These reports are in response to requests from FinCEN under section 314(a) of the Patriot Act. Through the process established under 314(a), FinCEN is able to send requests to more than 15,000 financial institutions to attempt to locate accounts and transactions of persons suspected of being involved in money laundering or terrorism. *Id.*

49. *See* Testimony of Daniel L. Glaser, Director, Executive Office for Terrorist Financing and Financial Crime before the House Government Reform Subcommittee on Criminal Justice, Drug Policy and Human Resources (May 11, 2004).

50. Campion Walsh, *U.S. Treasury Worried By Hamas Funders Allowed in Europe,* DOW JONES NEWSWIRES, Sept. 29, 2004, *available at* http://framehosting.dowjonesnews.com/sample/samplestory.asp?StoryID=2004092916030012&Take=1.

51. U.S. General Accounting Office, *Combating Money Laundering: Opportunities Exist to Improve the National Strategy*, GAO-03-813 (Wash. D.C. Sept. 26, 2003), *available at* http://www.gao.gov/htext/d03813.html.

activities. Our government must also work multi-laterally to develop international anti-money laundering standards which promote cooperation and efficacy, but at the same time respect issues of nationality and the unique concerns of particular jurisdictions. In short, if the global campaign against money laundering is to be successful, national standards must be harmonized and cannot be in conflict.

B. Reliance on Financial Intermediaries

If we are to be successful in the fight against dirty money, U.S. regulators must recognize the anti-money laundering compliance performed by reputable foreign firms. As it now stands under the Patriot Act, U.S. financial institutions cannot rely on the United Kingdom or other European financial institutions to help screen for money laundering.

U.S. rules must allow reliance on the financial institutions of our European allies because of the increasing number of transactions conducted in the global marketplace. This coordinated effort would help achieve the goals of the Patriot Act, which requires broker-dealers, banks, and other financial institutions to devote more resources than ever before to anti-money laundering efforts.

Securities firms today conduct many different kinds of business with financial institutions acting on behalf of their own third-party clients. Transactions involving these "financial intermediaries" are commonplace and include purchases or redemptions of mutual-fund shares conducted through a broker or other intermediary, clearing trades for another broker's customers, and executing transactions of large institutions investing funds for third-parties. The financial intermediaries involved in these transactions are typically well-known financial institutions that are subject to the Patriot Act or, in the case of foreign institutions, to similarly comprehensive laws and regulations.

By being able to depend on a financial intermediary to perform compliance, U.S. firms can avoid duplication, and focus their resources on those areas that present the highest risk. Financial intermediaries are best situated to perform customer identification and due diligence because they interact with their clients, and can obtain the necessary information directly from them. But the Patriot Act rules—despite the best efforts of the regulators—do not permit reliance on foreign financial institutions, and only permit limited reliance on specified types of U.S. financial institutions. U.S. firms, therefore, must repeat the screening already conducted by their European counterparts.

In contrast, the EU's Directives and the U.K.'s rules do not require firms to repeat the due diligence performed by financial intermediaries. For example, the EU permits reliance when a customer is introduced to a financial or credit institution by a third-party that is also subject to the EU Directive. In the United Kingdom., when a customer is brought to a financial institution by a U.S. financial institution, a second round of customer identification generally is not required by the U.K. institution.

U.S. broker-dealers and other financial institutions should be permitted to build on the efforts of reputable foreign intermediaries, rather than replicating them. The anti-money laundering and terrorist financing compliance performed in the United Kingdom is comparable to that done here, and there is no reason to think their review is any less effective.

This is not to say that U.S. firms should be able to blindly rely on foreign firms. Firms would first have to consider the reputation of the intermediary, whether it is regulated and where it is located. For example, firms would have to determine whether a financial intermediary not subject to Patriot Act-type requirements is a legitimate, reputable entity that has adequate policies and procedures. To rely on intermediaries from lesser regulated and thus higher risk countries, U.S. firms would need to conduct even more detailed scrutiny and may require an independent review demonstrating that the intermediaries' policies are adequate. Reliance may be altogether inappropriate when known information calls the foreign firm into question.

C. Information Sharing by Law Enforcement With Industry

Third, there must be more meaningful information-sharing by regulators with the industry to assist in detecting suspicious activity. Up until now, efforts made by law enforcement in the United States, while helpful, are inadequate. Through worldwide intelligence, the government can help focus industry on the areas that pose the greatest risk. The industry's ability to identify suspicious activity would benefit significantly from the many sources of information available to government such as known havens for money laundering, the names of known shell banks, and any trends or transactions in money laundering or the financing of terrorism. In addition, there should be improved coordination in the industry's efforts to identify accounts or transactions with "senior foreign political figures," which have been identified by the government as posing a higher risk of money laundering. The government is in a better position to identify these persons, and doing so would permit the industry to focus more of its resources on monitoring accounts, rather than trying to prepare its own list of such persons.

IV. CONCLUSION

While the world has changed greatly in the four years since the terrorist attacks, some things remain the same. The number of people killed on September 11th and the devastation inflicted remain forever etched into our memories. Moreover, that day made very clear who the enemy is and the threat posed to our country and financial system. We now know that terrorism presents new threats to our society and economy.

The war against terrorist financing and money laundering presents enormous challenges given the significant amount of money that flows though our financial system from all parts of the world. Advances in technology and the widespread

use of the Internet have created opportunities for those who wish to harm us—regardless of where they are located. The result is that our financial institutions must now ferret through the thousands upon thousands of daily transactions to find suspicious activity, potentially as small as the hundred dollar transactions used by the September 11 terrorists.

While our achievements are significant, the task at hand is great. The Patriot Act has given the industry and law enforcement tools to combat these evils. The world community has also stepped up protective efforts. However, the lessons learned to date demonstrate the need for more coordinated efforts between law enforcement and industry. We cannot afford to waste resources by duplicating the efforts of reputable financial institutions in allied and friendly countries. To be successful, we must work hand-in-hand with our allies.