CHAPTER

15 Elements of an Effective AML/CFT Framework: Legal, Regulatory, and Best Institutional Practices to Prevent Threats to Financial Stability and Integrity

IAN CARRINGTON AND HEBA SHAMS

In 1989 the G-7 Summit established the Financial Action Task Force (FATF). The original mission of the FATF was to study the problem of money laundering by criminal organizations and to propose measures for standardizing anti-money laundering (AML) regimes. The FATF's first recommendations were issued in 1990, then updated in 1996 and again in 2003. In 2001 the FATF took on the added task of recommending measures for combating the financing of terrorism (CFT).

Today the core question remains: How to implement an AML/CFT system that works.

This chapter addresses this question, arguing that the key challenge in implementing AML/CFT regimes is in obtaining, maintaining, and transmitting relevant information. International AML/CFT standards aim at addressing this challenge by harmonizing measures across countries, imposing obligations to obtain and maintain information, removing barriers to information sharing, and establishing channels for information flow.

International AML/CFT standards have entered a new stage of maturity. When FATF issued its revised standards in 2003 and a new round of compliance evaluations was launched worldwide by various assessor bodies,[1] it was clear that it is no longer considered progress for countries to declare political support for the international standard or merely to issue laws and regulations. What really counts is the *effective implementation* of AML/CFT measures. This new emphasis, while not absent in the 1996 version of the recommendations, has

brought to the fore important questions regarding the operational effectiveness of an AML/CFT regime.

The AML/CFT standard created by the FATF is an amalgamation of measures: (1) criminalizing money laundering and terrorist financing, (2) setting up freezing, seizing, and confiscation systems, (3) imposing preventive regulatory requirements on a number of businesses and professions, (4) establishing a financial intelligence unit (FIU), (5) creating an effective supervisory framework, (6) setting up channels for domestic cooperation, and (7) setting up channels for international cooperation.

The AML/CFT system purports to achieve a multiplicity of objectives:

- removing profit from crime through confiscation;
- detecting crime by following the money trail;
- targeting third-party or professional launderers who through their services allow criminals to retain the proceeds of their crime;
- targeting the upper echelons of the criminal organization whose only connection to the crime is the money trail; and
- protecting the integrity of the financial system against abuse by criminals.[2]

Assessing the effectiveness of a system that is so composite in nature and that aims to achieve such diverse objectives has so far proven to be both conceptually and practically difficult. To date, there is no clear formula to assess whether an AML/CFT system has been effective in achieving its objectives. In the absence of a reliable measure of how much money is being laundered or how much terrorist money is circulating, the question of effectiveness becomes even more elusive when it is couched in terms of "curbing" money laundering and terrorist financing. It is therefore impracticable to try to measure the success of a specific AML/CFT measure by attempting to establish the extent to which the measure has

contributed to reducing the amount of money being laundered or terrorist funds being funneled.

Starting from the premise that access to information is the main challenge that faces the governments around the world in seeking to fight money laundering and terrorist financing, or more specifically to attain the multiple objectives described above, this chapter first demonstrates how AML/CFT standards address this challenge by facilitating the flow of information by imposing measures for obtaining, maintaining, and sharing information on a myriad of public and private institutions.

The chapter then explores (1) the role of the private sector under the international standard in obtaining, verifying and maintaining information; (2) the role of the supervisory authorities in ensuring the effective performance of these functions; and (3) the mechanisms for ensuring interagency information flow. It also explores such issues as the importance of political commitment for the effective functioning of these measures and the need for risk-based proportionality between the measures adopted and the money laundering and terrorist financing threat.

The findings in this paper are based on the authors' experience in working with countries that are developing AML/CFT measures. They are also based on the findings from AML/CFT assessments conducted by the IMF and the World Bank, as well as other assessor bodies. Because both technical-assistance work and assessments are generally subject to confidentiality, the findings will be discussed and analyzed in general terms, and no reference to specific countries will be made unless the example is drawn from sources that are in the public domain.

The Challenge of Information Flow

Information is a prerequisite for the effective enforcement of laws and regulations. Law enforcement authorities need information in order to implement the law and ensure that violations do not occur or, when they occur, do not go unsanctioned. Information is needed at all stages of the enforcement process in order to detect violations and

subsequently to prove the violations to the requisite standard of proof either in an administrative or a judicial process.

Procedural laws have always provided for rules to access privately held information for law enforcement purposes. Because of the severe nature of penal sanctions, laws of criminal procedure have been particularly protective of the rights of the individual in regulating the access of law enforcement authorities to information for the purposes of criminal investigations and prosecutions. These procedural safeguards require time and naturally entail time lags in the information-gathering process.

Since the 1970s, however, a number of developments took place that altered governments' approach to law enforcement needs for information: (1) technological developments and liberalization led to the globalization of economic activities, including economic crime;[3] (2) cross-border movement of funds in particular became intensely global both in volume and speed; and (3) for various reasons, economic crime has reached higher levels of magnitude involving both activities and proceeds that are crossing national borders.[4]

In response, law enforcement strategies began to analyze criminal activities in market terms and develop an understanding of criminal organizations by reference to the behavior of legitimate economic enterprises. The assumptions in this regard are that criminal organizations, like legitimate ones, need funding for their operations and that criminals are economic agents that engage in criminal activities because of economic incentives.

These assumptions and the analysis based on them have led to law enforcement strategies that focus on attacking the financial streams of criminal organizations and removing the profit from crime through confiscation/forfeiture measures as a way of removing the economic incentive. This shift in strategy meant that law enforcement authorities needed enhanced access to reliable information on financial and commercial transactions in order to be able to carry out asset-tracing investigations.[5]

In view of the globalization of fund flows and the increasing use by criminals of the regular channels of commerce to move their assets

or to reinvest them, it became accepted that the needs of law enforcement authorities for transaction information, especially about financial transactions, could not be met by the traditional means of discovery and disclosure. Traditional methods, such as production orders, were slow and had a high evidentiary threshold that did not meet the needs of law enforcement for expeditious action carried out at an early stage of the detection process.

It also became apparent that some of the information that law enforcement authorities needed in order to reconstruct the financial trail was often not being gathered by the businesses and professions involved in executing the transactions. For example, financial institutions did not always retain records of verified customer identification of parties making wire transfers.[6]

The problems that faced law enforcement authorities in implementing asset-based law enforcement strategies were present at the domestic level but were exacerbated once the crime or the proceeds crossed national borders. When they did, law enforcement authorities were confronted with the problems arising from differences in legal systems and with the procedural safeguards that foreign jurisdictions applied to protect their sovereignty. Differences in legal and regulatory systems also meant that the information that businesses and professions gathered about their financial and commercial transactions varied from country to country, and law enforcement authorities could not confidently assume that the financial trail would be possible to reconstruct once it is routed through foreign jurisdictions.

To illustrate these challenges, this section will offer two cases: one real, the BCCI example, and one hypothetical.

The BCCI Case

The case of the Bank of Credit and Commerce International (BCCI)[7] offers the best example of the abuse of the banking sector to carry out cross-border criminal activities of shocking magnitude. Regulators found it to be involved in money laundering, support of terrorism, bribery, tax evasion, and other criminal acts.

BCCI is also an illustrative case of the challenges of access to information faced by law enforcement authorities when the matter involves financial information in multiple jurisdictions. While the facts of this case have been widely publicized and are therefore familiar to most readers, the account presented here will recount only the facts that illustrate the issues of information flow.

The BCCI was specifically structured to evade effective government control. It was made up of multiple layers of corporate entities connected to each other through a complex web of affiliates, subsidiaries, and holding companies. This segmented corporate structure ensured that corporate records were spread worldwide and that the regulation and audit of BCCI was fragmented across different jurisdictions without any single jurisdiction having consolidated access to all the bank's records.

When the criminality of BCCI was finally uncovered, the New York district attorney had great difficulty in obtaining any documents held outside the jurisdiction of New York. These problems were particularly challenging in relation to documents held outside the United States in the United Kingdom, Luxembourg, Grand Caymans, Panama, and Abu Dhabi. The prosecutor's main hurdle was the fact BCCI had ensured that most of the important documents were kept in jurisdictions that adhered to strict bank secrecy.

One example of this conundrum can be seen in the attempts of the New York prosecutors to obtain the records that Price Waterhouse relied upon to certify the financial statements and balance sheets that were filed by BCCI in the state of New York. Price Waterhouse at the time of the investigation declined to do so on the basis that the entity that audited BCCI was based in Bermuda and was legally separate from Price Waterhouse U.S. The New York district attorney later lamented, "So here you have financial statements, profit and loss, filed in Washington, filed in Virginia, filed in Tennessee, filed in New York, and audited by auditors who are beyond the reach of law enforcement."[8]

A Hypothetical Case

To understand the information needs of law enforcement authorities and the challenges that faces them in meeting these needs, consider the following hypothetical case.[9]

An employee of a British bank based in Singapore commits bank fraud in the 1980s and wire transfers some of the stolen money to the United States, where the funds are invested in an account of a brokerage firm in New York. He then instructs the brokerage firm to sell all the securities purchased on his behalf and wire the funds to a bank in a bank-secrecy haven. His lawyer in the bank-secrecy haven then uses part of the funds to purchase a house in Germany, where the perpetrator eventually settles. Singaporean authorities open an investigation in the case with the aim of convicting the offender and recovering the funds in order to restitute the victims.

Tracing the funds is essential for the Singaporean authorities not only to confiscate and repatriate the assets but also to locate the offender, who has gone to live in his new house in Germany. In attempting to trace the assets, the authorities are confronted with the lack of records on the originator and beneficiary of the wire transfers sent out of Singapore to the United States. This case hypothetically occurred prior to the international standards on AML/CFT that included customer due diligence (CDD) for wire transfers.

Even when the Singaporean authorities eventually manage to obtain information on the destination of funds from Singapore to the United States, and later to the bank-secrecy haven, it is still impossible to obtain any information from the bank-secrecy haven, which protects every piece of financial information relating to the perpetrator. Unknown to the Singaporean authorities, the fraudster becomes aware of the investigation into his affairs and liquidates his property in Germany, carries the cash across borders, and establishes himself under false identity in a remote but comfortable country. The process of requesting international assistance lasts five years until it is abandoned without significant results.

To sum up, law enforcement authorities in performing their functions of fighting economic crime are confronted by two

fundamental informational challenges: (1) availability and reliability of the information necessary to detect and prove economic crimes, and (2) access in a timely fashion to such information wherever it is around the world.

The next section discusses how AML/CFT measures can build a reliable system for detecting financial flows for law enforcement purposes to avoid these problems.

Standard AML/CFT Measures Facilitate Information Flow

AML/CFT standards arose as a direct response to the informational challenges faced by law enforcement, such as those identified above. The FATF 40+9 Recommendations provide a comprehensive system of minimum interventions that countries can implement to address the informational deficit that law enforcement authorities face in pursuing economic crime. The recommendations create a comprehensive, multidisciplinary, asset-based enforcement model.

Under the FATF's 40+9 Recommendations, international AML/CFT standards recommend that countries adopt three types of interventions:

1. Impose obligations on key players to obtain and verify certain pieces of information in relation to specific transactions. The subjects of these regulatory obligations include financial institutions broadly defined, and other categories of businesses and professions such as real estate agents and casinos (Recommendations 5 and 12).

2. Impose obligations on the same key players to maintain records of such information for a specific period of time. The standard also requires that such records should be retrievable in a timely fashion (Recommendations 10, 12 and SRVI).

3. Create a legal environment that enables the sharing of this information between various parties to the extent that is relevant to the fight against money laundering and terrorist financing—in other words, to the extent that it is relevant to the function of competent authorities in pursuing and

> preventing economic crime. This category of interventions includes removing unjustified barriers to information flows, such as detrimental financial and professional secrecy provisions, as well as creating channels for the sharing of information between the regulated institutions and the competent authorities, among the competent authorities, and between the competent authorities and their foreign counterparts (Recommendations 4, 13, 16, 31 and 36-40).

Even Recommendation 26, which relates to creating a financial intelligence unit designed to receive, analyze, and disseminate information relating to suspicious activities, fits within these three categories of interventions necessary to create financial and commercial transparency and to allow law enforcement authorities optimum access to the necessary information.[10]

Getting the Institutional Buy-In

The effectiveness of any regulatory regime depends, in part, on the extent to which it is understood and accepted by those persons on whom it has an impact. A significant challenge, therefore, is fostering the acceptance of a regulatory regime among key stakeholders. In the broad context of the regulation of financial sector activities, these key players include policy makers, consumers of financial products and services, financial institutions, regulators, and other government agencies. Acceptance among stakeholders is more likely to occur if they understand the wider environment in which regulation occurs and the varied interests that must be satisfied. Borrowing customers of a bank, for example, are more likely to understand the factors that influence the terms and conditions imposed on their loans and other financial services when they appreciate the bank's duty towards its shareholders, depositors, and the wider community. The chances of successfully implementing a regulatory strategy are therefore enhanced under circumstances in which the stakeholders understand the competing interests and the various issues on which the regulator must focus.

The challenge of understanding these factors is amplified in the case of a regulatory regime geared to address AML/CFT risks. First, the factors that influence the design of the regulatory framework go

beyond the basic prudential concerns of financial sector regulation to include concerns related to illicit activity in the wider society. Second—and this is especially the case in smaller economies and societies—the design of an AML/CFT regulatory framework is influenced not only by local circumstances but also by international criminal activity and financial flows that may have very little to do with the local market. It can sometimes be quite challenging for regulators to ensure that local stakeholders understand how seemingly remote events can influence the regulatory measures adopted by the local authorities.

Parliament

Parliamentarians need to be convinced of the level of priority that should be accorded to developing an AML/CFT infrastructure. Support at this level is critical because a successful regime will depend on the passage of comprehensive and timely legislation and the provision of the resources necessary to make the regime effective. In this regard it would be useful for members of parliament to understand the obligations that arise from the relevant UN conventions, resolutions of the UN Security Council, and other regional commitments. To the extent that countries either directly or through membership in an FATF-style regional body (FSRB) subscribe to the FATF recommendations, there is an increased obligation to develop robust AML/CFT regimes. Government officials should also be aware that a number of governments have shown a willingness to impose various sanctions on other countries that are deemed to be inadequately applying the FATF recommendations. The United States has utilized Section 311 of the PATRIOT Act to designate countries or institutions as "primary money laundering concerns." Such designations, in conjunction with rules subsequently issued by the Financial Crimes Enforcement Network (FINCEN), will often have the effect of severely restricting the ability of U.S. financial institutions to deal with these countries or institutions.

Government Officials

Government officials will need to understand the various roles they are expected to play in the system and how it relates to other

aspects of their work. Regulators, for example, will need to develop methodologies for the integration of AML/CFT oversight into their existing supervisory regimes and determine how much of their resources to devote to the management of this risk. All entities will need to understand the role of the FIU, which will inevitably be a new institution or function within the government's institutional arrangements. It will be important for all parties within the government bureaucracy to understand the fundamental requirements and protocols that are associated with their new responsibilities. This will be especially important in the arrangements for the handling and processing of information as it flows from reporting institutions through the FIU and on to law enforcement and prosecution authorities.

Reporting Institutions

Even in the best of times, reporting institutions are prone to perceive themselves as being subject to onerous regulatory obligations. The imposition of an AML/CFT infrastructure creates another layer of obligations to which they will be subject. They, like the policymakers, will need to be sensitized to the need to play their important role as the gatekeepers of the system and should also be aware of the sanctions that can arise if they fail to meet their legal obligations. They will need to understand that money laundering and the financing of terrorism will thrive to the extent that there are areas of weakness in the system and that such weak points may either be their own institution or institutions with which they have a business relationship. In countries with a robust sanctioning regime, financial institutions that fail to establish effective AML/CFT regimes face not only reputational risks but may also be subject to heavy fines. In extreme cases of AML/CFT failures, regulators have closed an institution. One of the most severe actions taken by regulators in response to concerns about management of AML/CFT risk was that taken by Japanese regulators against Citigroup in 2004. The Japanese regulators ordered Citigroup to close its private bank operations over their concerns about the failure of the bank's AML internal controls.[11]

Public

Perhaps the most difficult stakeholders to bring on board are the members of the public since they are a diverse and disparate constituency. But they are also the stakeholders who are likely to suffer the greatest inconveniences from AML/CFT as they conduct their everyday business. It is therefore important to have a program of public outreach that helps members of the public to understand concerns related to the potential abuse of the financial system by persons engaged in illicit activity and the measures necessary to combat such abuse. A critical issue to address in outreach programs is the importance of providing adequate levels of information to covered persons/institutions because some AML/CFT requirements may be contrary to the general expectations about the privacy of some types of personal information.

The Role of the Private Sector

Obtaining Information

An AML/CFT regime should establish strong disincentives to the use of the financial and other covered sectors to facilitate illicit activity. To this end, the framework should create an environment that promotes high levels of transparency in the conduct of business by covered entities.[12] A major cornerstone in this regard is ensuring that covered institutions have thorough and pertinent information about their customers and the nature of their customers' business.

Before discussing the measures that institutions should take to obtain the information necessary to manage AML/CFT risk, it is important to consider the measures that should be taken by government authorities. Measures taken by covered institutions will be built on the frameworks first established by the government. It is important that the framework for the formation of companies and other vehicles used in the conduct of business activity promotes high levels of transparency. There should be arrangements that allow for the identification of all persons who participate in the ownership of corporate entities, serve as directors, or are in positions to exert significant control over corporate vehicles or other entities. It is therefore important for countries to enact legislation that minimizes

opportunities for persons to obscure the extent and nature of their participation in corporate or other forms of business activity. A recent FATF paper on the misuse of corporate vehicles reemphasizes the importance of a framework that requires institutions to obtain, in a timely manner, accurate and comprehensive information on the beneficial ownership of companies and to determine who are the trustees, settlors, and beneficiaries of trusts. The paper found that it is less important where such information is maintained, once it is comprehensive, up to date, and readily available to competent authorities.[13]

The other major component for obtaining such information is the action taken by the covered institutions themselves. There is often a perception that AML/CFT requirements place new and onerous responsibilities on covered institutions. While the advent of an AML/CFT regime will indeed impose a number of new requirements, there are a number of objectives that can be satisfied by measures that traditional financial institutions are likely to already have in place. In protecting their own commercial and financial interests, these institutions have a strong incentive to undertake due diligence on a customer, whether it is a bank managing its credit risk or an insurance company understanding a customer's risk profile before pricing a product offer. This type of information will not be adequate to meet the requirements of a comprehensive Know Your Customer (KYC) regime,[14] but it represents an important starting point as institutions try to obtain information on their customers in line with their AML/CFT obligations. Designated nonfinancial businesses and professions (DNFBPs)[15] are the exception in the context of the responsibilities that are associated with requirements for robust customer due diligence (CDD). In many instances the nature of their relationship with their customers in the performance of their core business activity does not present risks that necessitate the performance of due diligence. This is particularly so for dealers in precious metals and stones and real estate agents. Casino operations are perhaps the one area of DNFBP activity that has traditionally been more proactive in undertaking some forms of CDD, for they are more vulnerable than other DNFBPs to losses through the fraudulent activity of their customers.

There are a number of core questions that covered institutions are expected to ask themselves as they contemplate the establishment of a customer relationship:

- Who is this person?
- What type of activity does this person want to conduct with my firm?
- What type and pattern of activity can I expect?
- Is this person representing a third party?
- How can I verify the information presented to me?

An important standard for an AML/CFT framework is its usefulness in the context in which it takes place. In addressing the issue of verifying a customer's identity, FATF requires that countries should use "reliable, independent source documents, data or information" and cites the Basel Committee's "General Guide to Account Opening and Customer Identification" as guidance on the types of documents that would be acceptable for this purpose.[16] The paper suggests that government-issued identification documents such as passports, birth certificates, identity cards, and social security records would be appropriate for verifying identity, but it also points out that other documents "of an equivalent nature" may be used as well. While the use of such documents is clearly recommended in countries where they are commonplace, there are a number of countries where significant segments of the population do not possess such documents. In such instances the legal and regulatory framework should be designed in a manner that successfully bridges the requirements of the standard in way that is reasonable given the country's circumstances.

There is often a strong temptation to design legal and regulatory instruments and practices in a manner that conforms closely with the standards and best practices in developed societies. If this is attempted in an environment where such conformity is virtually impossible to achieve, there is a danger of establishing legal and

regulatory requirements with which most institutions cannot comply, which runs the risk of the framework being ineffective. It would clearly be more desirable to design a system that meets the test of independence and reliability within the local context. One country in which few citizens have state-issued identification has developed a system in which customers are identified on the basis of assurances provided by senior, well-respected community leaders. While this is not an ideal approach, to require government-issued identity documents in this instance would not only exclude persons who lack such documents from the formal financial sector but could also provide an incentive for the development of informal financial activity, which itself could become a source of AML/CFT vulnerability.

A crucial aspect of the CDD process is the establishment of a customer profile that assists institutions in understanding the type of activity that they should reasonably expect to be conducted through the customer's accounts or facilities. It is only by establishing such a profile at the beginning and in the early stages of the relationship that an institution's suspicion can be subsequently aroused by unusual or suspicious customer behavior. Such a profile is therefore the foundation for the subsequent function of monitoring customer activity and determining whether a suspicious activity report should be filed.

Maintaining Information

The principle reason to gather information is to ensure that accurate information is held on customers and their activities. This includes not only the information originally obtained on the customer but all subsequent information obtained, particularly information that relates to transactions conducted for or on behalf of the customer. Again, this is not a requirement that arises solely in the context of AML/CFT because there are many incentives, from a commercial perspective, for companies to maintain good records of customer activity and transactions. From an AML/CFT perspective, information needs to be comprehensive enough to facilitate detailed investigations into customer activity and should be easily accessible by the covered institutions and ultimately the competent authorities. The standard establishes minimum periods for the maintenance of

identification and transaction records and stresses that records should be maintained for periods beyond these minimums, if specifically requested by competent authorities.

It is important to update the original CDD information on the customer, particularly in instances where information comes to light that can potentially alter some aspect of the original customer profile. The standard requires that where an institution has reason to doubt the accuracy of information held on the customer, it should undertake a new CDD process.

A crucial aspect of maintaining information is the ongoing monitoring of customer activity. This function will initially identify unusual activity, which will be further examined to determine if it meets the test of suspicion. Institutions are challenged to determine what types of monitoring systems are most appropriate for their needs. Factors that will influence their decision are the volume, nature, and complexity of their regular business transactions. In some instances, it is possible that a system based on manual oversight may be an effective monitoring mechanism, but as institutions grow in size and transactions become more frequent and complex, it is inevitable that this function will have to be computerized. The challenge for institutions, particularly those in relatively small and unsophisticated economies, or those who deal with relatively few transactions, is to recognize when they have reached the point where it is necessary to computerize the function. At this stage it is challenging to choose the software that is the best suited to the institution's needs. A system that generates a large number of "false positives" is not effectively serving the need of the institution or the FIU. It should be the goal of covered institutions to produce a favorable ratio between the number of transactions that are originally identified as suspicious and the number of reports that are eventually filed with the FIU. The use of an automated system should not be seen as a replacement for human judgment and intervention, which are indispensable in making a final determination whether a transaction can be explained in the context of information held or known about the customer or whether it merits the filing of a suspicious transaction report (STR). The bottom line is that regulators will want to be convinced that an institution is able, with a

reasonable degree of consistency, to identify suspicious activity that merits reporting to the FIU.

Transmitting Information

A significant feature of AML/CFT regimes is the number of interfaces between various groups or stakeholders, including members of the public, covered institutions, the FIU, investigatory authorities, and the officials who will eventually prosecute cases. Each group has its core functions and specific interests and each has a distinct view of its responsibilities in respect of information in its possession.

One overriding concern is the need to treat information with the appropriate level of confidentiality. In the conduct of everyday commercial and private activity there is an expectation of reasonable levels of privacy by all parties. Customers often wish to limit the amount of personal information they provide to a financial institution or make publicly available, and often have legitimate reasons for wanting to do so. Use of instruments such as trusts, for example, is sometimes driven not only by financial planning objectives but also by a desire to protect information that the settlors prefer to keep out of the public domain. In many instances these vehicles obscure the link between an asset and the person or persons with a beneficial ownership interest in the asset. Financial institutions also place priority on protecting the confidentiality of customer-specific information, and government agencies such as supervisors, FIUs, and prosecutors are no less concerned about the confidentiality of information, especially when such information could be market-sensitive or could be related to a criminal investigation or prosecution. A fundamental challenge to the transmission of information, therefore, is to establish a framework for the sharing of information that is acceptable to all parties and meets reasonable AML/CFT objectives.

Authorities should seek to establish quite clearly that all reasonable expectations to privacy will be respected. This is not only necessary for the efficient conduct of everyday business activity. It should also foster the levels of confidence that will encourage persons, both natural and corporate, to continue their use of the

formal financial system. In a number of countries authorities have to balance requirements of AML/CFT legislation with confidentiality principles implicit in data-protection laws. However, notwithstanding the importance of an appropriate framework for confidentiality in the normal conduct of business, it is equally important to communicate to members of the public and the business community that there will be occasions when it will be necessary for persons and institutions to share such information. A major challenge in this regard is establishing a framework that provides for sharing of information while continuing to respect confidentiality to the extent possible.

The sharing or transmittal of information commences at the start of the business relationship. Customers should expect that their ability to initiate a business relationship with a covered institution will depend, in some measure, on the extent to which they are willing to provide information requested by the institution. If a customer is unwilling to provide information that is critical to the CDD process, the law should prohibit the institution from establishing the relationship. There are also times during the course of a business relationship when customers will be required to provide specific information to assist institutions to meet their AML/CFT obligations.

The information required for sending funds by wire transfer is a case in point. FATF Special Recommendation VII requires not only that specific customer information be obtained by the originating institution but also that such information should remain with the transfer throughout the payment chain. If the originating institution cannot obtain the information, it should decline to effect the transfer. Recipient institutions have a similar obligation to ensure that the requirements of the standard are met under these circumstances.

There should also be clear legal provisions indicating the circumstances under which covered institutions have an obligation to provide information to the FIU and other competent authorities and to provide explicit protection against civil and criminal liability for reporting institutions, their directors, and their employees, and obligating such parties to treat all reports in strict confidence.

The sharing of information when reporting institutions file suspicious transaction reports presents specific challenges that

require institutions to strike an important balance. Reporting institutions are not expected to perform the role of investigatory authorities, and the test to be met before taking a decision to file a report is that there are reasonable grounds for suspicion on the part of the reporting institution. In making a determination in this regard, it is expected that an institution will review its information on the customer, consider the customer's general profile, and where possible make discreet enquires that may be necessary to clarify the information being reviewed. The process of making inquiries is a sensitive one because it is important not to "tip off" the customer about the reasons for the enquiries. In fact, it is a requirement that there be an explicit prohibition against disclosing the fact that a report is being made to the FIU.

In attempting to meet their obligations to file STRs, institutions sometimes engage in defensive reporting. This is a practice in which they report all cases where there is the slightest level of suspicion about customer conduct. In taking this action, institutions are driven by a concern that they may be sanctioned if deemed to be failing to meet their reporting obligations. Defensive reporting is in fact counter-productive because it inundates the FIU with information of varying quality and makes the FIU's job of analyzing the data more difficult that it should be. Reporting institutions are therefore challenged to find the right balance between meeting their reporting obligations and being a responsible partner by providing the FIU with quality data on which to undertake its analysis.

Corporate Governance Infrastructure

As already discussed, many of the measures that institutions are expected to employ in satisfying AML/CFT obligations are not unique to an AML/CFT regime. Such measures can operate in conjunction with an underlying infrastructure that provides general support for the operation of the covered institution. An important aspect of this infrastructure is the institution's corporate governance framework. AML/CFT requirements will only be successfully executed to the extent that there is a framework of clear and effective policies and procedures, clear lines of accountability, appropriate control mechanisms, and internal and external audit functions. Financial sector regulators have often determined that failures within

licensed institutions can be linked to either a failure to establish effective risks-management systems or the failure to adequately use effective systems that are already in place. In a number of instances, regulators have given as a rationale for the imposition of AML/CFT-related sanctions the failure of institutions to maintain critical aspects of their corporate governance.

In December 2005 the Office of the Controller of the Currency (OCC) in the United States fined the Arab Bank US$24 million for failures in its internal controls related to the Banking Secrecy Act and general anti-money laundering compliance. The OCC found that the bank failed to (1) adequately implement a program to monitor funds transfers for suspicious activity, (2) obtain sufficient information about funds transfers to determine if it was necessary to file an SAR, and (3) adequately audit the program established to monitor funds-transfer procedures.[17] The OCC was therefore concerned that the corporate governance arrangements failed not only at the primary level of establishing appropriate monitoring mechanisms but also at a secondary level in relation to weaknesses in the audit function.

In October 2006 the Financial Crimes Enforcement Network (FINCEN) assessed a civil penalty against the Foster Bank in the amount of US$8.5 million. FINCEN found that the bank "failed to implement an adequate Banking Secrecy Act compliance program, including an anti-money laundering program with internal controls, independent testing and other measures to detect and report potential money laundering, terrorist financing and other suspicious activity."[18]

Role of the Supervisor

In general, supervisors should seek to create and maintain an environment in which institutions are able to conduct legitimate business activity. They should ideally see themselves as partners with the institutions they supervise and should seek, to the extent possible, to minimize unnecessary regulatory burdens not only in the interest of the efficiency of the system but also to avoid creating incentives for the emergence of informal or parallel systems. Notwithstanding this broad objective, supervisors also have an obligation to protect the integrity of the financial and wider business community. They must develop a supervisory framework that is

effective for the institutions for which they have supervisory responsibility and should seek to understand the AML/CFT risk profile of these institutions in an effort to develop appropriate supervisory strategies. An important aspect of the supervisor's function is the articulation of supervisory objectives and strategies in a manner that makes clear what is expected of industry. Instruments such as regulations and guidance notes are commonly used to give more detailed expression to the basic framework as established in the primary legislation. In the context of risk-based approaches to the management of AML/CFT risks, it is very important for supervisors to give industry a clear indication of the extent to which such approaches will be accepted.

In the practice of supervision, strategy comes into play as early as the licensing stage. The basic fit-and-proper tests that are commonly applied by financial sector supervisors are a useful starting point. However, supervisors need to go beyond this type of assessment and consider whether the applicant for a license is appropriate from the perspective of its potential AML/CFT risk profile. An entity that is likely to be conducting significant portions of its business with persons from jurisdictions with weak AML/CFT laws and oversight regimes would, for example, raise certain concerns about AML/CFT vulnerabilities. As with all other areas of general supervisory concern, it is important to get it right at the licensing stage because addressing problems after an institution is up and running is far more difficult.

It is important for supervisors to have the necessary powers to undertake their responsibilities. This includes the power to request information from licensees, the power to undertake on-site inspections, and the power to apply sanctions. The international standard requires countries to have in place "effective, proportionate and dissuasive criminal, civil or administrative sanctions" that can be applied to both legal and natural persons. Actions taken by supervisors internationally have demonstrated the use of a wide range of sanctions, tailor-made to address specific supervisory concerns.

In November 2005 in the United Kingdom, the Financial Services Authority (FSA) announced that it had imposed a fine of £175,000 on Investment Services UK Limited (ISUK) "for conducting its business

without due skill, care and diligence and for failing to control its business effectively in relation to anti-money laundering (AML) systems and controls." In addition to the fine imposed on the business, the FSA fined its managing director £30,000, indicating that "he failed to act with due care, skill and diligence, failed to ensure that his firm complied with AML requirements and was knowingly concerned in the actions taken by ISUK."[19]

In December 2005 four U.S. government agencies took joint action against ABN AMRO, imposing penalties totaling US$80 million. In a joint public announcement the agencies indicated that the penalties were based on "findings of unsafe and unsound practices; on findings of systemic defects in ABN AMRO's internal controls to ensure compliance with U.S. anti-money laundering laws and regulations, which resulted in failures to identify, analyze, and report suspicious activity; and on findings that ABN AMRO participated in transactions that violated U.S. sanctions laws."[20]

These actions demonstrate the importance of regulators having flexible sanction powers to address failures in accordance with the perceived severity of the failure and in a manner that can sanction both legal and natural persons.

A Question of Risk

Supervisors and reporting institutions both face resource constraints in the performance of their AML/CFT responsibilities. It is not possible to devote similar levels of resources to all functions and responsibilities, and judgments have to be made about how resources can be most effectively employed. While the debate about risk-based approaches has been the focus of considerable attention in recent years, it is certainly not new; both supervisors and supervised institutions have always had to make judgments on how best they can employ the limited resources at their disposal to effectively manage the risks they confront. For institutions the focus is on the risk inherent in their business lines. Supervisors, on the other hand, have a broader perspective and are more concerned about the risk faced by individual institutions and the financial system as a whole.

Supervised Institutions

A supervised entity must define its appetite for risk in the context of AML/CFT and develop strategies to manage the risk inherent in the business it conducts. It is therefore expected that institutions will be able to demonstrate that they understand the risk they take on and that they have devised internal mechanisms and controls to manage it. The FATF recommendations have provided some broad guidance in this regard and have identified activities considered to represent a level of risk that is higher than normal. These include businesses with politically exposed persons (PEPS), correspondent banking relationships, and businesses with persons or entities from countries that do not adequately apply the FATF Recommendations. This list is not exhaustive, and institutions are expected to understand their own risk profile and employ the appropriate measures to manage the risks. For example, a number of banking institutions worldwide have made the judgment that providing services to money services businesses is a high-risk activity in the context of AML/CFT and have either reduced services to these entities or have discontinued the business relationships. Six U.S. regulators were concerned enough about this development to issue a joint statement suggesting that a bank's concerns in this regard "may stem, in part, from a misperception of the requirements of the Banking Secrecy Act and an erroneous view that money services businesses present a uniform and unacceptably high risk of money and other illicit activity."[21] The regulators stressed that "a decision to accept or maintain an account with a money services business should be made by the banking institution's management, under standards and guidelines approved by its board of directors and should be based on the banking institutions' assessment of the risks associated with the particular account and its capacity to manage those risks." The action taken by the U.S. regulators underscores the importance of devising risk management strategies that are tailored to the risk profile inherent in an institution's business lines and customer relationships, and it also highlights the regulators' concerns that measures taken to manage AML/CFT risk should be proportionate to the perceived risk and should not be unnecessarily disruptive to the conduct of legitimate business activity.

It is permissible, using a risk-based approach, to determine that some lines of business represent a lower-than-average level of risk

and accordingly can devote fewer resources to managing the AML/CFT risks. Institutions adopting such measures should be prepared to justify to their supervisor the basis of their analysis of the risks that they perceive to be inherent in their various business lines and customer relationships and the rationale for the choice of measures they have adopted to manage those risks.

The Supervisor

The obligation of the supervisor is to understand and manage the AML/CFT risk that can be posed by all institutions for which it has responsibility. The supervisor must adopt strategies and determine the extent to which a disproportionate amount of supervisory resources may be focused on some institutions. The supervisor's judgment in this regard will be influenced by a number of factors, including the nature of the business undertaken by an institution and the effectiveness of the oversight regimes to which the institution is subject. A risk analysis might determine, for example, that a branch of a large international bank that has strong internal controls and is subject to rigorous headquarters oversight and independent audit might represent a lower AML/CFT risk than a small, locally owned bank that is neither subject to head office supervision nor comes under the consolidated supervisory responsibility of a foreign supervisor. Another perspective of the relative AML/CFT risks posed by these two institutions might be that notwithstanding the more robust oversight mechanisms to which the first institution is subject, its higher volume of large international financial flows may make it more vulnerable to money laundering and financing of terrorism than a small bank catering primarily to a local market. On issues of risk management, there are no easy answers. However, supervisors are expected to assess and understand the risks to which their licensees are exposed and to make appropriate decisions on the most effective use of their supervisory resources.

Interagency Information Flows

AML/CFT measures create unlikely partners. An effective AML/CFT regime depends on the successful cooperation between multiple agencies spanning the entire regulatory and law enforcement system. The scope of AML/CFT measures keeps expanding, leading

to an increase in the variety of agencies that must cooperate and exchange information for the system to work.

Initially, AML/CFT measures centered around the cooperation between financial sector supervisors, law enforcement authorities, and the FIU. The definition of financial institutions under the AML/CFT standards is quite broad.[22] It is not restricted to the traditional sectors of banking, insurance, and securities. Rather, it expands to include, for example, foreign exchange bureaus and all types of providers of fund transfers. Countries adopt different approaches to financial sector supervision. The majority, however, continue to assign the supervisory function to different agencies. The more dispersed the supervisory function, the more complex the process of interagency cooperation and exchange of information.

In 2003 the AML/CFT standard expanded to include a list of designated nonfinancial businesses and professions (DNFBPs), which includes casinos; real estate agents; dealers in precious stones; dealers in precious metals; lawyers, notaries, other independent legal professionals; and trust and company-service providers. With these additions comes an increase in the number of supervisory agencies involved in the fight against money laundering and terrorist financing. These agencies must then be incorporated in the stream of information flow.

FATF Recommendations on Domestic Cooperation and Information Sharing

The key Recommendation dealing with domestic cooperation between competent authorities is Recommendation 31. It states:

> Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

Recommendation 31 is an open recommendation in that it defines the necessary measure by its objective, which is achieving effective cooperation. In other words, the recommendation does not tell countries what to do; it only guides them to implement effective mechanisms to achieve this objective.

Recommendation 31 does, however, offer some further guidance on the scope and nature of interagency cooperation. It defines the relevant authorities that should be integrated through mechanisms of cooperation. It suggests that countries bring into cooperative arrangements not only the FIU, the supervisory authorities, and law enforcement authorities, but also policy makers and other competent authorities. In the elaboration provided in the methodology for assessing compliance with the standard, it is clearly noted that law enforcement authorities should include customs authorities where appropriate. The involvement of customs authorities is particularly important because the focus on cross-border movement of cash and other negotiable instruments gained more prominence in the AML/CFT scheme with the introduction in 2004 of Special Recommendation IX, which specifically addressed this issue.[23]

Policy makers include any agency that has the power to influence or determine policies and practices. The exact scope of this category of stakeholders varies from country to country. Broadly speaking, it may include certain key ministries, such as the ministries of justice, foreign affairs, or finance.

Countries should also consider whether other competent authorities are relevant. For example, in countries where AML measures are not utilized to combat tax evasion, tax authorities may still be relevant because the information they possess may help in conducting financial investigations for the purposes of AML/CFT. A country may consider taking the necessary measures to achieve cooperation with tax authorities on AML/CFT issues, subject to that country's approach to confidentiality of tax information and the appropriate use of such information.[24]

Recommendation 31 also distinguishes between policy cooperation and operational cooperation, and requires countries to take measures to achieve cooperation at both levels. Countries should

take measures that help achieve cooperation in the development of AML/CFT policies. At the same time, they should have mechanisms in place to secure operational cooperation in carrying out AML/CFT activities such as cooperation in investigating money laundering offenses.

In addition to Recommendation 31, in this regard one should also take note of Recommendation 26, which requires that the FIU have access, directly or indirectly and on a timely basis, to the financial, administrative, and law enforcement information that it needs to undertake its functions. This aspect of Recommendation 26 spells with clarity an integral component of a system of information sharing that is essential for the operational success of the FIU.

A similar requirement is to be found in Recommendations 33 and 34, which require countries to make it possible for their competent authorities "to obtain or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control" of legal persons and legal arrangements.

Formal and Informal Mechanisms

Countries have adopted a variety of mechanisms to induce enhanced collaboration and information sharing among the agencies that have a role to play in fighting money laundering and terrorist financing, both at the level of policy making and at the operational level. In addition to the distinction between formal and informal mechanisms, there are four types of formal mechanisms that countries have adopted in order to facilitate interagency cooperation and information flows: legislative stipulation, formal multi-agency committees, interagency memoranda of understanding, and staff exchange arrangements.

Legislative Stipulation

Some countries have addressed issues of interagency cooperation and information sharing by legislation. This is consistent with the recommended approach in the UNODC/IMF Model Legislation on Money Laundering and Financing Terrorism [hereinafter, the Model Law],[25] which provides in article 3.1.4(4) that:

> The financial intelligence unit may request in relation to any report it has received, any additional information it deems useful for the accomplishment of its functions from:
>
> - Police departments
> - Authorities responsible for the supervision of the entities and persons subject to this law;
> - Other administrative agencies of the State
>
> The information requested shall be provided within the time limits set by the Financial Intelligence Unit.

Another aspect of interagency cooperation, which may be established by legislation or other formal mechanisms such as ministerial orders, requires supervisory authorities to inform the FIU of any weaknesses identified in the suspicious-transactions reporting systems of any institution subject to their supervision and to require the FIU to inform the relevant supervisory agency of any such weaknesses that it detects in the reports submitted by a supervised institution.

This approach is also endorsed by the Model Law in article 3.1.5, which provides:

> Whenever the financial intelligence unit determines that a financial institution or designated non-financial business and profession is not complying or has not complied with the obligations set out in this law, it may apprise the relevant supervisory authority accordingly.

Multi-Agency Committees and Steering Groups

Many countries employ multi-agency committees and steering groups, both in the area of policy cooperation as well as operational cooperation. Some of these committees are established formally by law, executive orders, or an interagency memorandum of understanding (MOU). Many countries have opted for creating an AML multi-agency, high-level committee with representatives from all relevant ministries and agencies charged with the task of coordinating AML policies. Some countries have added CFT to the

scope of operations of these committees, while others have opted for a separate committee with similar composition but often a different lead agency. The responsibilities of such agencies often include the task of facilitating information exchange between the member agencies.

Memorandum of Understanding

As a way of delineating the boundaries of their respective responsibilities or establishing protocols for the sharing of information or other resources, competent authorities in some countries are opting to sign MOUs with other competent authorities. This is a helpful tool because it clarifies roles and responsibilities, especially in the area of AML/CFT, where fragmentation and overlap often creates jurisdictional ambiguity.

MOUs between authorities are often not based on any explicit legislative authorization but rather are part of the general prerogative available to the administrative agencies to do what is necessary to perform their functions efficiently. As a result, while some agencies may be in the habit of entering into MOUs whenever the context merits it, other agencies find the MOU totally alien. Similar trends could be discerned at country level, for MOUs are more familiar in some jurisdictions than in others.

Staff Secondment and Staff Sharing

In order to enhance institutional cooperation, many agencies opt for entering into agreements with other agencies by virtue of which they second staff to the other agency. This approach aims to establish a continuous point of contact as well as develop a common understanding of each other's institutional culture.

Some agencies, especially law enforcement bodies, also opt for creating task forces to handle specific issues or cases. Also, because of the complex technical nature of some money laundering investigations, law enforcement authorities are relying increasingly on borrowed expertise from the supervisory agencies.

Aside from these formal mechanisms of cooperation, one of the most effective tools of cooperation and information sharing is the informal personal ties that are developed between the staff of various agencies. Because AML/CFT systems are still novel and it is mandating new connections between agencies that had little interaction before, these informal ties are in many cases still nascent. In addition, some countries opt for developing ad hoc working groups, committees, and task forces to foster cooperation and information sharing on particular issues.

Causes of Failure

Collaboration between authorities is not an easy matter. Agencies come into the process with different institutional cultures, mandates, and priorities. But tackling economic crime is nearly impossible without cross-agency effort.[26] It is possible to identify the common causes for failure or constraints in interagency information flow.

One of the biggest impediments to collaboration is the overlap of jurisdiction among agencies. This is a problem in many countries, regardless of their level of development or the sophistication of their AML/CFT system. Overlap of jurisdiction often creates turf fights and competitiveness that is detrimental to the collaborative process. This tension and competitiveness is often expressed in the systematic withholding of information from the other agencies, which clearly undermines the flow of information necessary for an effective AML/CFT system.

Turf fights resulting from overlap of mandates occur among competing supervisory authorities as well as competing law enforcement agencies. For example, the AML/CFT laws of some countries assign to the newly established FIU the function of supervising the regulated institutions' compliance with AML/CFT measures while still maintaining their default supervisory authorities over the same subject matter. In their attempt to protect their supervisory turf, the FIU and the supervisory authorities may withhold from each other information relating to the regulated institution's compliance, to the detriment of the effectiveness of the AML/CFT regime.

It has been observed, especially in larger countries with complex economic systems, that there is a substantial fragmentation of supervisory and law enforcement functions, which creates difficulties for coordination. One reason is related to the overlap of jurisdiction. Fragmentation of functions often results in ambiguity in the scope of the jurisdiction of each agency, which has the same effect as the overlap of jurisdiction. Fragmentation also increases the number of agencies that need to be involved, which aggravates conflicts of cultures, mandates, and priorities.

The reverse of fragmentation of functions—that is, concentration of functions—can also be problematic. Some country assessments have found that cross-agency cooperation is undermined when all the powers and responsibilities relating to AML/CFT are concentrated in one agency. This may seem paradoxical, for it would seem that if all AML/CFT responsibilities are concentrated in one agency, there would be no need for interagency cooperation. This conclusion would, however, be incorrect, for AML/CFT measures are only means to other ends. They are meant to facilitate the achievement of the wider objectives, including protecting the integrity of the financial system and facilitating law enforcement efforts against all types of financial crimes. Without cooperation and information flow between the agencies responsible for AML/CFT measures specifically and the agencies responsible for these wider objectives, the effectiveness of AML/CFT measures cannot be achieved.

The detrimental effects of concentrating AML/CFT functions could be attributed to the fact that it tends to lower the priority level of AML/CFT issues in other agencies and therefore reduces the level of resources committed to AML/CFT and the level of expertise developed in this area.

Staff turnover also poses a problem in jurisdictions that are small or have an underpaid civil service. Under such circumstances, staff of supervisory and law enforcement agencies tend to leave the service at a high rate in order to pursue better employment opportunities. This affects informal interagency collaboration because it undermines the development of sustainable collaborative relationships between individuals in various agencies.

Some structural factors may also pose challenges for the efforts to collaborate and share information. The sheer size of a country when accompanied by severe resource constraints results in difficulties of cooperation and sharing of information between agencies that operate in various parts of the country.

Finally, each authority is governed by certain rules relating to the use and disclosure of information that becomes available to it. Some of these rules are justified either for operational reasons, such as the success of criminal investigations or intelligence gathering, or for reasons of civil rights and due process, such as the restrictions relating to self-incrimination that apply in certain jurisdictions. Such rules have implications, for example, for the sharing of information between tax authorities that receive voluntary disclosures for tax purposes and criminal enforcement agencies gathering evidence to prosecute a criminal offense.

When confidentiality rules are too strict, they hamper institutional cooperation and information flows. While some of the confidentiality rules are justified, others may be out of date and not in line with the current complexity and magnitude of economic crime, which poses a much higher demand for information sharing. Some confidentiality practices are merely the result of institutional culture as opposed to either legal provisions or operational considerations.

Identified Good Practices

The findings from country experiences also point toward a number of good practices in achieving institutional cooperation and effective information flow. For example, there is strong evidence from country studies that when AML/CFT efforts are led by a strong agency such as a key ministry or other key institutions (e.g, the central bank), cooperation is enhanced. This is particularly relevant in the early stages of setting up an AML/CFT system. When successful, the lead institution, especially when adequately represented, plays an important role in resolving jurisdictional conflicts and facilitating the flow of information.

Multi-agency committees, whether formally or informally constituted, have succeeded in performing the functions of

facilitating cooperation and information sharing when they meet regularly and have a clear and realistic agenda. It is also good practice for member agencies to keep a representative on the committee who has sufficient authority to make commitments on behalf of the agency.

It is valuable to designate specialized AML/CFT units within each competent authority or to identify a specific liaison officer. This allows other agencies to easily identify the contact person. It also helps to develop expertise and institutional memory. An additional value is the harnessing of cooperative personal relationships across agencies.

Country experiences lend credence to the argument that the use of existing institutions instead of creating new ones to handle AML/CFT issues can benefit cooperation and information sharing. Building on already existing channels of cooperation where they exist between agencies has also proved beneficial. This does not preclude the creation of new channels, especially in situations where collaboration between particular agencies was minimal prior to the AML/CFT agenda.

Conclusion

Sixteen years after the development of the FATF 40 Recommendations, many countries are still facing the challenge of implementing effective AML/CFT regimes. The challenge is likely to be ongoing, in part because of the dynamic nature of financial sector activity and the widening of the AML/CFT net to cover nonfinancial institutions. Setting aside these two variables, success in this regard will still depend on the ability of countries to develop frameworks that create an environment in which relevant information can flow efficiently through the AML/CFT chain. Countries need to create legal frameworks that promote the easy availability of relevant and useful information, remove obstacles to the flow of such information, develop pathways through which such information can efficiently flow, and achieve a culture of cooperation across all private-sector and public-sector entities and persons that play a role in AML/CFT regimes.

Notes

[1] Compliance with AML/CFT assessments is conducted by the International Monetary Fund and the World Bank in the context of the Financial Sector Assessment Program, as well as by the FATF and the FATF-Style Regional Bodies (FSRBs) in a process of mutual evaluations among their members. All AML/CFT assessments are carried out in accordance with a commonly agreed methodology. Reference to "assessors bodies" is therefore a reference to the IMF, the World Bank, the FATF, and all FSRBs. Currently, there are eight FSRBs representing different regions of the world.

[2] For a discussion of these objectives and how they correspond to law enforcement strategies, see Mariano-Florentino Cuéllar, "The Tenuous Relationship between the Fight against Money Laundering and the Disruption of Criminal Finance," 93 *Journal of Criminal Law and Criminology* 311 (Winter/Spring 2003).

[3] In this paper, the term *economic crime* is used to refer to any crime committed for profit or economic gain.

[4] For a historical analysis of these developments and their link to the evolution of AML/CFT standards see Heba Shams, "Legal Globalization: Money Laundering Law and Other Cases," Sir Joseph Gold Memorial Series, Vol. 5, Chapters 2–3 (BIICL: London, 2004).

[5] For clear description of this approach to law enforcement, see wriiten statement of J. Rannazzisi before the Senate Committee on Finance "Breaking the Methamphetamine Supply Chain: Law Enforcement Challenges," (US Senate, September 18, 2007).

[6] For a good analytical discussion on the early debate relating to regulating wire transfers for AML purposes, see Sarah Jane Hughes, "Policing Money Laundering through Funds Transfers: A Critique of Regulation under the Bank Secrecy Act," 67 *Indiana Law Journal* 283 (Winter, 1992).

[7] For the details of the case, see Senator John Kerry and Senator Hank Brown, The BCCI Affair: A Report to the Committee on Foreign Relations, United States Senate (December 1992, 102d Congress 2d Session, Senate Print), 102–140.

[8] Ibid., Chapter 9.

[9] Parts of this hypothetical were drawn from a hypothetical case developed by Richard T. Preiss, "Privacy of Financial Information and Civil Rights Issues: The Implications for Investigating and Prosecuting International Economic Crime," 14 *Dickinson Journal of International Law* 525 (Spring, 1996), at 530 *et seq*.

[10] For a critical perspective on this issue of transaction transparency see Christopher Slobogin, "Transaction Surveillance by the Government" 75 *Mississippi Law Journal* 139 (Fall, 2005).

[11] "Japan Shuts Down Four Citigroup Offices," *Financial Times*, September 20, 2004.

[12] "Covered entities" are generally financial institutions and a category known as "designated non-financial businesses and professions" (DNFBPs), which includes but is not limited to, real estate agents, casinos, lawyers, accountants, trust and company service providers and dealers in precious metals and stones.

[13] Financial Action Task Force, *The Misuse of Corporate Vehicles, Including Trust and Company Service Providers*, October 2006.

[14] Refers to a comprehensive set of measures to be taken by financial institutions to satisfactorily identify their customers, and have a sound understanding of their background including their personal, business, and financial profiles and the type of transaction activity in which they are likely to engage.

[15] Designated Non-Financial Businesses and Professions is the term used by the FATF 40 + 9 Recommendations to refer to six categories of businesses and professions that should be covered by AML/CFT preventive requirements. These categories include: casinos, real estate agents, lawyers and other independent legal professionals, dealers in precious metals, dealers in precious stones, and trust and company service providers.

[16] Basel Committee on Banking Supervision, General Guide to Account Opening and Customer Identification February 2003—Attachment to Basel Committee Publication 85—Customer Due Diligence for Banks.

[17] Office of the Comptroller of the Currency, Enforcement Action—Consent Order for Civil Money Penalty (No. 2005 -101) http://www.occ.treas.gov/ftp/eas/ea2005-101.pdf

[18] FINCEN, "Enforcement Action in the Matter of The Foster Bank," Assessment of Civil Money Penalty (No. 2006-8) http://www.fincen.gov/news_room/ea

[19] Financial Services Authority, "FSA fines bond broker and managing director for anti-money laundering failures" (9 November 2008). http://www.fsa.gov.uk/Pages/Library/Communication/PR/2005/117.shtml

[20] FINCEN, "Enforcement Action in the Matter of The New York Branch of ABN Amro Bank N. V. New York, New York," Assessment of Civil Money Penalty (No. 2005 -5) http://www.fincen.gov/news_room/ea

[21] Federal Deposit Insurance Corporation, Financial Institutions Letters-Joint Statement on Providing Banking Services to Money Services Businesses—March 30, 2005 http://www.fdic.gov/news/news/financial/2005/fil2405a.html

[22] Financial Action Task Force, The Forty Recommendations (20 June 2003), 13.

[23] Special Recommendation IX requires countries to implement a comprehensive framework to monitor the cross-border movement of cash and other negotiable instruments specifically for the purposes of preventing and detecting money laundering and terrorist financing. The system is based on countries requiring travelers to either report spontaneously or disclose upon request from a competent officer their cargo of cash or other negotiable instruments above a certain threshold.

[24] See discussion below on the issue of confidentiality as an impediment to information flow.

[25] UNODC/IMF Model Legislation on Money Laundering and Financing Terrorism (December 1, 2005).

[26] On interagency cooperation in economic crime control, see Anne Puonti, *Learning to Work Together: Collaboration between Authorities in*

Economic-Crime Investigation, Dissertation, University of Helsinki, Department of Education, 2004).

This page intentionally left blank