Seminar on Current Developments in Monetary and Financial Law
Washington, D.C., October 23-27, 2006

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****

Sixteen years since the creation of the first Financial Action Task Force in 1989 launching the process of standardizing anti-money laundering regimes globally, core questions remain: *how to implement an AML/CFT system that works*. This paper addresses this question arguing that the key challenge in implementing AML/CFT regimes is obtaining, maintaining and transmitting relevant information. The 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.

1. INTRODUCTION

International AML/CFT standards have entered a new stage of maturity. When FATF issued the revised standard in 2003 and a new round of compliance evaluations was launched

*

** Financial Sector Specialist, Financial and Private Sector Development Vice Presidency, The World Bank.

worldwide by various assessor bodies,[1] it was clear that at this stage it is no longer considered progress for countries to declare political support for the international standard or to merely issue laws and regulations. What really counts is the *effective implementation* of AML/CFT measures. This new emphasis, while not absent under 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 is an amalgamation of measures that can be summarized as follows: (1) criminalization of 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 an FIU, (5) creating an effective supervisory framework, (5) setting up channels for domestic cooperation, and (6) setting up channels for international cooperation.

The system purports to achieve a multiplicity of objectives: (1) removing profit out of crime through confiscation, (2) detecting crime by following the money trail, (3) targeting third-party or professional launderers who through their services allow criminals to retain the proceeds of their crime, (4) targeting the upper echelons of the criminal organization whose

[1] Compliance with AML/CFT assessments are conducted by the IMF 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 amongst their members. All AML/CFT assessments are carried out in accordance with a commonly agreed assessment methodology. Reference to "assessors bodies" is therefore a reference to the IMF, the World Bank, FATF and all FSRBs. Currently, there are 8 FATF-Style Regional Bodies representing different regions of the world.

only connection to the crime is the money trail, and (5) protecting the integrity of the financial system against abuse by criminals.[2]

Attempting to assess the effectiveness of a system that is so composite in nature and that aims to achieve such diverse objectives has so far proved 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 funds are 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 an AML/CFT measure by attempting to establish the extent to which this 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 paper will demonstrate how AML/CFT standards address this challenge by facilitating the flow of information through imposing measures of obtaining, maintaining and sharing information on a myriad of public and private institutions.

[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).

2. 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 be able to perform their function of ensuring the effective implementation of the law and ensuring that violations do not occur or, when they occur, do not go unsanctioned. Information is needed at all stages of the enforcement process. It is needed 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, criminal procedural laws 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 a number of interconnected developments took place that altered governments' approach to law enforcement needs for information: (1) technological developments and liberalization trends 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, (3) due to various factors economic crime have

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

reached higher levels of magnitude involving both activities and proceeds that are crossing national borders.[4]

In this context, law enforcement strategies began to shift towards analyzing criminal activities in market terms and developing 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 to continue their operations and that criminals are economic agents that engage in criminal activities because of the economic incentives that they provide.

These assumptions and the analysis based on them translated into law enforcement strategies that focus on attacking the financial streams of criminal organizations and removing the profit out of crime through confiscation/forfeiture measures as a way of removing the economic incentive out of crime and diminishing the capacity of criminal organizations. This 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]

---

[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 (BIICL: London, 2004), Chapters 2 & 3.

[5] For clear description of this approach to law enforcement *see* "Breaking the Methamphetamine Supply Chain: Law Enforcement Challenges" a testimony by J Rannazzisi, Deputy Assistant Administrator before-Office of Diversion Control before the Senate Committee on Finance

In view of the intense 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 financial transactions information, could not be met by the traditional means of discovery and disclosure. Most evidently, traditional methods, such as production orders, were slow and had 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.

In addition to the constraints of access to information, it became apparent that some of the information that law enforcement authorities needed in order to reconstruct the financial trail were not being gathered by the businesses and professions involved in one capacity or another in executing the transactions. For example, financial institutions did not always retain records of verified customer identification data relating to the parties to the wire transfers that they executed.[6]

These problems that faced law enforcement authorities in implementing asset-based law enforcement strategies were present at the domestic level and were exacerbated once the crime or the proceeds crossed the borders. In the latter case, law enforcement authorities were confronted with the problems arising from differences in the 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 gathered by

[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).

businesses and professions in relation to financial and commercial transactions that they carried out 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 and one hypothetical:

The BCCI Case[7]

The BCCI case offers the best example of the abuse of the banking sector to carry out cross-border criminal activities of shocking magnitude. It is also an illustrative case of challenges of access to information that face law enforcement authorities, when the matter involves financial information and multiple jurisdictions. While the facts of this case has been widely publicized and are therefore familiar to most readers, the account presented here will recount some of these facts in order to illustrate the issues of information flow that are discussed in this paper.

The BCCI was specifically structured with the objective of evading effective government control in mind. It was made up of multi-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 the regulation

[7] *See for the details of the case* 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.

and audit of the BCCI was fragmented across different jurisdictions without any single jurisdiction having consolidated access to all the bank's records.

The BCCI's criminality spanned the full spectrum of economic crime including: fraud, corruption, contraband, professional money laundering, tax evasion, and many forms of financial crime.

When finally the criminality of the BCCI was uncovered, the New York district attorney had great problems 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 countries like the United Kingdom, Luxembourg, Grand Caymans, Panama, and Abu Dhabi. The main hurdle that faced the prosecution was the fact the BCCI has ensured that most of the important documents were kept in jurisdictions that adhered to strict bank secrecy and were protected by it.

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, which 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 legally separate from Price Waterhouse US and was based in Bermuda. The New York District Attorney later on 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[9]

To understand the information needs of law enforcement authorities and the challenges that faces them in meeting these needs it is worthwhile considering a hypothetical case. 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 and aim to convict the offender and recover the funds in order to restitute the victims.

Tracing the funds is essential for the Singaporean authorities not only for the purposes of confiscating and repatriating the assets but also for the purposes of locating the offender who has gone to live in his German newly obtained house. 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 US. This case hypothetically occurred prior to the international standards on AML/CFT including CDD for wire transfers.

---

[8] 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), Chapter 9.

[9] Parts of this hypothetical case 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.*

Even when eventually the Singaporean authorities manage to obtain information on the destination of funds from Singapore to the US, and later on to the bank secrecy haven it is impossible to obtain any information from the bank secrecy haven which protected every piece of financial information relating to the perpetrator. Unbeknown 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 5 years until it is abandoned without significant results.

To sum up, law enforcement authorities in performing their functions of fighting economic abuse are confronted by two fundamental informational challenges: (1) availability and reliability of the information necessary to detect and prove economic crimes, and (2) access to such information wherever it is around the world in a timely fashion. In the next section, this paper will discuss how AML/CFT measures aim to build a reliable system of financial flows for law enforcement purposes.

3. STANDARD AML/CFT MEASURES FACILITATE INFORMATION FLOW

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

In order to achieve this objective, the international AML/CFT standards recommend countries to adopt three types of interventions:

1. Imposing 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, other categories of businesses and professions such as real estate agents and casinos. (E.g., Recommendations 5 and 12)
2. Imposing 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. (E.g., Recommendations 10, 12 and SRVI)
3. Creating a legal environment that enables the sharing of this information between various parties to the extent that this is relevant to the fight against money laundering and terrorist financing. Or 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 include 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, amongst the competent authorities, and between the competent authorities and their foreign counterparts. (E.g. 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 creating financial and

commercial transparency and allowing law enforcement authorities optimum access to the necessary information.[10]

The remaining sections of this paper will explore in more detail (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 of ensuring interagency information flow critically assessed on basis of countries approaches and experiences. The remaining sections will also explore such overarching issues such 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.

4. GETTING THE 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 a direct or indirect 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 include policy makers, consumers of financial products and services, financial institutions, regulators and other government agencies. Acceptance among stakeholders is more likely to occur where they understand the wider environment in which regulation occurs and the varied

[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).

interests that must be satisfied. A borrowing customer of a bank, for example, is more likely to understand the factors that influence the terms and conditions imposed on his loans and other financial services, when he appreciates 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 interest 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 framework go beyond the basic prudential concerns of financial sector regulation to include concerns related to illicit activity in the wider society. Secondly, 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, by their geographic origin may have very little to do with the local market. It can sometimes therefore 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 and senior policy makers will need to be convinced of the level of priority that should be accorded to the development of an AML/CFT infrastructure. Support at this level is critical as a successful regime will depend on the passage of comprehensive, meaningful 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 and senior policy makers to understand the obligations that arise from the relevant UN conventions, resolutions of the Security Council and other relevant regional commitments. To the extent that countries either directly or through membership of a FATF style regional body (FSRB), subscribe to the FATF recommendations, there is an increased level of obligation to develop robust AML/CFT regimes. Policy makers should also be aware that a number of countries have shown a willingness to impose various sanctions on countries that are deemed to be inadequately applying the FATF recommendations. The USA has, for example, 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 US 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 make determinations on the proportion of their resources that should be devoted to the licensees' management of this risk. All entities will need to understand the role of the Financial Intelligence Unit, which will inevitably be a new institution or function within the government's overall institutional arrangements. It will be important for all parties within the government machinery 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

At 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 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 in instances of failure to meet their legal obligations. They will need to understand that ML and FT will thrive to the extent that there are areas of weakness in the system and that such weak points may either be there own institution or institutions with which they have a business relationship. In countries with robust sanctioning regimes, financial institutions that fail to establish effective AML/CFT regimes, face not only reputational risks but may also be subject to heavy fines which can have a significant financial impact on their operations. In extreme cases, action by regulators in response to AML/CFT failures, have led to the closure on an institution or loss of important lines of business. One of the most severe actions taken by regulators in response to concerns related to management of AML/CCT 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 group AML internal controls.[11]

[11] Financial Times, September 2004 – Japan Shuts down four Citigroup offices.

Public

Perhaps the most difficult stakeholders to bring on board are the members of the public since they are a diverse and disparate constituency. Paradoxically they are the stakeholders who are likely to be subject to the greatest levels of inconvenience as they conduct their everyday business. It is therefore desirable 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 various forms of illicit activity and the measures necessary to combat such abuse. A critical issue that should be addressed in outreach programs is the importance of providing adequate levels of information to covered persons/institutions as some AML/CFT requirements may go against the general expectations of privacy in respect of some types of personal information.

5. THE ROLE OF THE PRIVATE SECTOR

Obtaining information

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

Before we discuss the measures that institutions should take to obtain the information necessary for the effective management of the AML/CFT risk implicit in their lines of business, it is important to consider the measures that should be taken by the authorities.

Measures taken by covered institutions will be built on the frameworks for transparency that are 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 effective arrangements in place that allow for the identification of all persons who participate in the ownership of corporate entities, serve as directors or who are in positions to exert significant control over corporate vehicles or other entities. It is therefore important for countries to enact legislation that creates an environment 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 who is the trustee, settlor and beneficiary 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.[12]

The other major component in the context of obtaining such information is the action taken by the covered institutions themselves. There is often a perception that AML/CFT requirements place new and very onerous responsibilities on covered institutions. While the advent of an AML/CFT regime will impose a number of new requirements, there are a number of objectives that can be satisfied on the basis of measures that traditional financial institutions are likely to already have in place. In protecting their own commercial and

[12] Financial Action Task Force - The Misuse of Corporate Vehicles, Including Trust and Company Service Providers – October, 2006

financial interest these institutions have a strong incentive to undertake due diligence on their customers whether in the context of a bank's management of its credit risk or the need for an insurance company to understand 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, but it represents an important starting point as institutions try to obtain information on their customers in line with their AML/CFT obligations. Designated Non-Financial Businesses and Professions (DNFBPs)[13] are the exception in the context of the responsibilities that are associated with robust CDD requirements. 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 in the case 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 as 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. These include the following:

- Who is this person?

[13] 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.

- What type of activity does he/she want to conduct with my institution?
- What type and pattern of activity can I expect?
- Is he/she representing a third-party?
- How can I verify the information presented to me?

An important criterion by which the effectiveness of any aspect of an AML/CFT framework should be assessed, is its ability to be meaningful 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 Basle Committee's paper, "Guidance Paper on CDD for Banks" as providing good guidance on the types of documents that would be acceptable for this purpose.[14] This paper suggests that government issued identification documents such as passports, birth certificates, identity cards and social security records would be appropriate means of verifying identity but 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 with what can be reasonably achieved given the country's circumstances. There is often a strong temptation to

[14] Basle Committee on Banking Supervision: Customer Due diligence for Banks, Publication No 85 October 2001.

design legal and regulatory instruments and practices in a manner that conforms closely with the standard and known best practices in more developed societies. The danger of attempting this in an environment where such conformity is virtually impossible to achieve, is the likelihood of establishing legal and regulatory requirements with which most institutions cannot comply. This runs the risk of the framework becoming irrelevant and therefore ineffective. It would be clearly be more desirable to design a system that meets the test of independence and reliability within the local context. In one country, many citizens of which have no 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 vulnerability in the context of ML/FT.

A crucial aspect of the CDD process is the establishment of a customer profile. This is an important step that assists institutions in understanding the type of activity that they should reasonable 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. The establishment of such a profile is therefore the basic foundation for the subsequent function of monitoring customer activity and making a determination as to the need to file a suspicious activity report.

Maintaining Information

The principle objective for the maintenance of information is ensuring that accurate and meaningful information is maintained 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. This again is not a requirement that arises solely in the context of AML/CFT as 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 relevant 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 minima, where specifically requested by competent authorities.

It is important to update the CDD information originally obtained 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, that it should undertake a new CDD process.

One of the most crucial aspects of maintaining information, is the on-going monitoring of customer activity. It is this function that will initially identify unusual activity that 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 and 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. Beyond this stage it is also 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. These considerations 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 an 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. This includes members of the public, covered institutions, the FIU, investigatory authorities, and the officials who will eventually prosecute cases. Each group has its core functions or specific interest and each has a distinct view on its responsibilities in respect of information that its has 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 very 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 prosecution authorities 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 establishing 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, but should foster the levels of confidence that will encourage persons, 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 on which 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 the sharing of that information, while continuing to respect its confidentiality, to the extent possible.

The sharing or transmittal of information commences at the start of the 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 that such information should remain with the transfer throughout the payment chain. Where this information cannot be obtained by the originating institution it is expected that it will 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, providing 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 in the context of filing suspicious transaction reports by reporting institutions has 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 of suspicion or 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 it may consider to be necessary to clarify the information being reviewed. The process of making enquiries is a sensitive one as it is important not to "tip off" the customer about the reasons for the enquiries. In fact it is a requirement that there should 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 as it inundates the FIU with information of varying quality and makes its job of analyzing the data much 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 good quality data on which to undertake its analysis.

Corporate Governance Infrastructure

As we have already discussed in the paper, many of the measures that institutions are expected to employ in satisfying AML/CFT obligations are not unique to an AML/CFT regime. In addition such measures 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 of various kinds within licensed institutions can very frequently 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 infrastructure.

In December 2005 the Office of the Controller of the Currency (OCC) in the USA fined the Arab Bank $24 million for its failures in 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 re funds transfers to determine if it was necessary to file an SAR and

(3) to adequately audit the program established to monitor funds transfer procedures.[15] 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 FINCEN, assessed civil money penalty against the Foster Bank in the amount of $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".[16]

6. ROLE OF THE SUPERVISOR

Supervisors should, in general, seek to create and maintain an environment in which institutions are able to effectively 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 burden not only in the interest of the general efficiency of the system but also to avoid the creation of 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 are challenged to develop a supervisory framework that is meaningful and effective in the context of the institutions for which they have supervisory responsibility and should seek to

[15] http://www.occ.treas.gov/ftp/eas/ea2005-101

[16] http://www.fincen.gov/foster

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 it clear to industry what is expected of them. 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 context of on-going supervision, the supervisory 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 in the context of AML/CFT vulnerabilities. As with all other areas of general supervisory concern it is important to get it right at the licensing stage as addressing problems after an institution is up and running is far more difficult.

It is important for supervisors to be given the necessary powers to effectively 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 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 the UK 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 entity the FSA also fined its managing director in the sum of £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."[17]

In December 2005 four US government agencies took joint action against ABN AMRO imposing penalties totaling $80.0 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."[18]

---

[17] http://www.fsa.gov.uk/Pages/Library/Communication/PR/2005/117.shtml

[18] http://www.fincen.gov/abnamro.html

The above 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.

7. A QUESTION OF RISK

Both supervisors and reporting institutions face resource constraints in the performance of their AML/CFT responsibilities. It is essentially not possible to devote similar levels of resources to all functions and responsibilities and judgments have to be made about ways in which 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 as 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. The debate on the management of risk can be discussed separately in the context of supervised institutions and the supervisors. For institutions the focus is on the risk inherent in their business lines while supervisors have a higher-level perspective and are more concerned about the risk faced by individual institutions and the financial system as a whole.

Supervised Institutions

A supervised entity is challenged to define its risk appetite in the context of AML/CFT and develop strategies to effectively 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 mange that risk. The FATF recommendations have provided some broad guidance in this regard and have identified some activities generally considered to represent a higher- than-normal level of risk. These include business with politically exposed persons (PEPS), correspondent banking relationships, business with persons/entities from countries that do not adequately apply the FATF Recommendations and regimes for introduced business among others. This list is not exhaustive and institutions are expected to understand their own risk profile and employ the appropriate measures to manage the risks. A number of banking institutions worldwide have for example, 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 the services they offer to these entities or have discontinued the business relationships completely. Six USA regulators were concerned enough about this development, to issue a joint statement suggesting that 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."[19] 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 US 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 also highlights the regulators'

[19] http://www.fdic.gov/news/news/financial/2005/fil2405a.html

concerns that measures taken to manage ML/FT 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 devote proportionately fewer resources to managing the AML/CFT risks that might potentially be associated with these activities. 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 such risks.

The supervisor

From the perspective of the supervisor the question of risk focuses on its obligations to effectively understand and manage the AML/CFT risk that can be posed by all institutions for which it has responsibility. This has implications for the supervisory strategies adopted and 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 business undertaken by various institutions and the effectiveness of the oversight regimes to which the institutions are subject. A risk analysis might determine, for example, that a branch of a large international bank which 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 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 ML/FT than a small local bank catering primarily to the domestic market. In the debate on 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.

7. INTERAGENCY INFORMATION FLOWS

AML/CFT measures create unlikely partners. As we have already indicated, 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 and with that comes 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 very broad.[20] It is not restricted to the traditional sectors: banking, insurance and securities. Instead, it expands to include for example foreign exchange bureaus and all types of fund transfer service providers. Countries adopt different

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

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 designated list of non financial businesses and professions (DNFBPs). This list 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 new additions comes a parallel increase in the number of supervisory agencies involved in the fight against money laundering and terrorist financing. More agencies must then be incorporated in the stream of information flow.

In the following sections, this paper will analyze the requirements of interagency cooperation and information flow and then summarize the mechanisms countries adopt in achieving interagency coordination and information flow. The paper will also provide analysis of the causes of failure in interagency coordination and provide examples of good practice. The findings in these sections are based on the author's experience in working with countries developing their 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.

A. The FATF Recommendations on Domestic Cooperation and Information Sharing

The key Recommendation dealing with domestic cooperation between competent authorities is R. 31. According to R. 31

> 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 that defines the necessary measure by it objective, which is achieving effective cooperation. In other words, the recommendation does not tell countries what to do exactly, it only guides them to implement effective mechanisms to achieve this objective.

R. 31 offers, however, offers some further guidance on the scope and nature of interagency cooperation. It defines the relevant authorities that should be integrated through mechanisms of cooperation. According to R. 31, countries should bring into cooperative arrangements not only the FIU, the supervisory authorities, and law enforcement authorities, but also the 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 since the focus on cross-border movement of cash and other negotiable

instruments gained more prominence in the AML/CFT scheme with the introduction of Special Recommendation IX in 2004 addressing specifically this issue.[21]

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 what other competent authorities maybe relevant. For example, in countries where AML measures are not utilized to combat tax evasion, tax authorities may still be relevant because of the information they possess which may help in conducting financial investigations for the purposes of AML/CFT. Countries may consider taking the necessary measures to achieve cooperation with tax authorities on AML/CFT issues. This is subject to countries' approach to confidentiality of tax information and the appropriate use of such information.[22]

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

[21] 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.

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

development of AML/CFT policies. They should also have mechanisms in place to secure operational cooperation in carrying out AML/CFT activities such as cooperation in investigating money laundering offences.

In addition to R. 31, one should also take note in this regard of R. 26, which requires that the FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions. This aspect of R. 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 R.33 and R. 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.

The next sections will illustrate how countries attempt to achieve the objectives of effective policy and operational cooperation.

B. Formal and Informal Mechanisms

Countries have adopted a variety of mechanisms to induce enhanced collaboration and information sharing between the different agencies that have a role to play in fighting money laundering and terrorist financing both at the level of policy-making as well as at the

operational level. In addition to the distinction between formal and informal mechanisms, one identify 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 memorandum of understanding, and staff exchange arrangements.

Legislative Measures

Some countries have addressed issues of interagency cooperation and information sharing by legislation. This is consistent with the recommended approach in the AML/CFT Model Law for civil law jurisdictions, 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 involves requiring supervisory authorities to inform the FIU of any weaknesses identified in the suspicious transactions reporting systems of any institution subject to their supervision and imposing a similar requirement on the FIU to inform the relevant supervisory agency of any such weaknesses that it detects in the reports submitted by a supervised institutions.

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

> 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

This is a commonly employed mechanism by countries, both in the area of policy cooperation as well as operational cooperation. Some of these committees are established formally by law, executive orders, or interagency memorandums of understanding (MOUs). 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 different lead agency. The responsibilities of such agencies often include the task of facilitating information exchange between the member agencies.

Memorandum of understandings (MOUs)

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 different countries are opting increasingly for signing MOUs with other competent authorities. This is a helpful tool because it helps clarifying 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 they 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 maybe in the habit of entering into MOUs whenever the context merits it, other agencies find the instrument of MOU totally alien. Similar trends could be discerned at country level. 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 would second staff to the other agency. This approach aims at establishing a continuous point of contact as well as developing a common understanding of each others institutional culture.

Agencies, especially law enforcement agencies, 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, discussions with authorities in the context of assessments and technical assistance reveal that 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 of the novelty of AML/CFT systems and the new ties that it is mandating between agencies that had little interaction before, these informal ties are in many cases still nascent. In addition, Countries also opt for developing ad hoc working groups, committees and task forces to foster cooperation and information sharing on particular issues.

C. Causes of failure

Collaboration between authorities is not an easy matter. Different agencies come into the process with a completely different institutional culture, mandate and priorities. It is now well accepted that tackling economic crime is nearly impossible without cross-agency effort.[23] Through extensive work with countries and a large pool of assessment reports, one can identify a set of common causes for failure or constraints in interagency information flow.

One of the biggest impediments to collaboration is the overlap of jurisdiction between various agencies. This is a common problem in many countries regardless of the level of development and sophistication of the 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

[23] On interagency cooperation in economic crime control *see* Anne Puonti, *Learning to Work Together: Collaboration between Authorities in Economic-Crime Investigation* (Vantaa, 2004).

from the other agencies. This clearly undermines the flow of information necessary for an effective AML/CFT system.

Turf fights resulting from overlap of mandates occur amongst 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 maintaining the supervisory role of their default supervisory authorities in relation to 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 institutions' compliance to the detriment of the effectiveness of the AML/CFT regime.

It has also been observed, especially in larger countries with complex economic systems, that there is a substantial fragmentation of supervisory and law enforcement functions. This creates difficulties in coordination for many reasons. 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, i.e.; concentration of functions, may also be problematic. Some of the findings of country assessments point to the fact that when all the powers and responsibilities relating to AML/CFT are concentrated in one agency, this tends

to undermine cross-agency cooperation. This may seem paradoxical. In other words, one may argue that if all AML/CFT responsibilities are concentrated in one agency there is probably no need for interagency cooperation. This conclusion would however be incorrect. AML/CFT measures, as discussed in the introduction to this paper, are 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 the concentration of functions could be attributed to the fact that it tends to reduce the level of priority of AML/CFT issues in other agencies and as a direct consequence the level of resources committed to AML/CFT and the level of expertise developed in this area. This concentration often occurs in countries with new AML/CFT framework, and the tendency observed so far is to vest all the powers in the FIU.

Staff turnover also poses a problem that is common to small jurisdictions and jurisdictions with underpaid civil service. Under such circumstances, staff of supervisory and law enforcement agencies tends to leave the service at a high rate in order to pursue better employment opportunities. This affects interagency collaboration in its informal forms 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 in the performance of its functions. Some of these rules are justified either for operational reasons, such as the success of criminal investigation or intelligence gathering, or for reasons of civil rights and due process, such as the restrictions relating to self-incrimination applicable 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 for a criminal offence.

When the confidentiality rules are too strict, they hamper institutional cooperation and information flows. While some of the confidentiality rules are justified as discussed above, others may be out-of-date and not in line with the current complexity and magnitude of economic crime, which poses 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.

D. Identified good practices

The findings from country experiences also point towards a number of good practices in achieving institutional cooperation and effective information flow:

There is strong evidence from country studies in the context of technical assistance and country assessments that when AML/CFT efforts are led by a strong agency such as a key ministry or other key institutions (e.g.; the ventral bank), cooperation is enhanced. This is particularly relevant at the early stages of setting up an AML/CFT system. It is also only successful when the leadership is not transformed into possessiveness of the mandate and exclusion and discouragement of the other relevant institutions. In the instances observed, the lead institution, especially when adequately represented, played an important role in resolving jurisdictional conflicts and facilitating the flow of information.

Multi-agency committees whether formally or informally constituted have been shown to succeed in performing the function of facilitating cooperation and information sharing when they meet regularly and have a clear and realistic agenda. It was also observed as good practice and a prerequisite for success that the member agencies keep a regular representative on the committee that has sufficient authority to make commitments on behalf of the agency.

Also proved of particular value for cooperation and information sharing to designate specialized AML/CFT units within each competent authority or to identify a specific liaison officer. This allows the other agencies to identify with ease the contact person. It also helps the development of expertise and institutional memory. An additional value is the harnessing of cooperative personal relationships across agencies.

Observed country experiences also lend credence to the argument that the use of existing institutions instead of creating new ones to handle AML/CFT issues has benefits for

cooperation and information sharing. Also, building on already existing channels of cooperation where they exist between agencies 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 on-going, in part because of the dynamic nature of financial sector activity and the widening of the AML/CFT net to cover non-financial institutions. Setting aside these two variables, success in this regard however will still depend on the ability of countries to develop frameworks that create an environment in which relevant and good quality 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 the achieve of a culture of cooperation across all private and public sector entities and persons that play a role in AML/CCT regimes.