March 2004

Anti–Money Laundering

2nd Edition

International Federation
of Accountants

The mission of the International Federation of Accountants (IFAC) is to serve the public interest, strengthen the accountancy profession worldwide and contribute to the development of strong international economies by establishing and promoting adherence to high-quality professional standards, furthering the international convergence of such standards and speaking out on public interest issues where the profession's expertise is most relevant.

In January 2002, IFAC published its first paper on anti-money laundering aimed at promoting awareness of important money laundering issues and of the related professional obligations imposed on accountants. In the last two years, the issue of money laundering has become even more important to regulators and law enforcement agencies around the world, particularly in their drive to combat the financing of terrorism. Accordingly, the role of accountants in combating money laundering has also taken on correspondingly greater significance.

This second edition of IFAC's Paper on anti-money laundering discusses legislative and other measures taken to fight money laundering and the increased expectations that the profession monitor and detect money laundering, as well as establish and strengthen controls and safeguards against money laundering.

The Board of IFAC wishes to acknowledge the assistance of Alan Abel, of PricewaterhouseCoopers, Washington DC, for his assistance in drafting this paper.

IFAC welcomes any comments you may have on this paper. Comments should be sent to:

James M. Sylph
International Federation of Accountants
545 Fifth Avenue, 14th Floor
New York, New York 10017-3610 USA
Fax: +1 212-286-9570
antimoneylaundering@ifac.org

Copies of this paper may be downloaded free of charge from the IFAC website at http://www.ifac.org.

ISBN 1-931949-29-8

Anti–Money Laundering

Contents

Preface

In recent years, we've seen a growing number of highly publicized money laundering scandals. They have involved major national (meaning local or within jurisdictions) and international providers of diversified financial services, along with their correspondents in "off-shore" jurisdictions, Russia, other former Soviet Republics, Latin America and the Caribbean. Increasingly, money laundering has also become a problem in many emerging financial services sectors. In addition, the events of September 11, 2001 and the many subsequent acts of terrorism around the world have prompted a whole new emphasis and "war" on terrorist financing, frequently referred to as "money laundering in reverse" – i.e., money that starts out legitimate and grows "dirty" in its ultimate purpose.

In response, governments and other legal authorities in various jurisdictions have accelerated their issuance of new legislation, regulations, programs and cooperative actions, pronouncements and enforcement steps focused on combating money laundering, terrorist financing and related financial crime. Fifteen years after experts first tried to estimate the size of the problem, it is still widely held that money laundering continues to be a US $1 trillion-per-year problem.

In June 2000, the OECD's Financial Action Task Force (FATF), the world's Anti–Money Laundering (AML) watchdog, cited various "non-cooperative" jurisdictions for having serious deficiencies in their AML programs. This prompted a series of related initiatives:

- The UK, the US and other countries issued parallel money laundering advisories against those same jurisdictions.
- In the autumn of 2000, the international press took up the cause, publishing various articles on money laundering detection and deterrence problems in many "higher-risk" jurisdictions.
- Also in October 2000, in an effort to more clearly identify money laundering and corruption as interrelated problems, a dozen of the world's largest (primarily European and US) banks, working with the anti-corruption arm of the OECD and Transparency International, issued the *Wolfsberg AML Guidelines*.
- Governments and intergovernmental organizations (IGOs) then issued similar new national and transnational guidance. For example, the US Treasury Department released *Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of Foreign Official Corruption*.
- Shortly after that, the Basel Committee on Banking Supervision issued its proposal, "Customer Due Diligence for Banks," outlining procedures in four areas: customer acceptance, customer identification, monitoring of high-risk accounts and risk management.

The September 11, 2001 terrorist attacks on the United States and the rapid passage of the USA PATRIOT Act of 2001 began a new global round of tougher AML legislation and related regulatory and law enforcement initiatives that remain very much in motion today.

Today, after more than 30 years of AML legislation, numerous intergovernmental initiatives and considerable law enforcement activity, including many money laundering prosecutions and arrests, regulators continue to sanction leading global financial institutions for compliance and control weaknesses – for having insufficient safeguards for protecting themselves against money laundering and related financial crime.

There is no doubt that "enhanced due diligence," "enhanced scrutiny" and related guidelines for strengthening and further promulgating *KnowYourCustomer* (KYC) principles (explained in a later section) and suspicious activity reporting (SAR) are, through coordinated intergovernmental efforts, spreading across the globe in the forms of hard and "soft" law and leading practices. Meanwhile, however, privacy rights initiatives have also continued to gain momentum. As the former serve to foster transparency and the latter may easily serve to deter it, there is a fundamental disparity between these two important objectives.

The accountancy profession around the world is increasingly involved in both arenas. It has been asked to play various roles in combating corruption, with a new emphasis on ferreting out and investigating "Politically Exposed Persons" (PEPs), money laundering, fraud and related financial crime. At the same time, the profession is promoting privacy and other forms of consumer protection compliance by advising, auditing[1] or attesting to compliance self-disclosures and reporting illegal acts. Both types of activities are presenting unique challenges – and risks – to the profession.

Given these events, developments and trends, the purpose of this Discussion Paper is to:

- explore the role of external auditors and other accounting practitioners in ongoing public and private sector efforts to safeguard against money laundering;
- promote awareness of important issues and how increasing professional obligations pertaining to money laundering relate to, and interact with, corruption and transparency, privacy and consumer protection, as well as other professional services, duties and risk; and
- provide thought leadership, practical guidance on leading practices and a foundation for developing subsequent IFAC professional guidance.

Why the Interest?

Until relatively recently, the battle against money laundering and related financial crime was the exclusive domain of law enforcement, and for good reason. Most governments around the world define money laundering and the activities that lead to it, such as drug trafficking, as serious crimes. Approximately 15 years ago, forensic accountants started to contribute their skills to detecting possible money-laundering activity buried in the books and records of victimized financial institutions. Now, governments and businesses increasingly look to the profession, not only to aid in their monitoring and detection efforts, but also to establish and strengthen controls and safeguards against money laundering, its perpetrators and their accomplices in organized financial crime.

Governments, inter-governmental organizations and the global business community have asked, or have even gone so far as to require, accounting practitioners to contribute to the battle against money laundering in at least two ways.

First, most governments have enacted, or are in the process of enacting, laws and regulations requiring businesses to detect and report to the legal authorities any suspicious activity pointing to possible money laundering. Typically, business owners, directors and employees are obliged to do the same. Therefore, any accountant, regardless of role or certification, may be similarly

[1] International Auditing Practice Statement 1006 (IFAC: New York, October 2001), paragraphs 26-27.

subject to such requirements. Internal auditors who conduct or participate in compliance and operational audits, and accountants who have managerial responsibilities for compliance and operational activities, may be particularly affected.

Second, many AML regimes, following the FATF and G-7 models, are requiring businesses to have compliance monitoring programs and to independently test the control environment and effectiveness of these programs. In some cases, internal auditors perform this independent testing.[2] Less frequently, external auditors are engaged to independently test compliance and to report to management and to regulators directly. A handful of governments have, however, enacted or are considering new laws and regulations that would require businesses to have independent audits of their compliance with local AML regimes. Such requirements have tended to take two forms: either an independent public accountant performs a compliance assurance engagement and directly reports the results to the business and the regulator, or the business performs a self-assessment and an external auditor provides assurance as to the integrity of the resulting report and its assertions. The nature of the engagement will also consider third parties' requests for reports. Hand in hand with these new requirements, the governments are also encouraging leading practices in this area.

Whether or not national AML regimes impose specific duties on accountants, practitioners are, of course, subject to local accounting body standards and guidelines. Few IFAC members have, however, established auditing standards or guidance specifically focused on money laundering. Primarily, this is because, as will be discussed below in "Money Laundering and Financial Statement Effects," money laundering is far less likely to affect financial statements than are such types of fraud as misappropriations. Consequently, it is unlikely to be detected in a financial statement audit. Nevertheless, money-laundering activities may have indirect effects on an entity's financial statements and, thus, are of concern to external auditors.

Local and IAASB auditing standards governing auditors' responsibilities for detecting and reporting illegal acts and for evaluating the control environment are also germane to money laundering (because, at this point, money laundering is considered an illegal and criminal act in most jurisdictions). The upcoming section "Ties to Fraud" will discuss how conditions and control deficiencies that may contribute to frauds going undetected may similarly contribute to money laundering going undetected. As this section will establish, however, money laundering and fraud have more differences than similarities.

Again, while external auditors and reviewers of financial statements are unlikely to encounter signs of possible money laundering, other professional accountants may have greater exposure. The section "Professional Accountants' Roles, Professional and Ethical Obligations and Risks" identifies accounting occupations that will be affected, and this paper will be of greater relevance to them.

[2] This work is frequently outsourced to subject matter experts (SMEs).

Background and Understanding

Money Laundering Defined

Money laundering is the funneling of cash or other funds generated from illegal activities through legitimate financial institutions and businesses to conceal the source of the funds. Money laundering is a global activity that, like the illegal activities underlying it, seldom respects local, national or international borders. As mentioned previously, current estimates of the size of the global annual "gross money laundering product" range from $500 billion to $1.5 trillion.[3] Only within the past dozen years or so has the world community begun to recognize the threat money laundering poses to the orderly and open development of international financial systems and world trade.[4]

While the activities and methods of money laundering have become increasingly complex and ingenious, its "operations" tend to consist of three basic stages or processes — placement, layering and integration.

Placement is the process of transferring the proceeds from illegal activities into the financial system in a way that financial institutions and government authorities are not able to detect. Money launderers pay careful attention to national laws, regulations, governance structures, trends and law enforcement strategies and techniques to keep their proceeds concealed, their methods secret and their identities and professional resources anonymous. Common placement techniques include the structuring[5] of cash payments through legitimate bank and other financial institutions, which may involve deposits or money transfers, or the purchase of money orders, cashiers or travelers' checks or other monetary instruments.

Layering is the process of generating a series or layers of transactions to distance the proceeds from their illegal source and to obscure the audit trail. Common layering techniques include outbound electronic funds transfers, usually directly or subsequently into a "bank secrecy haven" or a jurisdiction with lax record-keeping and reporting requirements, and withdrawals of already-placed deposits in the form of highly liquid monetary instruments, such as money orders or travelers checks.

Integration, the final money-laundering stage, is the unnoticed reinsertion of successfully laundered, untraceable funds into an economy. This is accomplished by spending, investing and lending, along with cross-border, legitimate-appearing transactions.

The world's largest and wealthiest economies tend to serve as the primary hosts for money launderers and their operations. These economies generally harbor the greatest demand for illegal drugs, which is still the primary money-laundering activity. Also, to successfully place, layer and

---

[3]By definition, money launderers are in the business of cloaking their activities and revenue in secrecy, making approximation difficult.

[4]Alan S. Abel and James S. Gerson, "The CPA's Role in Fighting Money Laundering," *The Journal of Accountancy* (AICPA: New York, June and July 2001).

[5]"Structuring" in this context means breaking up large amounts of currency into smaller amounts for use in further transactions to avoid regulatory reporting requirements, suspicion and detection.

integrate their illegal proceeds, the more sophisticated money launderers look for a similarly sophisticated financial services sector.

Emerging financial markets and developing economies are also important targets and easy victims for money launderers, who continually seek out new places and ways to avoid the watchful eye of the law. The consequences of money-laundering operations can be particularly devastating to developing economies. Left unchecked, money launderers can manipulate the host's financial systems to operate and expand their illicit activities. Apparently legitimate, but criminally owned, businesses financed by laundered capital can quickly undermine the stability and development of established institutions.

Money launderers and their colleagues are often highly intelligent and well-informed criminals, who are able to quickly adapt and change their *modus operandi* to cope with a growing global profusion of AML laws, regulations and initiatives.

Money laundering is not just about cash and other monetary instruments; neither is it a problem isolated to conventional deposit taking and lending institutions and activities. Money launderers have greatly diversified their operations across financial services sectors and, increasingly, across the core and non-core financial activities of non-financial services businesses.

The OECD Financial Action Task Force

In 1989, the Group of Seven Industrial Democracies (G-7) created a global money-laundering watchdog organization called the Financial Action Task Force (FATF), with an Organization of Economic Cooperation and Development (OECD) Secretariat in Paris. In 1990, the FATF issued its first annual report, containing its now-famous *FATF 40 Recommendations* on actions for governments to take to combat money laundering.

These 40 recommendations fell into three categories:

> *Legal:* What law-making bodies need to do create an overall legal framework to combat money laundering. For example, the first legal recommendation was that governments criminalize money laundering in its own right, and not merely in connection with drug trafficking.
>
> *Financial Regulatory:* How governments should regulate their financial systems. An important example is that governments should require financial institutions to report suspicious activity to authorities. To make this work, governments would need to enact safe harbors to indemnify businesses and employees.
>
> *International Cooperation:* How governments should work together. For example, they should collaborate and exchange information in criminal matters and enter into bilateral treaties to facilitate asset seizure and forfeiture and the sharing of proceeds.

The *FATF 40 Recommendations* are still the most important set of international AML standards and have been a substantial force in encouraging government AML initiatives. In June 2003, the FATF issued a report revising and augmenting the 1990 Recommendations.[6] Today, FATF membership includes 33 jurisdictions and several other IGOs, including the international lending

[6] *The* 40 *Recommendations* (Paris: The Financial Action Task Force on Money Laundering, June 2003).

agencies. The FATF conducts mutual evaluations of members' progress in implementing the *FATF 40* every four years, and also assesses the cooperation of other nations in combating international money laundering. There are also regional FATFs, such as the Caribbean Financial Action Task Force (CFATF), which has similar goals and objectives. The FATF also publishes annually an update of *Money Laundering Typologies*, providing refreshed assessments of money laundering risks and techniques.

The accounting profession can and does contribute to the *FATF 40* in two compelling ways:

- The "General Framework" recommendations call for transparency and multi-lateral cooperation. Promoting transparency is a mission-critical objective of the profession and, as the worldwide organization for the profession, IFAC is the enabler for multi-lateral coordination and cooperation.
- The *sine qua non* of the "Financial System" recommendations are record-keeping, reporting and promoting transparency. These recommendations emphasize the importance of controls, systems and audit trails. Clearly, these are matters that speak to the core competencies of the profession.

Other Inter-Governmental Organizations

Beyond FATF and the regional FATFs, a number of other IGOs increasingly play global and regional AML roles, ranging from technical guidance and assistance, facilitation of regulatory and enforcement efforts, and information exchange. Appendix I provides a brief compendium of the major IGOs of consequence, along with their corresponding, relevant guidance.

Financial Statement Effects

Money launderers tend to use business entities more as a conduit than as a means of directly expropriating assets. For this reason, money laundering is far less likely to affect financial statements than are frauds such as misappropriations. Consequently, money-laundering activities are unlikely to be detected in a financial statement audit. In addition, while most frauds result in the loss or disappearance of assets or revenue, money laundering involves the manipulation of large quantities of illicit funds to distance them from their source quickly and in as undetectable a manner as possible. Because money-laundering activities may, however, have indirect effects on an entity's financial statements, they are of concern to external auditors.

The Going Concern Assumption

An important issue for accountants to consider is whether and how money laundering can potentially affect the going concern assumption.

Experience provides five important examples of where going concerns were seriously threatened, or even toppled, as a result of being exploited by money launderers:

- Where law enforcement seized and shut down a going concern for being owned and operated by money launderers or by being highly exploited by them (e.g., money service businesses, especially retail currency exchange houses, automobile dealerships and certain gaming establishments).
- Where a going concern was a sham operation owned or operated by money launderers whose intentions were never to operate the enterprise in perpetuity in the first place; money

launderers and their accomplices will inevitably vanish into the sunset with little warning and difficult-to-detect trails.

- Where law enforcement seized assets in the belief that illicit proceeds were in the process of being laundered or that such assets were linked to suspected terrorists or other persons, organizations and even governments subject to national interdiction, economic or military sanctions. The seizing and freezing of material assets in the laundering pipeline may seriously threaten a going concern's operations, liquidity and, of course, reputation. Similarly, law enforcement has, on numerous occasions, intercepted and arrested principals and employees thought to be laundering funds or aiding and abetting money laundering. In many cases, they emptied out whole offices for indefinite periods of time, resulting in major business interruptions or failures.
- Where regulators revoked business charters (e.g., bank charters) because an enterprise failed to demonstrate good governance, safety and soundness, or failed to remediate serious control deficiencies identified in the course of examinations.
- The increasing importance regulators place on money laundering risk assessment, performing more in-depth customer due diligence in establishing business relationships and enhancing scrutiny in executing transactions may also have an impact on the going concern. Businesses that in fact constitute, or are regarded to be, in higher-risk categories, e.g., money service businesses, may be denied access to financial services, funds or credit required to sustain their livelihood and even their existence.

Finally, in all cases, associations or merely alleged associations with money laundering can cause significant and even fatal damage to a business's reputation.

Indications of Possible Money Laundering

Money launderers use many different and sophisticated types of schemes, techniques and transactions to accomplish their ends. While it would be difficult to describe all money laundering methodologies, the following are the more frequently observed signs of suspicious activity:

- broadly, transactions that appear inconsistent with a client's known legitimate (business or personal) activities or means; unusual deviations from normal account and transaction patterns;
- any situation where personal identity is difficult to determine;
- unauthorized or improperly recorded transactions; inadequate audit trails;
- unconventionally large currency transactions, particularly in exchange for negotiable instruments or for the direct purchase of funds transfer services;
- apparent structuring of transactions to avoid dealing with identification requirements or regulatory record-keeping and reporting thresholds;
- transactions passed through intermediaries for no apparent business reason; and
- introduction of a client by an overseas associate or financial institution based in a country or jurisdiction known for drug trafficking and production, other financial crimes and "bank secrecy."

Appendix 2 provides other indications of possible money laundering. Governments, IGOs and trade associations also publish considerable guidance on this subject.[7]

KnowYourCustomer, Suspicious Activity Reporting and Tipping Off

An important element and theme of the FATF model and a number of FATF members' AML regimes, the Wolfsberg AML Guidelines and the Basel Committee's Customer Due Diligence for Banks are the KYC principles.[8] The primary objective of KYC principles is to enable effective identification and reporting of suspicious activity.[9] The underlying assumption is that, unless you truly know your customer, and well enough to understand and anticipate that customer's business behavior, you can neither reasonably nor effectively distinguish unusual and possibly suspicious activity from usual and customary behavior. KYC guidelines require or recommend developing a thorough understanding, through appropriate due diligence, of the true beneficial parties to transactions, the source and intended use of funds and the appropriateness and reasonableness of the business activity and pattern of transactions in the context of the business.

Regulators and law enforcement increasingly expect businesses and their professional accountants to expand the concept of KYC to include "KnowYourEmployee," "KnowYourAgent" and "KnowYourCorrespondent" and, increasingly, "KnowYourThirdPartyServiceProvider."[10] Through their considerable experience, they have learned that money laundering is directly perpetrated or facilitated by "blindness" on the part of employees and principals alike. Many businesses and their owners have proven to be not what they first appeared to be.

Most FATF governments and many others have enacted and implemented, or are in the process of implementing, SAR or Suspicious Transaction Reporting (STR) models as an essential component of their overall anti-money-laundering regimes. As FATF learned and recommended early on, SAR/STR is far more effective and reinforced when two other legal conditions are simultaneously established.

The first condition is that SAR/STR laws should provide a safe harbor. This means indemnifying businesses, their principals, employees and, often, their agents against lawsuits launched by suspects learning that reports of suspicious activity have been made about them. The second condition is that there should be a corresponding ban imposed on "tipping off" any suspects that their activities may be viewed as suspicious and reported to the authorities. Clearly, SAR/STR would be of limited value to law enforcement if suspected money launderers were tipped off

[7] For example, *Suspicious Activity Review* (Washington: The U.S. Treasury Department).

[8] The terms "Customer Due Diligence" (CDD) and "Enhanced Due Diligence" (EDD) are also used in connection with KYC. In many jurisdictions, regulators increasingly expect financial institutions to perform EDD connected with assessed higher risk.

[9] The revised FATF recommendations urge governments to ensure that financial institution secrecy laws do not inhibit implementation of the KYC principles. In addition, FATF now recommends the application of additional KYC procedures in relation to PEPs, and that financial institutions pay special attention to any money laundering threats that may arise from new or developing technologies that might favor anonymity.

[10] More recently, law-makers and regulators have increased their focus on correspondent banking relationships as targets for money launderers. It is not uncommon, particularly in the securities and investment management sectors, to rely on external transfer agents, clearing brokers and other third parties for a host of record-keeping and reporting services.

while being monitored. Governments imposing SAR/STR rules have tended to include provisions to annul the safe harbor when, for example, it can be proven that a principal or employee of the reporting entity has, in fact, tipped off the suspect.

Accountants should be aware that the statutory definition of the crime of money laundering and, even more so, the predicate offenses that are held to generate illicit proceeds, vary considerably among jurisdictions.[11] Accordingly, and not always in a clear *a priori* manner, there can be wide variation in what constitutes unusual and suspicious activity and legally reportable conditions of suspicious activity. Given this variation, it is not hard to imagine scenarios where an activity that may be illegal and reportable as suspicious in one jurisdiction may not be (or not be so clear cut) in another. In particular, it is not unusual for a financial institution with global operations to encounter jurisdictional inconsistencies – i.e., between the home and the host jurisdictions – and, hence, potentially conflicting responsibilities and requirements.

For these reasons, accountants should familiarize themselves with the legal and operative definitions of money laundering, predicate offenses, unusual and suspicious activity and reportable conditions that apply to the entities in question in jurisdictions of consequence. Because governments are increasingly broadening the spectrum of reportable conditions, professional accountants should be aware that entities may need to expand their scope of monitoring for, and reporting of, suspicious activity to cover certain types of frauds, including even identity theft and computer intrusion. Typically, the foreign operations of an international business are subject to the compliance requirements of both home and host country, unless there are conflicts that transcend mere differences. Also, professional accountants should acquaint themselves with IGO guidance, in particular, the FATF money laundering typologies, which attempts to establish global definitions and criteria.[12]

Finally, most legal systems that require identification and reporting of suspicious activity stress the importance of deploying sound judgment in applying these definitions, in particular, “unusual” and “suspicious.” With near ubiquity, these terms are strongly contextual and highly judgmental. This should come as welcome news to professionals who are trained and reputed to be masters of deploying sound professional judgment.

Vulnerability of Banks, Non-Bank Financial Institutions and Other Entities

Until recently, core banks, or conventional deposit taking and lending institutions, were the primary targets of money launderers. As banks improved their controls for preventing, detecting and reporting money laundering, however, and as law enforcement has made similar strides, criminals have learned to diversify their operations and to expand into other financial institutions or conduits of financial activity.

Other types of businesses that are vulnerable include:

- securities and commodities brokers or dealers;

[11] FATF’s first legal recommendation was that governments should criminalize money laundering in and of itself, apart from the predicate offenses that generate illicit proceeds. Many governments have adopted this recommendation and, consequently, have money laundering and numerous predicate activities spelled out in their criminal codes. The most common means to prosecute money laundering was, and still is, through the predicate activity of drug trafficking.

[12] The FATF Annual Reports on Money Laundering Typologies. www.oecd.org/fatf

- investment companies surrounding mutual fund complexes;
- currency exchange houses;
- casinos (including tribal casinos) and card clubs;
- issuers, redeemers or cashiers of checks, travelers checks, money orders or similar instruments;
- money transmitters;
- postal systems;
- insurance companies;
- dealers in precious metals, stones or jewels;
- pawnbrokers;
- loan or finance companies;
- travel agencies;
- dealers and sellers of automobiles, airplanes, boats and other vehicles;
- persons who close and settle real estate transactions;
- informal exchange networks, e.g., “hawalas”;
- federal, state or local government agencies with duties or powers similar to financial institutions; and
- businesses that engage in significant international trade (import/export).

As regulators and law enforcement have tried to keep pace with money launderers, they have recommended to legislators that the field of scrutiny and compliance requirements be enlarged. As a result, record-keeping, reporting and other control requirements first directed at core banks are generally being expanded to include other industries and sectors. Professional accountants should be aware that these businesses are vulnerable and should monitor rapidly evolving anti-money-laundering regimes in this regard.

Ties to Fraud

Two important characteristics of money laundering clearly distinguish this activity from fraud. Because of the conduit phenomenon, money laundering is far less likely to affect financial statements (as indicated above) than is the broad spectrum of frauds. A second important distinction is that fraudulent activity usually results in the loss or disappearance of assets or revenue, whereas money laundering usually generates large quantities of illicit proceeds that need to be distanced from their source as quickly as possible in an undetected manner.

Nevertheless, many conditions and control deficiencies that may contribute to fraud vulnerability may also contribute to money laundering vulnerability. Prominent among these are:

- the lack of a strong control environment, particularly, raising questions about the competency, integrity and tone-at-the-top of principals and senior management;
- the lack of strong regulatory compliance and risk management functions or departments;
- the lack of a related, independent, internal audit compliance program;
- signs of evasion or non-conformity with any internal anti-money-laundering controls;

- previous examiners' or auditors' reports, memoranda of understanding and past administrative and enforcement actions citing compliance problems, control deficiencies and concern over management's competence;
- significant revenues stemming from, or assets or liabilities associated with, "high risk" jurisdictions, notably "bank secrecy havens," and abnormally high electronic funds transfer activity from and to high-risk jurisdictions, and with insufficient controls;
- significant revenues from, or connected with, higher-risk businesses and individuals, products and services and distribution channels;
- a lack of background checks on new hires;
- weak or non-existent ethics policies and related training programs; and
- unreasonably infrequent or non-existent reviews of security software and systems.

Ties to Corruption, Terrorism and Politically Exposed Persons

Governments and IGOs now believe that there may be links between the proceeds of foreign official corruption and terrorist financing and the crime of money laundering. In several cases, they have enacted new laws to deal with this possibility, especially where the proceeds involved were generated by specified unlawful activities.

Guidance on best practices to comply with such guidance and laws includes:

- The *Wolfsberg AML Principles* issued by 11 major international private banks and Transparency International in October 2000.[13] One of these principles specifically addresses the connection between money laundering and the bribery of public officials.
- *Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption*, issued jointly by Treasury and US bank regulators, establishes a closer link between money laundering and corruption. This document encourages financial institutions "to develop and maintain enhanced practices and procedures designed to detect and deter transactions that may involve the proceeds of official corruption by senior foreign political figures, their immediate family, or their close associates" (PEPs).

A number of governments are considering or have enacted new legislation to clearly define corruption as a predicate offense to money laundering. [14]

Bank Secrecy and Consumer Privacy

New privacy laws in the European Community and the US are fundamentally about consumer protection. These rules frequently, albeit unintentionally, run counter to anti-money-laundering legislation. This is because, consistent with FATF recommendations, AML laws generally require businesses to create, keep and often report information about customers, especially suspicious activity. New privacy laws, on the other hand, require elaborate disclosures about why and how customer information is collected and maintained, and limit an institution's ability to share that

[13] *Global Anti-Money-Laundering Guidelines for Private Banking* (Wolfsberg, Revised May 2002).

[14] For example, the USA PATRIOT Act of 2001, Section 315, *Inclusion of Foreign Corruption Offenses as Money Laundering Crimes*.

information.[15] The KYC rule "KnowYourCustomer" is about transparency. Privacy is, by its very nature, at odds with transparency. A new challenge for businesses and the professional accountants who advise them is to reconcile the two requirements and comply with both areas of the law in an optimal way.

Application of Risk-Focused Supervision

The Basel Committee of the Bank of International Settlements and most of the major national financial institution regulators of the world have adopted fairly consistent models of risk-focused supervision. Most of these models define from six to 10 risk categories. Some of these categories, for example, liquidity risk and interest rate risk, have little if anything to do with money laundering and related financial crime. However, four risk categories universal to most models – compliance, operational, reputational and strategic risk – apply squarely to money laundering.

Compliance Risk

Most major international businesses, especially banks and non-bank financial institutions subject to risk-focused supervision, clearly understand that money laundering represents a major compliance risk in sophisticated financial services centers. But many of them continue to struggle with two major money-laundering compliance issues. First, they tend to focus more on AML record-keeping and reporting rules and less on compliance program development and management. Second, they are frequently confused about what are clearly-articulated KYC rules, what are implied rules and what are otherwise best practices in money-laundering risk management.

KYC standards are particularly important because of the rapidly spreading requirement to report suspicious activity. As discussed earlier, systems of suspicious activity reporting can be neither effective nor compelling without an enterprise-wide KYC regime and culture.

Whether or not KYC standards have been legally enacted, they certainly are generally becoming a "soft law" requirement or, at least, a best practice. Regulatory expectations are increasingly found in examination manuals, in supervisors' and governments' controllers' offices' guidance and pronouncements and in examination results that have led serious enforcement actions. Regulators around the world are accelerating their pace in evaluating internal controls and the scope, magnitude and effectiveness of their underlying KYC regimes.

Operational Risk

Operational or transactional risk is conventionally thought of as risk to a business arising from problems with service or product delivery. This risk is a function of internal controls, information systems, employee integrity and the many operating processes. This risk is also pervasive to products and services, assets and people, sites of operation, markets and distribution channels.

Of the four money laundering risk areas, operational risk is probably the most difficult to map out and yet the most pervasive. Financial institution supervisors increasingly expect management to assess those risks and implement controls to mitigate them on an enterprise-wide basis – across all businesses, products and services, jurisdictions and technologies. Money-laundering

[15] In the EU, in particular, privacy advocates wish to limit the government's access to customer information.

operational risk increases as conventional deposit taking and lending institutions transform themselves into omnibus providers of diversified financial services serving many marketplaces, with business processes, products and transactions all over the map. The more complex and varied the operations, the greater the operational risk.

Demonstrating to regulators that management is fully in control of its money-laundering operational risk is best achieved by documenting the risk assessment process, oversight and the related governance process. A "gap analysis" will map out, process by process, the inherent risks and the controls in place to manage those risks, and also identify control deficiencies requiring action or remediation. The outcome of such an exercise should be a remediation or action plan identifying priorities, resources and a timetable. Professional accountants are increasingly being asked to assist their clients or management with operational risk assessment.

Reputational Risk

"Reputational" risk as it relates to money laundering is very straightforward – it is event-driven and is almost always devastating. There are two basic types of money laundering events that can be very damaging to a business's reputation:

- a compliance failure (compliance risk) or major control deficiency (compliance or operational risk), resulting in bad examination results or even an enforcement action by a regulator and consequent bad publicity, and
- a direct money-laundering or terrorist financing scandal, or merely an alleged link to a money-laundering operation or transaction, resulting in a tangle with law enforcement and, worse, long-drawn out, adverse publicity.

During the past few years, law enforcement has become far more successful in identifying, investigating and prosecuting possible money-laundering activity connected with, or potentially facilitated by, a business, its principals or employees. Much of this success is attributed to the rapidly growing number of reports of suspicious activity being made by businesses, their principals and employees around the world. Law enforcement's growing knowledge about the money-laundering universe has resulted in a far greater likelihood of detecting a suspicious pattern of behavior of which a business itself may be unaware. As a result, there is also a growing likelihood of triggering reputational accidents, like a major money laundering scandal. To avoid such accidents, it is important to continually improve systems of internal control – or at least to acknowledge that a money-laundering "accident" occurred despite state-of-the art internal controls and compliance practices.

Strategic Risk

Finally, money-laundering vulnerability will manifest itself in strategic risk – the risk that a business is unable to effectively plan, implement and respond to changes and developments within an industry (e.g., competitive or regulatory changes) and within its own domain (e.g., introducing a new product). As the battle against money laundering gets more complicated and criminal activity becomes more difficult to detect, management's efforts in planning for monitoring systems, procedures and controls are ever more challenged, as is making business cases for new products, services and distribution channels. It is inevitably a strategic matter to decide whether or not to enter, or to continue in, a marketplace fraught with money-laundering

vulnerability and where the compliance, operational and reputational risks in that marketplace may be intolerable.

Application of the Integrated Framework of Control

The discussion that follows shows how the accounting profession's integrated framework of control (IFC) applies to money laundering.

Money Laundering and the Three Control Objectives

The IFC's compliance control objective has the most obvious and direct connection to money laundering or, more accurately, AML. Compliance is the theme most central to the *FATF 40 Recommendations*. For business entities that operate within the various legal and financial regulatory frameworks of the world, compliance is clearly a crucial success factor to achieving AML effectiveness. External compliance sets the stage for internal compliance, i.e., compliance with policies, procedures and systems (generally referred to by the IFC methodologies as "critical control activities").

The operations control objective also has an important AML aspect to it. Years ago, when money laundering was perceived to be "just about cash" and a vulnerability characteristic solely of conventional deposit-taking and lending institutions, the context of money-laundering operations was correspondingly more narrow. It encompassed only the operations surrounding cash handling and monitoring cash transactions. Today, this is no longer the case. Now, money launderers use all kinds of monetary instruments, electronic funds transactions, stored value, trade and a concomitant array of new technologies.

Our banks and non-bank financial institutions are rapidly becoming "omnibus providers of diversified financial services," and our non-bank, non-financial institutions are increasingly providing indirect financial services to support or facilitate their core business lines. Jurisdictional boundaries are becoming less important to the operations of all of the above.

Finally, operational control must also cover support operations – the functions and business processes that provide the fabric and glue that make business units function as an organism. Support operations include human resources, internal audit, risk management, compliance management, counsel, security, financial management and information technology. In a nutshell, money-laundering deterrence and detection are now pervasive to many aspects of operations.

The remaining IFC control objective, financial reporting, is, of course, the primary concern and focus of accountants, especially financial statement auditors. Nevertheless, as stated earlier, money laundering is unlikely to affect financial statements.

Money Laundering and the Five Control Elements

The prevailing IFC models generally define five elements of control: the control environment or foundation, risk assessment, control activities, information and communication, and monitoring. Each of these is briefly discussed and applied to money laundering below.

The control environment

The control environment determines the tone of an organization and how it operates. A healthy and effective business that has a positive tone at the top employs, deploys and retains competent people. It also espouses, communicates and reinforces positive cultural values such as integrity,

teamwork and accountability. The parallel between a healthy control environment and a pillar of money-laundering deterrence is nothing less than striking – it is frequently held that Control/KnowYourCustomer "is everyone's job."

While it's hardly the fault of businesses that there are financial criminals incessantly looking for ways to compromise their safeguards, those with healthy control environments are far better able to protect themselves. It is not a difficult message for principals and directors to convey: "Money laundering is a crime, it will not be tolerated and detection and deterrence is everyone's responsibility."

Risk assessment

The importance of risk assessment (the process through which management decides how it will respond to business risks that pose a threat to achieving business and control objectives) was dealt with earlier in the discussion of risk-focused supervision. While many types of non-banks are not subject to this sort of supervision, there is a clear trend in this direction, paralleling global financial services modernization, consolidation and convergence. Regardless, the four types of risks closely associated with money-laundering vulnerability – i.e., compliance, operational, reputational and strategic – are universal to most businesses, whether or not they are currently subject to risk-focused government supervision. It is, therefore, equally important that businesses have the capability and the mechanism for assessing risk, and that professional accountants, as employees or external accountants, be informed and be prepared to conduct or assist these efforts.

Control activities

Control activities are the policies, procedures and mechanisms in place to provide assurance that management's directives are carried out as intended. These activities are pervasive throughout business, and they align readily with the three control objectives: compliance, operations and financial reporting. A well-managed business has comprehensive polices, robust operating procedures and effective and efficient systems with well-integrated controls. Among the most potent weapons against money laundering are good anti-money-laundering compliance policies and procedures. Regulated financial services providers should be mindful that examiners and compliance auditors will assess those policies and procedures. Operating policies and procedures should have equal stature in the money-laundering prevention arsenal, but they tend to be less visible, less well understood and, consequently, less well adhered to. This is an area where businesses are often vulnerable.

Many businesses do not really understand that policies and procedures cannot be boilerplate – merely copying anti-money-laundering statutes and regulations and putting them in binders on shelves will achieve nothing. To be effective, control activities must be tailored very specifically to the organization's control environment and its risk tolerance. Designing, implementing, deploying and monitoring control activities of money-laundering deterrence compliance programs constitute an area where professional accountants have much to contribute.

Information and communication

Good information and effective, enterprise-wide communication are crucial elements of strong internal control. A business cannot function well without systems that capture, produce and

distribute timely, accurate and meaningful information. This area, unfortunately, is too often lacking.

Clear and open channels of communication go hand in hand with good information. Information that is not well communicated up, down and across the organization is no better than non-existent information. Channels of communication should also clearly articulate and reinforce roles and responsibilities for internal control, and precisely spell out how individual control responsibilities fit in to the whole.

Quite simply, effective money-laundering deterrence requires both the tools and the media. Employees need to carefully monitor external events, developments and conditions and to report them to management and directors. Management needs to have powerful and comprehensive information systems governed by strong human processes to monitor customer account and transaction activity. KYC principles require reliable information and the successful implementation of sound business processes. A formidable challenge for large, multi-jurisdictional, multi-service line "omnibus providers" is to be able to collect and communicate information across lines and jurisdictions. Similarly, an effective SAR system will require everyone in the organization to maintain good records and communicate effectively. Good money-laundering compliance and risk management will require continuous, reliable information about events and controls enterprise-wide.

Monitoring

There are three types of monitoring: (1) continuous monitoring during the normal course of operations; (2) separate management evaluation, either through a central or distributed compliance monitoring mechanism; and (3) internal or external auditing, which should independently test compliance and other controls to determine the extent to which they are effective. Deficiencies in anti-money-laundering compliance programs and integrated operational controls should be reported to senior management and audit committees for action. In this way, monitoring activities can be strong defenses against money laundering.

Professional Accountants' Roles, Professional and Ethical Obligations and Risks

As pointed out earlier, external auditors performing financial statement audits are less likely than other professional accountants to encounter signs of possible money laundering. Reviewers of financial statements, whose work does not generally include evaluating the control environment, are even less likely than auditors to detect signs of possible money laundering. But accounting professionals acting in the following capacities are more likely to encounter such evidence:

- accountants in management positions who record and report entity transactions, such as CEOs, COOs, CFOs, CIOs, controllers, risk managers, compliance officers and related staff;
- in-house financial systems consultants;
- internal auditors responsible for operations and compliance auditing;
- practitioners who provide outsourced regulatory examination services;
- forensic accountants;
- public practitioners who perform compliance and operational audits;

- risk management professional accountants and compliance specialists;
- tax practitioners, especially in jurisdictions where filings connected with anti-money-laundering laws (currency transaction and SAR) are directed to tax authorities.

Businesses, especially bank and non-bank financial institutions operating in FATF-40 compliant jurisdictions (often because regulators have suggested or required it), are increasingly asking practitioners to conduct money-laundering risk assessment exercises. This is because financial institution supervisors expect or require businesses' assessments to serve as a blueprint for an AML strategy and controls. Practitioners, as business process and control professionals, are frequently asked to assist these efforts, or to review these strategies, their resulting programs and their effectiveness.

In addition, practitioners are being asked to conduct "best practice" reviews, compliance reviews and special audits. Obviously, professional risk at stake varies with the level of assurance required. In an extreme example, assuring that even one's own personal bank accounts are invulnerable to money laundering would be a difficult proposition.

More and more, governments are requiring businesses to have AML compliance programs that monitor for compliance, and independent testing (by internal or external auditors) to audit those programs.

Several governments are debating whether to require financial statement auditors (as well as lawyers) to report directly to regulators any suspicious activity detected in connection with client work. There are two major concerns here: (1) fundamentally, a financial statement auditor must always have free and open access to a client's books and records, which could be significantly impaired by such a requirement; and (2) among the many types of accounting practitioners, external auditors are least likely to encounter money-laundering activity (discussed earlier). Also, it should be underscored that accountants who are employees (and frequently internal auditors) of banks and non-bank financial institutions required to report suspicious activity are themselves already subject to this requirement.

Governance, Management Oversight and Reporting to Senior Management and the Board

As is the case for many domains of risk and regulatory compliance, regulators expect to see compelling evidence that bank and non-bank financial institutions govern themselves well. An essential dimension of AML good governance is to have principals and business executives who are well informed about key aspects of AML compliance, risk management and events that may require their attention, policy and program decisions, and other actions.

Principals and senior managers should never be in a position of being surprised by compliance deficiencies, or external sources exploiting their organization for money laundering purposes or instigating other reputation-damaging events. To prevent such surprises, they should ensure that they are up to date on all AML risk management and compliance matters affecting their organizations. Moreover, regulators and law enforcement expect them to be well versed and knowledgeable in this area. In fact, in many jurisdictions, principals and senior managers are potentially criminally liable for serious compliance deficiencies – including "willful blindness" – that could result in enforcement actions. At the same time, they should not be bombarded or

overwhelmed with large volumes of detailed reports that could cloud key points and impair clear thinking on policy, program and other actions. Information should be sufficiently high-level and meaningful – all consistent with IFC principles.

Boards vary considerably in respect of size, constitution and committee structure. They are increasingly differentiating functions and, more often than not, they assign to the audit or risk management committee the oversight of AML compliance and risk management programs. Regardless of committee structure, senior managers should make meaningful presentations on the state of AML compliance, risk management and significant matters to all principals.

Whether or not legally required in a jurisdiction, leading practices in AML governance recommend the following:

- Board or audit committee policy setting and reaffirmation of written AML compliance program. Policy statements should articulate an organization's subject matter risk tolerance (e.g., what are the criteria and thresholds for not accepting new customers – where do you draw the line?), addressing the primary money laundering risk criteria.[16]
- AML, KYC, anti-corruption and anti-terrorist, risk assessment, SAR/STR, and information-sharing policies and procedures.
- Corporate Code of Ethics – statement of AML policy and responsibility.
- Formal designation of an AML compliance/money laundering reporting officer (MLRO).
- Training and awareness program.

The Board should periodically review and revise its strategic plan that assesses AML risk in the customer base, geographies, jurisdictions, products and services, distribution channels, service providers, mergers and acquisitions, strategic alliances and deployment of new technologies. The Board needs to get clear and meaningful business and customer profile information so that it clearly understands, and demonstrates understanding of, the customer base and segments, channels and jurisdictions of operation (lots of pie-charts), particularly highlighting higher-risk customers, areas and issues.

Counsel, Compliance Management, and Risk Management should periodically report to the senior management team and the Board on risk and potential institutional and individual potential criminal liability, and important legal cases in this area.

Principals and senior managers should be kept apprised of:

- AML reputational events as soon as they happen, e.g., negative press about a customer, counterparty or an employee;

[16] The AML policy-framework "frames" the entire program. This framework is separate and distinct from two other crucial written compliance program components, i.e., enterprise-wide guidance and standards and detailed, implementing operating policies and procedures. The written AML compliance program should neither get nor appear to get stale.

Principals and senior managers must be well informed about, and engaged in discussions about, AML risk criteria, risk thresholds and risk tolerance. These discussions should be well documented – supervisors (examiners) will be keenly interested in the principals' and senior managers' understanding and articulating money laundering risk and defining and accepting responsibility for risk tolerance setting.

- reputational and compliance events and law enforcement actions made public, adversely affecting other institutions ("Look what happened over at ____. Could that happen to us?");
- subpoenas and significant regulator and law enforcement requests or inquiries;
- communications with regulators and law enforcement about money laundering and AML, known or suspected terrorists or other criminals circulated by law enforcement agencies on "control lists," and PEPs;
- penalties assessed resulting from compliance failures or alleged compliance deficiencies;
- periodic reports on cases and number of cases (investigations) in the works;
- account closures or pending account closures;
- SARs/STRs in progress and reports filed to authorities (the written SARs/STRs themselves, by the way, should never leave the organization except for filing with law enforcement);
- any other reportable conditions;
- volumes of reports filed:
    - new account activity;
    - legal, regulatory and administrative changes, notices of proposed rule making of consequence, and periodic reports on complying with and implementing new laws and rules. Also, direct or professional association participating comments and correspondence;
    - the status of AML training among employees, employee certifications (principals themselves may be required or recommended to undertake periodic AML training and awareness sessions);
    - identification and reporting of potential terrorists or parties subject to national interdiction laws or economic sanctions;
    - AML risk assessment activities and their results;
    - significant AML compliance program activities or changes, e.g., program expansion, terminations and new hires, new or changes in business processes or systems and anticipated impact;
    - AML related examination activities and findings, matters requiring follow-up action and remediation, action item plans and progress on remediation action items; accounts of meaningful examiner discussions and examiner/supervisor correspondence. Also, periodic updates on the status of the continuous examination management plan;
    - the results of AML compliance reviews and management responses, including remediation plans;
    - the results of AML audits (independent testing) and management responses, including remediation plans;
    - the results of customer data quality assessments and remediation activities;
    - periodic update on the status of KYC responsibilities embedded in employee job descriptions and how employee compliance performance is assessed and compensated.

Senior management and Board meeting agendas should be circulated in advance and clearly highlight any AML matters slated for presentation and discussion, and the minutes of these meetings should clearly indicate that discussions took place and document their outcomes and action items. (Examiners will review these minutes carefully and ask for evidence that action items were followed up on.) Directors should have the opportunity to review and accept the minutes of these discussions.

Auditing AML and Suspicious Activity (Transaction) Reporting Programs

Entities sometimes retain an auditor to provide an independent review of AML and suspicious activity (transaction) reporting programs. This auditor may be the same individual or firm as performs the financial statement audit. Before accepting such an engagement, the financial statement auditor would consider the exact nature of the AML engagement and whether there are independence conflicts that prevent acceptance. The auditor's objectives include:

- Assisting financial institutions and other organizations with addressing their statutory or regulatory requirements (depending on the various requirements of jurisdictions) for independent testing of their AML and SAR/STR programs, processes and controls.
- Similarly, assisting business organizations in meeting parallel requirements imposed through contracts, or as conditions for, establishing and maintaining business relationships and for conducting transactions.[17]
- Identifying material program weaknesses, control deficiencies and opportunities for program, process and control enhancement, and reporting them to senior managers and audit committees/principals.
- Assisting senior managers with identifying money laundering and other financial crime vulnerability.
- Performing work that may be useful to regulators in conducting their supervisory examinations.[18]

Here are some criteria and leading practices that auditors may wish to consider in developing and administering an audit program to review and independently test AML SAR/STR programs.

The internal environment. Before drilling down into relevant business processes and controls, auditors should consider the "big picture" – the organization's overall internal control environment as it pertains to AML and SAR/STR. This means getting a sense of the "tone-at-the-top" of the organization – principals' and executives' attitude, posture and message about integrity, ethical values and competence. Are the right messages sent internally and externally about the importance of complying with the letter and spirit of the law and about protecting the

[17] For example, mutual fund complexes and introducing brokers are increasingly requiring independent audits of the AML and SAR/STR programs of their external service providers (transfer agents and clearing brokers), who maintain their books and records and who prepare and file their statutory reports but who themselves may not be subject to AML and SAR / STR program requirements. And, for example, money service businesses that may be considered higher-risk customers for their financial services providers are frequently required to undertake independent AML and SAR/ STR program audits.

[18] Note: Absent statutory or regulatory requirements, supervisors may be neutral as to whether AML program audits should be performed by internal or external auditors. What they *do* care about is the quality of the work, i.e., that the work is performed by seasoned professionals with appropriate technical AML expertise.

enterprise, its people, assets, operations and reputation from money launderers, money laundering and related financial crime? Does the Board-approved policy framework (a "should-be") contain a clear policy for, and commitment to, assisting global efforts to combat money laundering and related financial crime? To "KnowYourCustomer?" To monitor for and report suspicious activity/transactions? Does one get a sense from meeting with employees that these values are effectively communicated and shared? Do employees across the enterprise have a positive attitude, understand what unusual and suspicious activity is and the importance of identifying and reporting it to management? Do they know what to do and whom to contact? How frequently does the subject matter show up on internal communications?

Written compliance program. Auditors should look for evidence of AML and SAR/STR compliance program documentation about unusual and suspicious activity identification and reporting at three levels:

Level I: Board-approved policy framework (see above). Auditors must gain an understanding of the specific AML statutory and regulatory requirements that apply to the enterprise. For example, is the entity required to comply with SAR/STR rules enterprise-wide, or is there a voluntary SAR/STR policy anticipating future requirements or because senior management and the board believe that they are doing the right thing regardless of requirements? Do the policies fully comply with external requirements? Are aspects of the policy more stringent than required? (An SAR policy that exceeds the enterprise's regulatory requirements is perfectly acceptable – it reflects a more conservative risk appetite, which few would question. It is important, however, to understand what it is). Auditors should also review the agendas and minutes of senior management and board meetings to determine whether the right discussions and actions are taking place to support a well-considered policy framework and to get a sense of future plans or intentions to review or modify the policies.

Level II: Enterprise-wide standards and guidance. Auditors should determine what enterprise-wide standards and guidance are articulated and promulgated by senior managers and principals that underlie and glue together an enterprise-wide AML and SAR/STR program. Does management communicate to employees the conduct and response that is expected of them? Is internal and external subject matter guidance well communicated and accessible? How well do senior managers and principals articulate and convey the importance of KYC principles and provide guidelines on how to apply them to the organization? Are employees encouraged to seek out and stay abreast of external guidance? How frequently do they actually do this?

Level III: Implementing, operating policies and procedures. Many business organizations confuse policies with procedures, as is frequently evident from reviewing compliance program documentation. Accounting professionals, therefore, frequently assist their clients with revising their written compliance programs accordingly. Here's the distinction in a nutshell: policies are the "what" and procedures are the "how." Successful *implementing and operating* policies and procedures will robustly apply the Board-approved policy framework and the enterprise-wide standards and guidance to each of the business units and support areas of consequence. In other words, each of these areas should have a set of tailored policies and procedures that clearly describe how the overall AML policies, standards and guidance for the enterprise as a whole applies to them – the types of unusual and suspicious activity likely to be encountered, roles and responsibilities, specific operating procedures and controls. Are the required actions and follow-

up clearly articulated? What information should be produced and what are the appropriate channels of communication?

Robust risk assessment process. In the realm of money laundering and anti-money laundering, one size does not fit all. AML programs need to be tailored. Business processes and controls need to be business- and risk-based. Business units need to assess what types of unusual and suspicious activity are more likely to occur and what employees are more likely to encounter in their respective areas. To get a good sense of whether an enterprise has a sound risk assessment process in place, auditors should look to see whether there is a hands-on, sustainable AML committee, usually chaired or coordinated by the AML compliance officer and made up of individuals who properly represent the business units and support areas of consequence. Among their committee obligations and assignments, members should be actively engaged in periodic risk assessment and reporting results to the committee. The output of risk assessment should be a blueprint for the types of unusual and suspicious activity that the employees of respective areas are more likely to encounter. Management should prepare a risk assessment survey (designed with SAR/STR or other reportable conditions in mind) for the committee to administer. In particular, this exercise should be valuable for engaging employees in the risk assessment process, with the obvious, hoped-for benefits. Therefore, a robust risk assessment exercise is an important way of determining whether an AML program is suitably designed and operating effectively.

Also, it is a leading practice for an enterprise-wide AML and SAR/STR program to be active (as opposed to passive) and pre-emptive. The more effective program is one characterized by high-energy outreach versus one where management passively waits for internal reports to (maybe) come forward. Getting to and sustaining the state of “high-energy active” requires continuously deploying the other program elements and identifying and engaging opportunities for continuous improvement.

Risk profiling and benchmarking. As part of the risk assessment process, it is a good idea to periodically compare the enterprise’s SAR/STR performance with industry performance. The results should be reported to senior management. Auditors may wish to make an independent determination and compare it to management’s. It is important for compliance management to highlight, report and explain material SAR/STR filing variances to senior management. There are usually very compelling reasons for variances – everyone has a different risk profile and no two enterprises have the same profile of customers, products and services, geographies, distribution channels, employees and other business relationships. It is, however, a good idea for senior management to articulate the enterprise’ risk profile in any event and to explain SAR/STR filing performance variances in the context of that profile. Supervisors and law enforcement may walk in the door with a set of expectations concerning character and volume of SARs and STRs, and senior management should be prepared to present, discuss and explain their filing performance.

Training and awareness. Training and awareness programs are perhaps the most consistent and universal AML program requirement. Ideally, auditors should evaluate the quality and relevance of the AML program. They should assess the effectiveness of training by talking to employees and reviewing test results where applicable. Training materials should show signs of freshness and meaningfulness.

Centralized SAR / STR reporting. While it is rarely a specified regulatory requirement, it is generally a good practice to designate one person to be responsible for directing SARs/STRs to law enforcement. Ideally, an enterprise will have an internal mechanism for employees to report suspicious transactions, events or situations that is separate and distinct from the report that may ultimately be filed with authorities. There should be controls in place to make sure that only specifically authorized and designated individuals are part of the event escalation, analysis and reporting stream. Regulators and law enforcement expect to see SAR/STR filings and other reports to come from one or very few designated individuals – usually an AML compliance officer or MLRO. Auditors should test reports filed to determine whether these procedures are being followed and should note exceptions. They should also ask for process flow charts or descriptions of reporting process flows and then test them to see if they are functioning as designed.

For frequently compelling and also "legacy" reasons, omnibus providers of diversified financial services often have distributed or fragmented record-keeping and reporting processes, often with corporate security (internal law enforcement) handling fraudulent reporting and compliance management handling the money laundering, structuring and related SARs/STRs (or a distinction is made between internal and external reports). While this approach may work well in many respects, process fragmentation may more easily foster control deficiencies. Suspicious reports and their supporting cases may fall through the cracks, and "need-to-know," while important to the objective of confidentiality, frequently becomes a barrier to the balanced level of communication required for effective safeguards and risk management.

Sound Judgment and Quality Reporting Process. As indicated above, it is important to distinguish the internal detection and escalation process from the external reporting process. Employees should be sufficiently trained and engaged, and written policies and procedures should be sufficiently clear and robust, to ensure effective internal detection, reporting and escalation. Typically, employees prepare an internal report of unusual or suspicious activity in consultation with a supervisor and the designated compliance liaison. The internal report is then escalated for analysis and investigation (i.e., the internal report becomes a *case*) that is tracked and then quickly routed or further escalated to a committee to review the case and to make the "suspicious" determination. The committee members (the decision makers) should have sufficient authority and judgment to make the determination, and ought to be people who best know the customer. It is conventional for the AML Officer or MLRO to present the case and make a recommendation to the committee. Because external reports of suspicious activity are time sensitive, it is a good practice to present a draft report, already reviewed for completeness, quality and risk, to the committee for case review. Auditors should obtain a thorough understanding of the entire suspicious reporting process and the controls in place governing that process.

Compliance Monitoring and Assessment. Regulators frequently require or favor AML programs that have a strong compliance monitoring function as well as a transactions monitoring function. This should not be confused with independently testing the effectiveness of the AML program, which is what this section is about.

Auditors should review the compliance review, assessment or monitoring program (different terms are used among jurisdictions and businesses) to make sure that this requirement is being

adequately addressed. Compliance assessment is the primary mechanism through which the compliance function can assess the quality and effectiveness of the AML and SAR/STR program in place. Auditors should determine whether this component is in place and operating effectively, whether periodic assessment is being performed by sufficient and qualified professional staff and the results are being reported and acted upon.

Information and communication. Also consistent with the profession's IFC methodology, auditors should examine and assess the quality of strategic, compliance and operational information surrounding and driving the AML and SAR/STR processes and the adequacy of the channels of communication.

Enabling and strengthening the program elements and practices described above require quality information, information processing and well-defined and working channels of communication. Management information about program performance, risk assessment and response has to be accurate, meaningful and timely to enable senior management to make well-informed decisions. Assessing the quality of information and information processing connected with the AML and SAR/STR processes itself may require some in-depth analysis. This will likely include assessing the timeliness, accuracy, efficiency, effectiveness, quality and usefulness of the mechanisms, reports and reporting tools used by designated employees to support the monitoring, escalation, investigation, analysis and reporting of unusual and suspicious activity. Here, it may be prudent to assign an IT auditor to look at the automated processes.

Similarly, auditors must identify the channels of communication surrounding the AML program and SAR/STR processes and evaluate their effectiveness. Conventional channels include: internal conveyances of written compliance programs (usually email, web-site postings and employee manuals), compliance and business unit meetings, and training and awareness sessions.

Responsibility for Detecting and Reporting Suspicious Activity

Unless specifically engaged to do so, it is not the auditors' responsibility to detect and report suspicious activity in connection with a compliance or operational audit of an AML program or testing a SAR/STR process. When performing these types of engagements, however, auditors frequently identify unusual and suspicious activity. When this occurs, auditors should report their suspicions to management immediately.

Anti–Money Laundering

Acronyms used throughout this Paper

AML	*Anti-Money Laundering*
ATM	*Automatic Teller Machine*
CDD	*Customer Due Diligence*
CFATF	*Caribbean Financial Action Task Force*
EDD	*Enhanced Due Diligence*
FATF	*Financial Action Task Force*
IFC	*Integrated Framework of Control*
IGO	*Inter-Governmental Organization*
KYC	*Know Your Customer*
MLRO	*Money Laundering Reporting Officer*
OECD	*Organization of Economic Cooperation and Development*
PEP	*Politically Exposed Person*
SAR	*Suspicious Activity Reporting*
SME	*Subject Matter Expert*
STR	*Suspicious Transaction Reporting*

Appendix I

Compendium of AML Guidance

Auditing Practices Board, UK - http://www.frc.org.uk/apb

- *Practice Note 12, Money Laundering (May 1997)*

Asia/Pacific Group on Money Laundering - http://www.apgml.org

- *Annual Report 1 July 2001 – 30 June 2002 (December 2002)*

AUSTRAC - http://www.austrac.gov.au

- *Annual Report 2002-03 (October 2003)*
- *An overview of Australia's Anti-Money Laundering Strategy (May 2000)*
- *Guidelines on Suspect Transaction Reporting and Areas of Suspect Activity*

Basel Committee on Banking Supervision - http://www.bis.org/bcbs

- *The Joint Forum – Initiatives by the Basel Committee on Banking Supervision, International Association of Insurance Supervisors and International Organization of Securities Commissions to Combat Money Laundering and the Financing of Terrorism (June 2003)*
- *The Joint Forum – Basel Committee on Banking Supervision, International Association of Insurance Supervisors and International Organization of Securities Commissions: Core Principles – Cross-Sectoral Comparison (November 2001)*
- *Survey of Electronic Money Developments (November 2001)*
- *Customer Due Diligence for Banks (October 2001)*
- *Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (December 1988)*

Caribbean Financial Action Task Force - http://www.cfatf.org

- *Annual Report 2000-2001 (October 2001)*

Council of Europe - http://www.coe.int

- *1990 Convention on Laundering, Search, Seizure and Confiscation of The Proceeds from Crime (1998)*
- *Explanatory report on the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1998)*

CTIF-CIF (Belgian Financial Intelligence Processing Unit) - http://www.ctif-cfi.be

- *Money Laundering Indicators (February 2003)*
- *9th Annual Report 2001-02 (October 2002)*

The European Communities Council - http://www.europa.eu.int

- *Directive 2001/97/EC of 4 December 2001 Amending Council Directive 91/308/EEC on Prevention of the Use of the Financial System for the Purpose of Money Laundering (December 2001)*

Egmont Group - http://www.egmontgroup.org

- *Information Paper on Financial Intelligence Units and the Egmont Group (September 2003)*
- *Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases (June 2001)*
- *Best Practices for the Improvement of Exchange Information Between Financial Intelligence Units*
- *FIUs in Action: 100 Cases from the Egmont Group (2000)*

FEE (The European Federation of Accountants) - http://www.fee.be

- *Charter of the European Professional Associations in Support of the Fight Against Organised Crime (July 1999)*

Financial Action Task Force - http://www.fatf-gafi.org

- *The 40 Recommendations (June 2003)*
- *Annual Report and Annexes 2002-03 (June 2003)*
- *Annual Review of Non-Cooperative Countries or Territories (June 2003)*
- *Report on Money Laundering Typologies 2002-03 (June 2003)*
- *Combating the Abuse of Alternative Remittance Systems: International Best Practices (June 2003)*
- *Combating the Abuse of Non-Profit Organisations: International Best Practices (October 2002)*
- *Evaluation of Laws and Systems in FATF Members Dealing with Asset Confiscation and Provisional Measures (1998)*

FinCen (Financial Crimes Enforcement Network, US Department of the Treasury) -

http://www.fincen.gov

- *2003 National Money Laundering Strategy*
- *Suspicious Activity Reporting Guidance for Casinos (December 2003)*
- *The SAR Activity Review, Issue 6 – Trends, Tips and Issues (November 2003)*
- *A Survey of Electronic Cash, Electronic Banking, and Internet Gaming (2000)*
- *FinCen Follows the Money – A Local Approach for Identifying and Tracing Criminal Proceeds (July 1999)*
- *FinCen Advisories*

Fintrac (Financial Transactions and Reports Analysis Centre of Canada) -

http://www.fintrac.gc.ca

- *Annual Report 2003 (September 2003)*
- *Presentation of the Proceeds of Crime (Money Laundering) and Terrorist Financing: The Act, Regulations and Related Issues (June 2003)*
- *Fintrac Guidelines*

Financial Services Authority, UK - http://www.fsa.gov.uk

- *Reducing Money Laundering Risk – Know Your Customer and Anti-Money Laundering Monitoring (August 2003)*
- *Briefing Note: Identification of Existing Customers by Regulated Firms (July 2003)*
- *Money Laundering - Independent Financial Advisors Handling Client Money from Abroad (February 2003)*
- *Money Laundering – Results of the On-Line Broking, Spread Betting and Domestic Retail Banking Clusters Projects (August, October 2002)*
- *The Money Laundering Theme – Tackling Our New Responsibilities (July 2001)*

IAIS (International Association of Insurance Supervisors) - http://www.iaisweb.org

- *Guidance Paper No. 5, Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities (January 2002)*

ICAEW - http://www.icaew.co.uk

- *Tech 15/03 – Anti-Money Laundering (Proceeds of Crime and Terrorism) – Interim Guidance for Accountants (May 2003)*

IMF - http://www.imf.org

- *AML and Combating the Financing of Terrorism – Status Report of the Work of the IMF and the World Bank on the Twelve-Month Pilot Program of AML/CFT Assessments and Delivery of AML/CFT Technical Assistance (September 2003)*
- *Factsheet: The IMF and the Fight Against Money Laundering and the Financing of Terrorism (April 2003)*
- *Report on the Outcome of the FATF Plenary Meeting and Proposal for the Endorsement of the Methodology for Assessing Compliance with Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Standard (November 2002)*
- *"Combating Money Laundering and the Financing of Terrorism" (Eduardo Aninat, Daniel Hardy & R. Barry Johnston, Finance & Development Magazine, September 2002)*
- *Money Laundering and Terrorism Financing – An Overview (Jean-Francois Thony, May 2002)*
- *Intensified Fund Involvement in Anti-Money Laundering Work and Combating the Financing of Terrorism (November 2001)*
- *Enhancing Contributions to Combating Money Laundering: Policy Paper (April 2001)*

- *Financial System Abuse, Financial Crime and Money Laundering – Background Paper (February 2001)*

Imolin (International Money Laundering Information Network, United Nations Office on Drugs and Crime) - http://www.imolin.org

- *United Nations Model Bill on Money Laundering, Proceeds of Crime and Terrorist Financing (2003)*
- *Money Laundering and Related Issues in Turkmenistan (November 2002)*
- *Money Laundering and Related Issues in Uzbekistan (May 2002)*
- *Money Laundering and Related Issues in Kazakhstan (April 2002)*
- *Russian Capitalism and Money Laundering (March 2001)*
- *United Nations Model Legislation on Laundering, Confiscation and International Cooperation in Relation to the Proceeds of Crime (1999)*
- *Commonwealth Model Law for the Prohibition of Money Laundering & Supporting Documentation (May 1996)*

Institute of Internal Auditors, UK - http://www.iia.org.uk

- *Professional Issues Bulletin: Money laundering – Some Background and Thoughts for Internal Auditors (March 2003)*

Interpol - http://www.interpol.int

- *The Hawala Alternative Remittance System and its Role in Money Laundering (Interpol General Secretariat, Lyon, January 2000)*
- *Alternative Remittance Systems Distinguishing Sub-Systems of Ethnic Money Laundering in Interpol Member Countries on the Asian Continent (Lisa C. Carroll)*

IOSCO - http://www.iosco.org

- *The Function of Compliance Officer (October 2003)*
- *Objectives and Principles of Securities Regulation (May 2003)*
- *Report on the Implementation of IOSCO Resolutions (September 1998)*
- *A Resolution on Money Laundering (October 1992)*

Joint Money Laundering Steering Group, UK - http://www.jmlsg.org.uk

- *Presentation to FSA Conference on Anti-Money Laundering (by Ian Mullen, Chief Executive, British Bankers' Association, July 2002)*

KPMG Forensic, UK - http://www.kpmg.co.uk

- *Review of the Regime for Handling Suspicious Activity Reports – Report of Recommendations (July 2003)*

Money Laundering Reporting Office, Switzerland - http://www.admin.ch/bap

- *Combating Money Laundering in Switzerland (October 2003)*

- *Second Annual Report 1999-2000*
- *Swiss Legislation Against Money Laundering*

National Criminal Intelligence Service, UK - http://www.ncis.co.uk

- *United Kingdom Threat Assessment of Serious and Organised Crime 2003 – Money Laundering (2003)*
- *The UK's Anti-Money Laundering Legislation and the Data Protection Act 1998 – Guidance Notes for the Financial Sector (April 2002)*

Office of the Comptroller of the Currency of the United States -

http://www.occ.treas.gov/handbook/compliance.htm

- *Bank Secrecy Act — AML Comptrollers Handbook (September 2000)*

Organization of American States - Inter-American Drug Abuse Control Commission

(CICAD-OAS) - http://www.cicad.oas.org

- *Model Regulations Concerning Laundering Offenses Connected To Illicit Drug Trafficking And Other Serious Offenses (November 2003)*
- *Prevention of Money Laundering: The International Legal Framework, Professor William C. Gilmore, University of Edinburgh (2002)*

Public Accountants' and Auditors' Board, South Africa - http://www.paab.co.za

- *Money Laundering Control: A Guide for Registered Accountants and Auditors (June 2003)*

United Nations Office on Drugs & Crime - http://www.unodc.org

- *Global Programme Against Money Laundering*
- *Money Laundering and the Financing of Terrorism: The United Nations Response*
- *Study: Financial Havens, Banking Secrecy and Money Laundering (Jack A. Blum, Prof. Michael Levi, Prof. R. Thomas Naylor and Prof. Phil Williams, 1998)*
- *Control of the Proceeds of Crime – Report of the Secretary-General (1996)*
- *United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)*

***U.S. Department of State* -** http://www.state.gov

- *Money Laundering and Financial Crimes – International Narcotics Control Strategy Report 2003*

U.S. Senate - http://www.senate.gov

- *Minority Staff of the Permanent Subcommittee on Investigations – Report and Case Histories on Correspondent Banking: A Gateway for Money Laundering (February 2001)*

U.S. Department of Treasury - http://www.ustreas.gov

- *Guidance on Enhanced Scrutiny for Transactions that may Involve the Proceeds of Foreign Official Corruption (January 2001)*

Wolfsberg - http://www.wolfsberg-principles.com

- *Global Anti-Money Laundering Guidelines for Private Banking – Wolfsberg AML Principles (May 2002)*

World Bank - http://www1.worldbank.org/finance/html/amlcft

- *Informal Funds Transfer Systems in the APEC Region: Initial Findings and a Framework for Further Analysis*
- *The Hawala System in Afghanistan (June 2003)*
- *Comprehensive Reference Guide on Anti-Money Laundering/Combating the Financing of Terrorism (2002)*
- *Anti-Money Laundering And Combating Financing of Terrorism: Proposals to Access a Global Standard and to Prepare ROSCs – Joint Progress Report on the Work of the IMF and World Bank (July 2002)*
- *Proposed Action Plan for Enhancing the Bank's Ability to Respond to Clients in Combating Money Laundering and the Financing of Terrorism (January 2002)*

Appendix II

Additional Indications of Possible Money Laundering

Supplementing the information provided under "Indications of Possible Money Laundering," the following items are additional indications of unusual or suspicious activity:

1. Common Indicators

1.1 General

- Frequent address changes.
- Client does not want correspondence sent to home address.
- Client repeatedly uses an address but frequently changes the names involved.
- Client uses a post office box or general delivery address, or other type of mail drop address, instead of a street address when this is not the norm for that area.
- Client's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact client shortly after he/she has opened an account.
- Client is accompanied and watched.
- Client shows uncommon curiosity about internal systems, controls, policies and reporting; client has unusual knowledge of the law in relation to suspicious transaction reporting.
- Client has only vague knowledge of the amount of a deposit.
- Client gives unrealistic, confusing or inconsistent explanation for transaction or account activity.
- Defensive stance to questioning or over-justification of the transaction.
- Client is secretive and reluctant to meet in person.
- Unusual nervousness of the person conducting the transaction.
- Client is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Client insists on a transaction being done quickly.
- Client appears to have recently established a series of new relationships with different financial entities.
- Client attempts to develop close rapport with staff.
- Client offers money, gratuities or unusual favors for the provision of services that may appear unusual or suspicious.
- Client attempts to convince employee not to complete any documentation required for the transaction.
- Large contracts or transactions with apparently unrelated third parties, particularly from abroad.
- Large lump-sum payments to or from abroad, particularly with countries known or suspected to facilitate money laundering activities.
- Client is quick to volunteer that funds are "clean" or "not being laundered."

- Client's lack of business knowledge atypical of trade practitioners.
- Forming companies or trusts with no apparent business purpose.
- Unusual transference of negotiable instruments.
- Uncharacteristically premature redemption of investment vehicles, particularly with requests to remit proceeds to apparently unrelated third parties or with little regard to tax or other cancellation charges.
- Large or unusual currency settlements for investments or payment for investments made from an account that is not the client's.
- Clients seeking investment management services where the source of funds is difficult to pinpoint or appears inconsistent with the client's means or expected behavior.
- Purchase of large cash value investments, soon followed by heavy borrowing against them.
- Buying or selling investments for no apparent reason, or in circumstances that appear unusual, e.g., losing money without the principals seeming concerned.
- Forming overseas subsidiaries or branches that do not seem necessary to the business and manipulating transfer prices with them.
- Extensive and unnecessary foreign travel.
- Purchasing at prices significantly below or above market.
- Excessive or unusual sales commissions or agents fees; large payments for unspecified services or loans to consultants, related parties, employees or government employees.

1.2 Cash Transactions

- Client frequently exchanges small bills for large ones.
- Deposit of bank notes with a suspect appearance (very old notes, notes covered in powder, etc).
- Use of unusually large amounts in traveler's checks.
- Frequent domestic and international ATM activity.
- Client asks to hold or transmit large sums of money or other assets when this type of activity is unusual for the client.
- Purchase or sale of gold, diamonds or other precious metals or stones in cash.
- Shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (for example, student, unemployed, self-employed, etc.).

1.3 Transactions Involving Accounts

- Apparent use of personal account for business purposes.
- Opening accounts when the client's address is outside the local service area.
- Opening accounts with names very similar to other established business entities.
- Opening an account that is credited exclusively with cash deposits in foreign currencies.
- Use of nominees who act as holders of, or who hold power of attorney over, bank accounts.

- Account with a large number of small cash deposits and a small number of large cash withdrawals.
- Funds being deposited into several accounts, consolidated into one and transferred outside the country.
- Use of wire transfers and the Internet to move funds to/from high-risk countries and geographic locations.
- Accounts receiving frequent deposits of bearer instruments (e.g., bearer checks, money orders, bearer bonds) followed by wire transactions.
- Deposit at a variety of locations and times for no logical reason.
- Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers.
- Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
- Account that was reactivated from inactive or dormant status suddenly sees significant activity.
- Cash advances from credit card accounts to purchase cashier's checks or to wire funds to foreign destinations.
- Large cash payments on small or zero-balance credit card accounts followed by "credit balance refund checks" sent to account holders.
- Attempting to open accounts for the sole purpose of obtaining online banking capabilities.

1.4 Transactions Related to Offshore Business Activity

- Loans secured by obligations from offshore banks.
- Loans to or from offshore companies.
- Offers of multimillion-dollar deposits from a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank.
- Transactions involving an offshore "shell" bank whose name may be very similar to the name of a major legitimate institution.

2. Industry-Specific Indicators

2.1 Financial Entities

a) Personal Transactions

- Client makes one or more cash deposits to general account of foreign correspondent bank (i.e., flow-through account).
- Client runs large credit card balances.
- Client visits the safety deposit box area immediately before making cash deposits.
- Client wishes to have credit and debit cards sent to international or domestic destinations other than his or her address.
- Client has numerous accounts and deposits cash into each of them, with the total credits being a large amount.

- Client has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.
- Client acquires significant assets and liquidates them quickly with no explanation.
- Client acquires significant assets and encumbers them with security interests that do not make economic sense.

b) Corporate and Business Transactions

- Financial statements of the business differ noticeably from those of similar businesses.
- Representatives of the business avoid contact with the branch as much as possible, even when it would be more convenient for them to have such contact.
- Client makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same bank or elsewhere.
- Client makes a single and substantial cash deposit composed of many large bills.
- Asset acquisition is accompanied by unusual security arrangements.

2.2 Businesses that Provide Loans

- Client suddenly repays a problem loan unexpectedly.
- Client asks to borrow against assets held by another financial institution or a third party, when the origin of the assets is not known.
- Loan transactions are entered into in situations where the client has significant assets and the loan transaction does not make economic sense.
- Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction.

2.3 Life Insurance Companies, Brokers and Agents

- Atypical incidence of pre-payment of insurance premiums.
- Insurance policies with premiums that exceed the client’s apparent means.
- Insurance policies with values that appear to be inconsistent with the client’s insurance needs,
- Client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment.
- Client conducts a transaction that results in a conspicuous increase in investment contributions.
- Client shows more interest in the cancellation or surrender than in the long-term results of investments.
- The duration of the life insurance contract is less than three years.
- The first (or single) premium is paid from a bank account outside the country.
- Client accepts very unfavorable conditions unrelated to his or her health or age.

- Transaction involves use and payment of a performance bond resulting in a cross border payment.
- Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policyholder.

2.4 Securities Dealers

- Attempts to purchase investments with cash.
- Client makes large or unusual settlements of securities in cash.
- The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading.
- Large fund flows through non-resident accounts with brokerage firms.
- Transaction of very large dollar size.
- Unusually complex method of purchasing financial products.
- All principals of client are located outside of local jurisdiction.
- Third-party purchases of shares in other names (i.e., nominee accounts).

2.5 Foreign Exchange Dealers and Money Services Businesses

- Client exchanges currency and requests the largest possible denomination bills in a foreign currency.
- Client knows little about address and contact details for payee, is reluctant to disclose this information or requests a bearer instrument.
- Client wants a check issued in the same currency to replace the one being cashed.
- Client instructs that funds are to be picked up by a third party on behalf of the payee.
- Client requests numerous checks or postal money orders in small amounts and various names, which total the amount of the exchange.

2.6 Accountants

- Use of many different firms of auditors and advisers for connected companies and businesses.
- Client has a history of changing bookkeepers or accountants yearly.
- Client is uncertain about location of company records.
- Company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues without reasonable explanation of the continued loss.
- Company is invoiced by organizations located in a country that does not have adequate money laundering laws and is known as a highly secretive banking and corporate tax haven.

2.7 Real Estate Brokers or Sales Representatives

- Client arrives at a real estate closing with a significant amount of cash.

- Client purchases property in the name of a nominee such as an associate or a relative (other than a spouse).
- Client does not want to put his or her name on any document that would connect him or her with the property or uses different names on Offers to Purchase, closing documents and deposit receipts.
- Client inadequately explains the last minute substitution of the purchasing party's name.
- Client pays substantial down payment in cash and balance is financed by an unusual source or offshore bank.
- Client purchases property without inspecting it.
- Client purchases multiple properties in a short time period, and seems to have few concerns about the location, condition and anticipated repair costs, etc., of each property.
- Client pays rent or the amount of a lease in advance using a large amount of cash.
- Client is known to have paid large remodeling or home improvement invoices with cash, on a property for which property management services are provided.

2.8 Casinos and other Gaming/Betting Organizations

- Acquaintances bet against each other in even-money games and it appears that they are intentionally losing to one of the party.
- Client requests checks that are not for gaming winnings.
- Client purchases large volume of chips with cash, participates in limited gambling activity with the intention of creating a perception of significant gambling, and then cashes the chips for a casino check.
- Client exchanges small denomination bank notes for large denomination bank notes, chip purchase vouchers or checks.