

# The Offshore Institute

Caribbean Regional Conference & Exhibition  
Nassau, Bahamas  
June 5<sup>th</sup> - 7<sup>th</sup> 2000

## Anti-Money Laundering Developments Worldwide & When Due Diligence Fails

Presentation by

**Samuel M. Lohman<sup>1</sup>, partner**  
**Lohman, Schwab & Associés**  
**Attorneys at Law**

11 rue Verdaine  
1211 Geneva 3  
Case Postale 3377, Switzerland  
Phone: 41.22.317.8020  
Fax: 41.22.317.8030  
E-mail: [lohman@lohman.ch](mailto:lohman@lohman.ch).

### *‘KNOW YOUR CUSTOMER, KNOW THE SOURCE OF THE FUNDS’*

#### **I. Introduction:**

##### **1. Phase 2: Sector Specific Compliance**

International conventions, mutual legal assistance treaties, domestic legislation and the like are now firmly in place and being actively used by various governments in the international and domestic combat against white collar crime. Anti-money laundering is no longer at subject at the phase 1 or introductory stage / definitional stage. Therefore, from a

---

<sup>1</sup> Samuel M. Lohman is an international lawyer specializing in servicing the needs of high net worth individuals, private / public corporations, banks, fiduciaries, and other professional providers. His particular areas of emphasis are anti money laundering compliance (government and private sector), international structuring and commercial / contractual relationships. In regards to anti-money laundering, Mr. Lohman audits existing client relationships, reviews proposed relationships, advises on compliance, suspicious transaction reporting, mutual legal assistance, and related matters. In addition, he conceptualizes, implements, and ensures proper on-going administration of strategic international on and offshore commercial, asset protection, and estate planning / structures. He is on the Editorial Board of Advisors of [Money Laundering Alert](#) (leading publication on the subject) and is an appointed expert in the areas of Anti-Money Laundering and Banking Secrecy. Among other things, he is an Executive Committee of the Offshore Institute and maintains memberships in the Oregon, American, and International bar Associations as well as registration with the Geneva bar Association as a foreign lawyer authorized to carry out the practice of law.

compliance point of view, we are now focussing on “Sector Specific Compliance”<sup>2</sup> or Phase 2.<sup>3</sup>

“Sector Specific Compliance” defines specific sub-professions within the international financial service sector and has as its goal to identify potential unique problems associated with the provision of different services within the international financial service industry in order to develop greater sensitivity and provide insight on how to reasonably proceed if confronted with the same.

## **2. Reasonableness Standard**

Over the last ten years, Anti-Money law and regulation has had the single most important influence on the manner in which Professional Providers<sup>4</sup> working in the international financial service sector conduct business

At the end of the day, you will be measured by a standard of reasonableness and what is reasonable is dependant on the case involved. Therefore, one ought to always adapt to the needs of the situation involved and consult with domestic and international experts who are actively involved in matters relating to anti-money laundering compliance.

## **3. The Anti-Money Laundering Compliance Industry**

Laws and regulations are changing daily in the area of anti-money laundering and banking secrecy and when we began following these areas eleven or so years ago in earnest, there was little information on the subjects. However, now an industry has been created in the field of anti-money laundering law and compliance. The industry consists of consultants, educators<sup>5</sup>, law enforcement, compliance officers, seminars, programs, newsletters, significant domestic, regional, and international studies, etc. Thankfully, the Internet allows us to keep up with an otherwise over abundance of information.

## **4. Anti-Money Laundering vs. Secrecy and Privacy**

White-collar crime must be stopped and getting at Professional Providers that assist criminals appears to be an effective means to slow down and eventually eliminate a portion of domestic and international criminal activity. However, any effort to control money laundering and

---

<sup>2</sup> The author originally introduced the term “Sector Specific Compliance” at the Caribbean Anti-Money Laundering Compliance Symposium, chaired by the author and sponsored by the Government of the British Virgin Islands in 1998.

<sup>3</sup> Phase 3 is underway. Since the quest is to do what is reasonable under the circumstances, we wait with anticipation for a more extensive body of regulation and laws that define further what “reasonableness” is in the area of anti-money laundering compliance.

<sup>4</sup> Reference to “Professional Providers” herein shall include lawyers, accountants, banks, portfolio managers, trust / fiduciary service providers, money changers, and all others associated with the financial service sector that may fall within relevant anti-money laundering laws and regulation.

<sup>5</sup> Unfortunately, mainstream business schools have not sufficiently incorporated anti-money laundering and white-collar criminal exposure into MBA or other programs designed to train business owners, management, board members, etc.

financial crime must address the secrecy issues head on.<sup>6</sup> It is important to balance the client's right to privacy against legitimate law enforcement interests of the State (or foreign country) as well as the public's right to know.

Most jurisdictions have traditionally recognized that an individual's affairs are personal and thus should remain confidential and remain undisclosed to third parties. This has led such jurisdictions to establish contractual, statutory, regulatory and other provisions ensuring the respect of this right to secrecy.

Despite certain popular thought, banking secrecy is not synonymous with illegal activities. There are many legitimate reasons<sup>7</sup> for clients wanting to place their assets in a jurisdiction with secure banking secrecy laws<sup>8</sup>. Examples of the same would include: protection of personal privacy<sup>9</sup>, protection of competitive information, insure personal safety (from kidnapping, extortion, and the like), or prevent the confiscation of asset for political reasons.<sup>10</sup>

This presentation is purposefully broad and is not intended to be conclusive on the matters that it addresses. Anti-money laundering compliance must be addressed on a case-by-case basis so as to adjust to the sector, industry, jurisdiction(s), and customers involved.

## **II. Typical Anti-Money Legislative and Regulatory Themes**

The overwhelming trend is in favor of stricter anti-money laundering laws / regulation, enforcement, prosecution, confiscation, international cooperation, and the like. Therefore, the odds are that as time goes on, the Professional Provider that finds him or herself intentionally or inadvertently assisting criminals in money laundering will eventually be caught and any structures that are set up to facilitate money laundering are likely to be found to be illegal. The illusory strength of such structures is secrecy (which is a near to impossible state to reach in today's evolving transparent international financial service sector).

---

<sup>6</sup> *Financial Havens, Banking Secrecy and Money-Laundering*, United Nations, 1998 (hereinafter "UN Report") at page 68.

<sup>7</sup> The UN Report likewise acknowledged several legitimate purposes for banking secrecy (and offshore financial centers), as including corporate and personal privacy.

<sup>8</sup> Offshore jurisdictions provide an integral service to the international business community. Traditionally practitioners based in such jurisdictions facilitate transactions by virtue of the legal structures and competent added value service that they offer. Once they are confident in the identity of the client and source of funds, then they are prepared to do what is necessary to get the job done. Whether in the field of private client wealth succession, estate, asset protection planning or main stream commercial corporate structuring for one of the thousands of multi-national corporations who plan their activities using offshore corporate, banking, and related facilities.

<sup>9</sup> In deed, the threat of criminal and / or financial exposure against the bank personnel involved has been good mechanisms over the years for protecting personal privacy. Although, banking secrecy has been abused by criminals and bankers as well (in the case of Nazi gold, dormant accounts and other terrible abuses of the fiduciary relationship), one could argue that placing confidential information with Governments in the first place, would not necessarily be more secure from a personal privacy point of view.

<sup>10</sup> UN Report at. page 69.

## **Know your customer**

### **Ascertain the source of the funds and the underlying reason for each transaction**

### **All crimes are indictable, not only those related to drug dealing**

In theory, the idea is good; however, it does lead to some problems in practice for it overlooks the fact that laws: (1) crimes are not defined in the same way in each jurisdiction, and (2) certain activities may be considered criminal in certain jurisdictions and not in others, especially as regards tax legislation.

### **Professional Providers included**

Money laundering compliance is no longer limited to the banking sector. All financial intermediaries are becoming affected and therefore responsible under the due diligence and compliance obligations of relevant law and regulation.

### **Compulsory reporting of suspicious activity**

Rather than voluntary (or no) reporting compulsory reporting of suspicious activity to the criminal authorities is now becoming the rule. Suspicious activity can be defined as a situation in which a 'red flag' is raised.<sup>11</sup>

### **Mutual Legal Assistance**

There has been an intensification of international cooperation and use of mutual legal assistance treaties (as well as informal means) to facilitate the sharing of information amongst Governments relevant to criminal investigations and prosecutions.

### **Focus on Other Professional Providers**

There is a growing focus on accountants and lawyers who work in the international financial service sector.

## **8. Monitoring of Trends: Anti-Money Laundering, E-Commerce**

Various types of crimes can be linked or facilitated by the application of computers, including: (1) computer penetration into public phone system and major computer networks, (2) privacy violations, (3) industrial espionage, (4) pirating of licensed software, (5) and any

---

<sup>11</sup> In its Recommendations, the FATF lists such 'red flags'. However, experience is an important tool in the arsenal of spotting the would be money launderer. Today there exist many novice parishioners who have been schooled in areas of regulation and compliance. In the extreme the client risks being viewed as the enemy and professional providers view their roles as police officers.

other crime where a computer is the major factor or tool in committing a criminal offense (cyber porn, etc.).

In the context of banking over the Internet, several issues need to be addressed, including: (1) effectiveness of current due diligence reporting requirements (including know your customer), in the context of cyber banking and cyber payments as “pier to pier” transactions are eliminated, (2) jurisdictional issues regarding law and regulation.

The FATF, in its 1999 Annual Report, acknowledged that all delegations participating continue to report that there have not been, as of yet, any investigated money laundering cases involving new payment (e.g. Cypbercash, E-money, Smart Cards, etc.) technologies.

However, there have been several instances of other types of crimes — generally fraud schemes against unsuspecting members of the public — that have used the Internet as a means for committing the underlying offence. Law enforcement in FATF member countries remains concerned about the potential for use of these new technologies in money laundering schemes. Specifically, some of these risks include:

1. Inability to identify and authenticate parties that use the new technologies;
2. Level of transparency of the transaction;
3. Lack or inadequacy of audit trails, record keeping, or suspicious transaction reporting by the technology provider;
4. Use of higher levels of encryption (thus blocking out law enforcement access); and
5. Transactions that fall outside current legislative or regulatory definition.

**a) Countermeasures**

The FATF within their 1999 report, agreed that the field of new payment technologies is changing very rapidly, and that developments in e-cash systems, along with those of the other proposed systems, should continue to be monitored. The experts discussed a number of possible measures, which included the following:

1. Limiting the functions and capacity of smart cards (including maximum value and turnover limits, as well as number of smart cards per customer);
2. Linking new payment technology to financial institutions and bank accounts;

3. Requiring standard record keeping procedures for these systems to enable the examination;
4. Documentation, and seizure of relevant records by investigating authorities; and
5. Establishing international standards for these measures.

### **III. Anti-Money Laundering vs. Banking Secrecy**

For better or worse, banking secrecy is under attack by various international organizations and / or State and local governments. It is seen, among other things, as a “tool” which facilitates harmful tax competition, tax evasion, drug trafficking, money laundering in general as well as other serious criminal conduct.

#### **1. Financial Action Task Force<sup>12</sup>**

In 1990 the Financial Action Task Force issued its monumental 40 Recommendations contained several provisions, which eventually impact banking secrecy practice:

*“Customer Identification and Record-keeping Rules*

*10. Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names...*

*In order to fulfill identification requirements concerning legal entities, financial institutions should, when necessary, take measures:*

*(i) To verify the legal existence and structure of the customer ...*

*15. If financial institutions suspect that funds stem from a criminal activity, they should be required to report promptly their suspicions to the competent authorities.*

*16. Financial institutions, their directors, officers and employees should be protected by legal provisions from criminal or civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the competent authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.*

---

<sup>12</sup> The FATF 40 Recommendations have had the single most impact on the development of international and domestic anti-money laundering law, regulation, and policy.

## 2. Organization Economic Cooperation and Development (“OECD”)

In addition, the OECD in its important 1998 Report in regards to combating harmful tax competition recommended to its members in part:<sup>13</sup>

*“Recommendation concerning access to banking information for tax purposes: in the context of counteracting harmful tax competition, countries should review their laws, regulation and practices which govern access to banking information with a view towards removing impediments to the access to such information.”<sup>14</sup>*

## 3. United Nations

### a) Article 4 of the 1988 United Nations Convention<sup>15</sup>

*“Special investigative powers and techniques*

*1. Each Party shall adopt such legislative and other measures as may be necessary to empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized in order to carry out the actions referred to in Articles 2 and 3. A Party shall not decline to act under the provisions of this article on grounds of bank secrecy.”*

### b) 1998 UN Report

Similarly, in the context of its review of financial centers and banking secrecy in general, the UN in its significant report published in 1998 noted:

*“...Those who seek secrecy by definition have something to hide. In the majority of cases it is safe to say that what they have to hide is the origin, provenance and destination of their wealth, not they’re political views or ethnic origins.... Bank secrecy, then, is a serious concern.”*

## VI. Swiss Notions of Secrecy and Privacy:

---

<sup>13</sup> *Harmful Tax Competition: An Emerging Global Issue*, 1998 (hereinafter “OECD Report”) at Appendix I, page 2.

<sup>14</sup> See also OECD Report at Appendix II where Switzerland lodges its rejection of the Report: “...Switzerland considers that it is legitimate and necessary to protect the confidentiality of personal data. In this respect. The Report... conflict with the Swiss legal system.”

<sup>15</sup> *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, December 1988

Switzerland has been a role model in this regard to banking secrecy. Swiss law does not protect only the now famous (or infamous) banking secrecy, but also other aspects of privacy, such as business privacy.

It is a fact that banking secrecy has been under increasing pressure over the last few years as a result many different factors. First, the recognition that banks are often used as instruments for money laundering. Also, the recent Nazi gold scandal has also given rise to widespread criticism of the Swiss secrecy laws. However, anybody with any experience of the country will tell you that secrecy is indeed very deeply rooted in the Swiss way of thinking. To the Swiss, secrecy is a fundamental right that extends to everyone and covers every aspect of professional, financial, and private life.

This concept is clearly reflected in current Swiss domestic legislation as well as in the international treaties to which Switzerland is a party.

Of course, secrecy can never be absolute. To summarize the Swiss approach, it can be said that secrecy is the principle and that any exceptions to it must be strictly regulated.

However, a brief examination of relevant international conventions concerning Switzerland is in order, as follows:

### **1. International Conventions:**

#### **a) The Hague convention on Taking Evidence Abroad in Civil or Commercial Matters:**

The Hague convention on Taking Evidence Abroad in Civil or Commercial Matters of March 18<sup>th</sup>, 1970 has been applicable in Switzerland as of January 1<sup>st</sup>, 1995. The United States is also a party to the treaty.

Swiss authorities apply this treaty to the exclusion of any other provisions in cases arising between parties to the Convention. The Convention defines a standard procedure for gathering evidence abroad, which is by way of letters rogatory, to be executed by the competent authorities of the country to which the request is sent. It is also possible for diplomatic or consular agents to execute the request, provided however; prior authorization from local authorities has been sought and obtained.

Thus, under the terms of the Convention, unless prior consent is obtained from competent authorities in the host country, a direct order from a foreign judicial authority cannot be recognized or implemented in the host country.

#### **b) The European Convention on Mutual Crime Matters of 1959 and Federal Statute on International Judicial Assistance in Criminal Matters:**

The European Convention on Mutual Crime Matters of 1959 and Federal Statute on International Judicial Assistance in Criminal Matters of March 20, 1981 have been effective as of January 1<sup>st</sup>, 1983.

Switzerland will grant assistance on the condition that the offenses under investigation must also be an offense in Switzerland as well. This is referred to as the requirement of “dual criminality”.

Dual criminality may be found in situations such as Insider Trading, Market Manipulation, Tax Fraud (but not simple tax evasion, which is considered in Switzerland as an administrative offense).

## **2. Bilateral and multi-lateral treaties:**

### **a) Treaty with the US Swiss-American Treaty on Legal Assistance in Criminal Matters:**

This treaty was signed in 1973 and became effective as of January 1<sup>st</sup>, 1977.

It contains a list of offenses in which the Swiss will cooperate, provide information and thus, if applicable, lift secrecy. The list includes, amongst others, murder, manslaughter, willful nonsupport or abandonment of a minor, robbery, embezzlement; misapplication or misuse of funds, extortion; blackmail, receiving or transporting money, securities or other property knowing the same to have been embezzled, stolen, or fraudulently obtained, fraud (including obtaining property, services, money, or securities by false pretenses or by defrauding, by means of deceit, falsehood, or any fraudulent means), fraud against the requesting state, its states or cantons or municipalities, fraud or breach of trust committed by any person; use of the mails or other means of communication with intent to defraud or deceive, as punishable under the laws of the requesting state as well as fraudulent bankruptcy.

## **3. Swiss domestic law:**

Developments affecting “financial intermediaries”, self-regulating bodies, etc. to be discussed.

## **IV. Practical Due Diligence and Managing Fiduciary Exposure**

The best (and today perhaps the only) form of asset protection planning for the concerned Professional Provider is to develop and scrupulously maintain a state of the art, in-house, global / local, anti-money laundering compliance / reporting system (hereinafter « Compliance Program »).

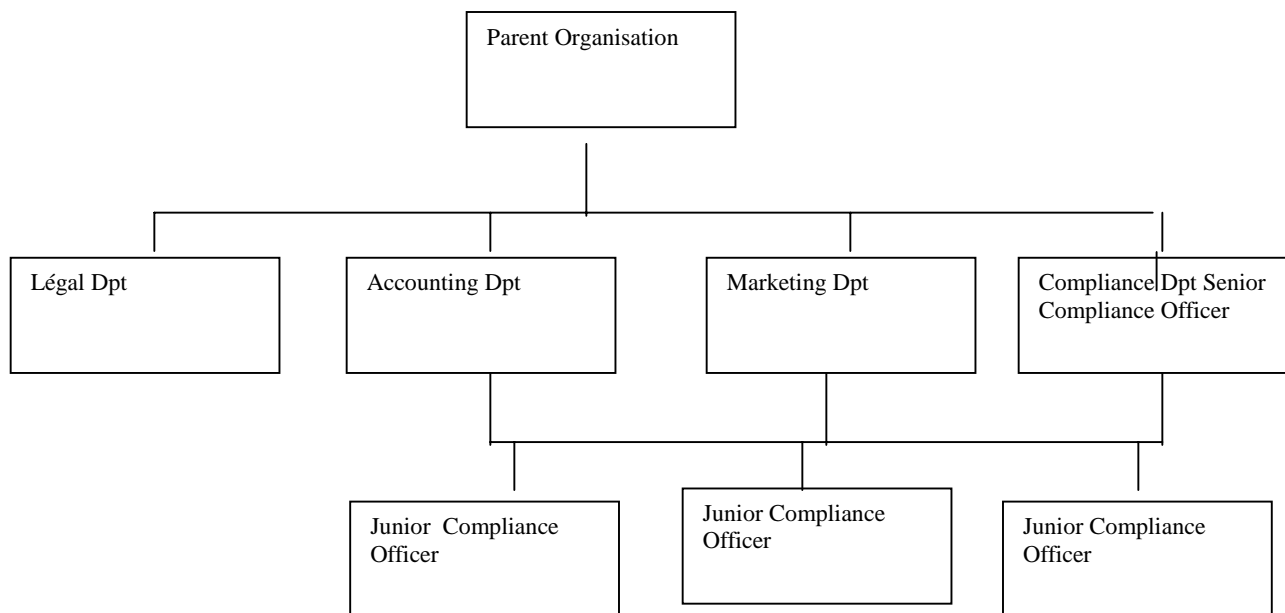
The benefits of an efficient, cutting edge Compliance Program far exceed the costs of non-compliance. Non-compliance, among other things, may lead to bad press, « client flight », civil / criminal exposure, and ultimately, the loss of ability to carry on commercial activity.

While a successfully conceived and maintained Compliance Program may lead to greater understanding, better competence within the organization, additional revenues from additional sales of goods and services, improved relations with regulators, and improved internal organizational communications as well.

The “bottom line” is that organizations that are able to develop, implement, and maintain a sound Compliance Program in conformance with relevant anti-money laundering laws and regulations will maintain a competitive edge in their respective market. Also, compliance is not an option – it’s the law.

### 1. Education and Training Keys to Compliance

The responsibility to develop, implement, monitor, and maintain a Compliance Program should rest at the top management level of the parent organization in the case of a group of related Professional Providers. Furthermore, it is important that the responsibility for the Compliance Program be placed at the same level as other major functional divisions within the corporate structure (e.g. strategic planning, finance, marketing, mergers and acquisitions, etc. as the case may be). Ideally there may be a Senior Compliance Officer at the parent organization with Local Compliance Officers at each group location.



The parent organization compliance unit should take the lead in developing an overall Compliance Program.

## **2. Establishing an Compliance Program**

A brief outline of the more significant steps towards establishing an anti-money laundering Compliance Program, would include:

- a) Designate Senior Compliance Officer
- b) Adapt the Compliance / Due Diligence Program
- c) Assemble and Disseminate Research
- d) Internal Policy Manual
- e) Educate Personnel, Existing, and Prospective Clients
- f) Group Adoption and Acceptance of Compliance Program
- g) Follow up, Monitor Files and Stay Current
- h) Enforce Standards
- i) Remember Fiduciary Responsibility to Client
- j) Damage Control

## **3. The Compliance Officer and the Compliance Manual**

The Compliance Officer must be chosen at a senior level of the management (ideally board level). He is to be responsible for the day-to-day monitoring of the Compliance Program and therefore must have all the necessary authority to do so. Such authority would include: (1) the authority to propose and carry out any changes to the Compliance program, (2) oversee the employees' training program and, (3) ensure that any necessary sanctions are taken so as to be certain that the program is strictly adhered to by all concerned.

A Compliance Program must be sensitive to many factors, including: relevant legal and regulatory requirements, the jurisdiction(s) involved, as well as the customer that is being serviced, or sold a product. General attributes of a successful Compliance Program suited for all jurisdictions include and indeed call for:

- a) Clarity
- b) Conciseness
- c) Sensitivity and compliance with local policies, marketplace, laws and customers

- d) Understanding and endorsement by senior management (expressly, by a signed undertaking)
- e) Communication, understanding, and acceptance at all affected levels within the organization (expressly, by a signed undertaking)
- f) Communication, understanding, and acceptance by customers of the organization (expressly, by a signed undertaking)
- g) Adaptation to the specific business involved
- h) Encouragement towards discerning and accepting “good business”, whilst at the same time making allowance for traditional notions of confidentiality and the like
- i) Acting in conjunction with other Professional Providers and governmental authorities in each market that operates
- j) Flexibility and dynamism in order to meet the needs of this changing area of domestic and international law
- k) Implementation of procedures beyond simple declarations of intent

#### **4. Establishing proper information flows**

#### **5. Maintaining critical information**

#### **6. Staff Training**

The Group Compliance unit should take the lead in developing a staff-training program.

An organization’s staff will generally be ‘at the sharp end’ dealing with prospective and existing customers. Anti-money laundering legislation places not only the organization, but also its employees individually responsible for the enforcement of anti-money laundering legislation.

Anti-money laundering legislation is not uniform amongst the jurisdictions, which have criminalized money laundering. Some jurisdictions require an organization to report money-laundering activities to the authorities whilst others require that the business be turned away or the account be closed. Therefore, training programs should be designed for each jurisdiction in which any given organization operates.

A proper training program informs the staff of the intent of the Compliance Program, its importance to the organization, staff, clients, and the public in general.

The staff should understand the benefits of compliance, including: (1) insulation from individual, criminal or negligent liability, (2) assistance in servicing clients, (3) ensure that the organization is not known as a 'weak' target for criminals, and (4) ensure that the organization's reputation and license to operate remain intact.

Training programs require: (1) careful selection of the trainers, (2) use and frequent updating of training material (written, audio, video, and other types of support material), (3) sensitivity to local and international laws and regulations, (4) integrate practical real and hypothetical cases, (5) training sessions should be formal and informal and (6) internal newsletters should be considered.

Documentation verifying the implementation of the training program should be maintained as well. Such documentation will include staff attendance records, internal communications keeping staff up to date on developments between training sessions, identification of new topics and problems as a result of new products, information concerning new laws and new technology.

The Compliance program will provide for how to handle incomplete account documentation when opening or administering an account. For instance, staff shall need to be instructed either to defer the opening of accounts and/or business relationships until all critical documentation can be obtained or to open the account and/or business relationship on a provisional basis with an agreed limitation of activity.

In addition, personnel shall be trained in the principles of:

- a). Customer acceptance and identification;
- b) Customer confidentiality;
- c) Distinguishing between principals and intermediaries;
- d) Requesting information on all principals and all persons having powers over accounts;
- e) Verification of information and references by economical and efficient use of branch offices, subsidiaries, and in appropriate cases, the use of independent investigators;
- f) Branch offices, subsidiaries and, in appropriate cases, the use of independent investigators;
- g) Ongoing monitoring of accounts;
- h) Suspicious transactions;

- i) Corporate compliance structuring / information flows;
- j) What to do in case of an investigation.

#### **4. Overview of use of reporting mechanisms:**

Suggested reporting mechanisms are answering machines, e-mail, fax machines, and hotline services.

##### **a) Overcome Cultural Taboo: Don't tattle.**

##### **b) Confidential, Anonymous Reporting Systems**

1. Answering machines:
2. Voice Mail, Fax Machines, and e-mail
3. Hotlines
4. In-house System
5. In-house Counsel as Monitors of a Company's Hotline
6. External Hotlines

#### **5. Communicating Compliance Requirements**

1. **Level 1:** board members, CEO, and executive managers: Cover fundamentals of a broad statute or regulatory directive, examine how to assess management compliance, and how to establish and monitor policy.
2. **Level 2:** middle managers, supervisors, line managers, group leaders, and staff specialist: cover legal matters in their particular areas, guidance on how to recognize and report violations, how to establish and monitor internal control.
3. **Level 3:** personnel: more specifics on prohibited behavior with specific examples, positive reinforcement for accepted behavior, how to report violations to supervisor or use of « reporting hotline ».

#### **6. Compliance Monitoring: how high are the costs of non-compliance?**

Governments have distributed examples of suspicious activities. Professional Providers should utilize the list in prevention planning and training. Examples of suspicious activities, include: (1) suspicious country of origin, (2) tax haven banking relationships, (3) the use of nominees, (4) the use of frequent cash transactions, (5) substantial international wire transfers, (6) travel patterns that do not match the business, (7) back to back loans, (8) multiple banking relationship in several countries with no logical rationale to support, (9) etc.

Suspicious activities generally create a duty to investigate further. It is more than likely that the situation involved can be explained. However, it is important to conduct the appropriate due diligence under the circumstances.

## **7. Mechanisms and considerations**

- a) Chinese walls, firewalls
- b) Ethical considerations and conflict avoidance

## **8. Questions To Ask:**

- a) Is the compliance program tailored to the company's unique corporate culture?

Each company has a way of doing things. The compliance program must be shaped by that culture and by the company's distinctive legal concerns, history, and the measures that will work in its particular environment.

- b) Is the compliance program written in plain language?
- c) Would a randomly selected employee be aware of the compliance program?
- d) Would a randomly selected employee know who to ask if confronted with a close call?
- e) Would a randomly selected director be aware of the compliance program?
- f) Is the company monitoring the compliance programs operation?
- g) Is the program being enforced?
- h) Has the compliance program been revised in the last two years?
- i) Is the company ready for crisis situation?
- j) Is the company realistic in its compliance program (i.e. tailored as needed)?

## **9. Transitional Compliance Planning and Ongoing Internal Practice**

Discovery hurts compliance efforts. Corporate counsel and others who conduct compliance efforts are seriously limited in their work by the excesses of discovery. The courts do not see the day-to-day injury to compliance programs that result from the court failure to understand the dynamics of corporate control. Unfortunately, the compliance environment is chilled by the threat of litigation.

Consider making your program litigation sensitive. Unfortunately, the litigation conflict will chill the use of all compliance, interactive tools, because of the risk that the paper trail will be used against the organization under fire.

*A lawyer must advise its client on how to minimize litigation risks. To maximize protection, lawyers must be in charge. They must edit, if not rewrite, every key document as if it were a trial exhibit. This will slow the program, however without protection, there is no choice.*

## **10. Protecting the Compliance Process**

Several points to consider in order protecting the compliance process:

- a). Compliance audits conducted by lawyers only upon formal written request of a senior manager, in order to assert attorney-client privilege.
- c) Review of the audit is conducted in the context of explaining the background at senior management level.
- d) Lawyers participate in the audit process. Sensitive matters are referred to lawyers and a minimum of memos is prepared. Auditors that do the work are employed by outside counsel and they take minimum notes, destroy unnecessary work papers, and orally report to counsel charged to conduct the audit.
- e) During interviews, interviewees are instructed to take no notes.
- f) Interview notes are not signed or reviewed by interviewees so as to keep privilege claim strong.
- g) Audit reports are issued once all issues are dealt with. There are no opinions or details about questionable conduct.
- h) Compliance reports have no underlining, no red ink, and no exclamation marks.
- i) Overall audit report will be given to one or two senior managers. To protect privilege it is in the form of legal advice and not management

recommendations. The discussion is strictly confidential, no junior members present, and no note taking by the client.

- j) Compliance quiz during training process are all collected and destroyed at the conclusion of the exercise.
- k) Lists of dos and don't could be used against the organization.
- l) You must consider litigation risk associated with each aspect of an effective compliance program including hotlines, audits, investigations, and interactive training.
- m)** Audits conducted only for the purpose of providing legal advice and must be under a lawyer's direct control.