MARKS PANETH

ACCOUNTANTS & ADVISORS

CONSEQUENCES OF HAVING A POOR ANTI-MONEY LAUNDERING PROGRAM

Sareena Sawhney, MBA, CFE, CFFA

April 2014

CONSEQUENCES OF HAVING A POOR ANTI-MONEY LAUNDERING PROGRAM

A surge in recent investigations suggests that financial and non-financial institutions are increasingly in violation of Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) policies and procedures as well as regulatory requirements. The Interim Report of the President's Report on Organized Crime defines money laundering as "The process by which one conceals the existence, illegal source, or illegal application of income and then disguises that income to make it appear legitimate." The IRS definition includes the act of hiding legitimately acquired money to avoid taxation; IRS statistics illustrate that the number of money laundering investigations and Bank Secrecy Act investigations has increased from 1,597 to 1,663 and 738 to 923 from 2010 to 2012, respectively.[1]

Some individuals and/or businesses may try to hide their assets offshore, often in tax havens and secrecy jurisdictions. The US Department of the Treasury has issued a model intergovernmental agreement to implement the information reporting and withholding tax provisions of the Foreign Account Tax Compliance Act (FATCA), which is intended to fight offshore tax evasion. Essentially, this agreement would require foreign financial institutions to report to the IRS information about certain financial accounts of US citizens. In addition to asset hiding, some foreign countries have a legal, banking or economic climate that makes them havens for money laundering. As an example, it was once thought that having a Swiss Bank account could unlock many financial secrets, but this no longer holds true. As a result of FATCA, the US government and Switzerland have reached an agreement that could expose Americans who have used Swiss banks to avoid paying taxes. This would allow the US government to get substantial information about their American clients, the value of their accounts and any assistance they received from tax professionals.

Many different kinds of businesses are at risk for money laundering and for penalties if AML programs do not meet regulatory standards. Financial institutions – banks, credit card companies, investment brokers, etc. – are under scrutiny to comply with AML requirements as are casinos and dealers in hard goods such as automobile, boat and airplane dealers and jewelers. Certain industries such as insurance and real estate, are also being scrutinized for potential money laundering because of specific procedures, such as claims against inflated insurance policies and the rapid sale of undervalued properties, that have been used by money launderers.

Money laundering can occur using various methods such as the following:

- Depositing small amounts of money so as to avoid anti-money laundering reporting requirement thresholds;
- Using cash-intensive businesses, such as casinos, where cash from a money launderer is intermingled with legitimate cash, thus making it difficult to measure the revenue base per customer since such cash transactions can be highly variable;
- Establishing a fictitious identity;
- Establishing a "shell company" which can disguise the true owner of money;
- Smuggling cash to a country with less stringent money laundering enforcement;
- Inflating invoices in order to disguise the movement of money;
- Purchasing insurance policies whereby the asset hider can over fund the policy and later receive disbursement checks upon withdrawal;
- Purchasing real estate only to sell it for a value less than what it is wort

[1] See www.irs.gov/uac/Statistical-Data-Money-Laundering-&-Bank-Secrecy-Act-(BSA)

MARKS PANETH
ACCOUNTANTS & ADVISORS

All the more reason to ensure that adequate anti-money laundering programs are in place as the US government is increasingly investigating Bank Secrecy Act/anti-money laundering regulatory cases. Where anti-money laundering programs are in place, what are the steps that compliance officers may be missing? Are businesses at risk because they are unaware of the threat posed by an anti-money laundering program that may have inadequate controls? Are businesses deficient in paying significant attention to the latest compliance rulings? Are there business owners who are unaware that they should have an AML compliance program in place?

RECENT EXAMPLES OF GOVERNMENT ANTI-MONEY LAUNDERING INVESTIGATIONS

Recently, The Las Vegas Sands Corp. agreed to pay $47 million to the government for failing to report suspicious customer transactions. Casino companies are being put on notice by the Justice Department that they need to improve their anti-money laundering procedures as they are not complying with federal reporting requirements. In addition, the Securities and Exchange Commission recently penalized investment advisors and their respective firms for compliance failures. In two of these cases – OMNI Investment Advisors Inc. and Asset Advisors LLC – SEC examiners previously warned the firms about their compliance deficiencies. Under the Investment Advisors Act, which is known as the "Compliance Rule," registered investment advisors are required to adopt and implement written policies and procedures that are reasonably designed to prevent, detect, and correct securities law violations. The Compliance Rule also requires annual review of the policies and procedures for their adequacy and the effectiveness of their implementation.[2]

Agencies are not just going after entities but are also penalizing individuals of such entities. In the OMNI Investment Advisors Inc. case, the SEC charged OMNI's owner, who served as the firm's chief compliance officer but essentially performed no compliance responsibilities. OMNI and its owner failed to adopt and implement written compliance policies and procedures after SEC examiners informed OMNI of its deficiencies. Additionally, OMNI failed to preserve certain books and records. The case settled and OMNI agreed to pay a $50,000 penalty. The owner also agreed to be permanently barred from acting within the securities industry in any compliance or supervisory capacity and from associating with any investment company. Similarly, Asset Advisors LLC, failed to adopt and implement a compliance program. Under the settlement, Asset Advisors LLC agreed to pay a $20,000 penalty, cease operations, de-register with the Commission, and was forced to move advisory accounts to a firm with an established compliance program.

Business entities and individuals suffer consequences when they don't have adequate BSA/AML programs in place. Often government agency cases are initiated due to an entities- inadequate AML compliance programs. Such compliance programs are necessary for both financial[3] and non-financial institutions.

[2] See www.sec.gov/news/press/2011/2011-248.htm

[3] Financial institutions include banks, investment firms, money service businesses, credit card issuers or operators, mutual funds, broker-dealers, currency exchanges, casinos, insurance companies, dealers involved in precious metals, stones or jewels, travel agencies, loan companies, auto, boat and airplane dealers and individuals involved in real estate closings and settlements.

COMPLIANCE WITH ANTI-MONEY LAUNDERING PROGRAMS

Section 352 of the Patriot Act requires all financial institutions to establish AML programs inclusive of the following:

- Establish internal policies, procedures, and controls to prevent money laundering;
- Designate a money laundering compliance officer;
- Establish an ongoing training program for awareness of money laundering;
- Establish an independent audit function to test the programs.

Section 326 of the Patriot Act expands on the Bank Secrecy Act by requiring financial institutions to implement Customer Identification Programs ("CIPs"). The CIPs are to be incorporated into financial institutions' money laundering programs and should verify and maintain records of any individual seeking to open an account.

The Patriot Act also prohibits foreign shell banks from maintaining correspondent accounts at any US financial institution. "Shell banks" lack a physical presence[4] in any country. It is strongly encouraged that the US institutions verify all the information provided by the foreign institution at least every two years. Additionally, financial institutions are required to establish due diligence policies, procedures and controls that are designed to detect money laundering through private and correspondent bank accounts[5] held by non-US citizens.

Brokers and dealers in securities must file with FinCEN (Financial Crimes Enforcement Network) a report of any suspicious activity that involves funds or assets of at least $5,000, and the broker-dealer knows, suspects or has reason to suspect that the transaction involves illegal activity, evades regulations under the Bank Secrecy Act or has no business or lawful purpose in which a particular customer would expect to engage in.

THE BANK SECRECY ACT – ADDITIONAL DUE DILIGENCE

AML Compliance programs should also include policies, procedures and internal controls designed to achieve compliance with the Bank Secrecy Act. Specifically, the purpose of the Bank Secrecy Act is to maintain a system of reporting and recordkeeping designed to track large or unusual financial transactions.

Record-keeping requirements are set forth for banks, nonbank financial institutions, securities brokers, casinos and currency dealers and exchangers. All institutions are required to keep a record of any financial transaction of more than $10,000.[6] Additionally, information on the identity of purchasers of monetary instruments in amounts greater than $3,000 must be kept for five years.

---

[4] "Physical presence" requires more than a post office box, e-mail address or physical location housing a server. The bank must be an actual place of business at a fixed address where a bank regulatory authority has licensed the operation of the bank.

[5] A private account is an account that requires a minimum of $1 million in deposit of funds or other assets. A correspondent account is defined as an account established to receive deposits from or make payments on behalf of a foreign financial institution.

[6] This includes records of any extension of credit of more than $10,000 as well as each transfer of $10,000 or more outside of the United States.

MARKS PANETH
ACCOUNTANTS & ADVISORS

All banks, and certain other financial institutions, are required to fill out currency transaction reports whenever there is a currency transaction of $10,000 or more.[7] Multiple transactions must be treated as a single transaction if the financial institution has knowledge that the transactions are by or on behalf of the same person and the amounts total more than $10,000 during any one business day. The Patriot Act requires individuals involved in any trade or nonfinancial business where they may receive more than $10,000 in coin or currency to file a report with FinCEN.

The Bank Secrecy Act also requires financial institutions to monitor suspicious activity and to disclose such activity by filing Suspicious Activity Reports with FinCEN if any of the following criteria applies:

- Any known or suspected violation involving the financial institution when the institution has a basis for identifying one of its employees, directors, officers or affiliated parties as having committed the act or aided in its commission;
- Any known or suspected violation involving the financial institution and aggregating $5,000 or more when the institution can identify a possible suspect or group of suspects;
- Any known or suspected violation involving the financial institution and aggregating $25,000 or more regardless of whether there is a substantial basis for identifying possible suspects;
- Any transaction conducted or attempted to be conducted through the financial institution when there is reason to suspect (1) the funds were from illegal activities, (2) the transaction evades any regulations of the Bank Secrecy Act and (3) the transaction has no business purpose.

The Bank Secrecy Act makes it illegal for financial institutions to notify any individual involved in the transaction that a Suspicious Activity Report was filed.

Casinos with gross revenues over $1,000,000 must file Suspicious Activity Reports if a transaction involves or aggregates at least $5,000 in funds and if it meets one of the four categories described above. Examples of suspicious activity include using wire transfers to deposit funds into casino accounts and using the money for little or no gaming activity before cashing out. Also some casino employees whose salaries are tied to how much the customer spends may not have an incentive to report suspicious activity.

Individuals who deal in jewels, precious metals and precious stones are required to establish anti-money laundering programs. Dealers are defined as individuals who have purchased at least $50,000 and who have sold more than $50,000 worth of jewels, stones or metals during the preceding year. Dealers, however, are not required to file Suspicious Activity Reports.

MONITORING AML PROGRAMS

1. **Ongoing AML program monitoring:** Once an AML program has been implemented it is important that an ongoing monitoring process be put in place as well. Monitoring account activity and transactions flowing through an institution is one means of ensuring that appropriate processes are in place that allow for the identification of unusual activity and unusual patterns of activity or transactions. Institutions must have the ability to analyze and determine if the activity, patterns or transactions are suspicious in nature with regard to potential money laundering. Financial institutions, in particular, should have the ability to review payment instructions and compare them against lists provided by governmental authorities in order to identify potential terrorists or terrorist financing.

[7] Any deposit, withdrawal, exchange or cashing of checks of $10,000 or more.

2. **Due diligence when accounts are opened:** Similarly, due diligence needs to be performed at the account opening process as well. Testing should occur to determine whether institutions are verifying the identities of new account holders, comparing their names against lists provided by government agencies and maintaining adequate records of the information used to verify an individual's identity. This initial step is crucial as it involves the profiling of potential client activity to aid in future monitoring.

3. **Monitor customers and activity with highest risk:** An ongoing monitoring process should be developed in order to assess activity for all customers placing emphasis on the customers and activity with the highest risk. The ongoing monitoring process should be used to identify suspicious activity that may ultimately result in the filing of a Suspicious Activity Report.

4. **Consider an independent assessment**: Institutions that already have an AML transaction monitoring system should consider having an independent consultant test their transaction monitoring systems in order to determine the adequacy of the monitoring system, evaluate whether changes need to be made to the system and policies, as well as test the adequacy of the institutions' efforts to have ongoing effectiveness and integrity. For this reason, it is extremely important that institutions have a program in place to continually review the performance of their transaction monitoring system and make enhancements to address any deficiencies.

   As an example, an institution may learn that their AML transaction monitoring system is not capturing important patterns of suspicious behavior and thus activity is not being flagged and will not be reported to the appropriate government agency. Performing a detailed, expert review of a sample of customer transaction data can help to identify these additional patterns and types of behavior that are not being monitored.

   Additionally, it is also important that once AML activity has been flagged, AML analysts at the institution put in adequate due diligence needed to assess whether a Suspicious Activity Report needs to be filed or a client profile needs to be updated if necessary. Often times, institutions run the risk of inadequately allocating resources to review cases of suspicious activity which can result in the institution being deemed as having an inadequate AML monitoring system and result in hefty fines.

   An independent review of an AML transaction monitoring system may also help determine whether the system is effective in comparing the customer's account/transaction history to the customer's specific profile information and a relevant peer group and/or compare the customer's transaction history against established money laundering scenarios to help identify potentially suspicious transactions.

Having an AML transaction monitoring system in place supplemented with employee training, compliance oversight, internal controls and independent testing should form the components of a complete AML compliance program.

Sareena M. Sawhney, MBA, CFE, CFFA, is a Director in the Litigation and Corporate Financial Advisory Services Group at Marks Paneth LLP. Ms. Sawhney focuses on providing services in the areas of complex fraud investigations and forensic accounting examinations as well as services related to commercial litigation and comprehensive damage analyses. She can be reached at 212.503.6372 or by email at ssawhney@markspaneth.com.

IRS CIRCULAR 230 DISCLOSURE
Treasury Regulations require us to inform you that any Federal tax advice contained in this communication is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.

MARKS PANETH
ACCOUNTANTS & ADVISORS