Don't risk facing AML/BSA violations in the US

By Sareena Sawhney, Marks Paneth LLP, USA

E: ssawhney@markspaneth.com

In August of 2017, the New York Department of Financial Services (NYDFS) assessed an approximate $600 million fine against a global bank and its New York branch for Anti-Money Laundering (AML)/ Bank Secrecy Act (BSA) violations. Specifically, the global bank failed to implement a strong AML/BSA compliance structure. Evidence of this was shown through the global bank's ties with a Saudi Arabian bank allegedly linked to Al Qaeda. The Saudi Arabian bank transactions comprised approximately 24% of the transactions conducted through the New York branch, and thousands of transactions were excluded as high risk even when essential information such as beneficiary identities could not be determined. US AML/BSA rules require financial institutions, like this global bank, to have an effective AML/BSA programme in place to prevent the company from being used to facilitate money laundering and the financing of terrorism.

Who is required to have an Anti-Money Laundering programme?

Many different kinds of businesses are at risk for money laundering and for penalties if AML/BSA programmes do not meet regulatory standards. Financial institutions such as banks, credit card companies, broker/dealers, money service businesses, insurance companies and casinos are under scrutiny to comply with AML/BSA requirements. Certain industries, such as insurance and real estate, are also being scrutinized for potential money laundering.[1] If you are a financial institution looking to do business in the US your institution and/or certain individuals of that institution may suffer consequences if adequate AML/BSA programmes are not in place. Often, government agency cases are initiated solely because of an entity's insufficient AML/

Many different kinds of businesses are at risk for money laundering and for penalties if AML/BSA programmes do not meet regulatory standards

BSA compliance programme, even if there is no suspicion of money laundering or terrorist associations. Such compliance programmes are necessary for both banks and non-bank financial institutions.

The components of an Anti-Money Laundering programme

An institution's AML/BSA programme should be risk-based. The institution should identify risks based on the type of customers it serves, geographic location of such customers, and the types of services it offers. Such risk-based programmes should be the basis for the institution's AML policies, procedures and internal controls. Section 352 of the Patriot Act requires all financial institutions to establish AML programmes that achieve the following:

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

Section 326 of the Patriot Act expands on the BSA by requiring financial institutions to implement Customer Identification Programmes (CIPs). The CIPs are to be incorporated into financial

Footnote

1. Other financial institutions also include dealers in precious metals, stones or jewels.

institutions' AML programmes and should verify and maintain records of any individual and/or business seeking to open an account. Additionally, such procedures should be documented. The procedures should address the types of information the firm will collect from the customer and how it will verify the customer's identity.

When is additional due diligence needed?

AML Compliance programmes should include comprehensive customer due diligence (CDD) policies, procedures and processes for all customers, especially those that present a higher risk for money laundering and terrorist financing. CDD begins with verifying the customer's identity and assessing the risks associated with that particular customer. Processes should also include enhanced CDD for higher-risk customers and ongoing due diligence of the customer base.

High-risk customers present increased exposure to financial institutions; therefore, these customers and their transactions should be closely scrutinized at the initial account opening and throughout the term of their relationship with the bank. Some accounts may be riskier based on the following:

- Customer's actual or anticipated business activity
- Customer's ownership structur
- Anticipated or actual volume and types of transactions
- Transactions involving high-risk transactions.

Consequently, according to the Federal Financial Institutions Examination Council (FFIEC), a financial institution should initially and periodically request the following information:

- Purpose of the account
- Source of funds and wealth
- Identification of individuals with ownership or control over the account such as beneficial owners
- Occupation or type of business
- Financial statement
- Banking references
- Location of where the business is organised
- Proximity of the customer's residence, place of employment or place of business to the bank
- Description of the customer's primary trade area and expected frequency of international transactions
- Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers
- Explanations of account activity.

To sum up, in order to prevent businesses and individuals from suffering penalties for not having an adequate AML and/or BSA compliance programme in place, the following must be incorporated into every financial and non-financial institution's compliance programme:

Monitoring AML Programmes

1. **Ongoing AML programme monitoring:** Once an AML programme has been implemented it is important that an ongoing monitoring process be put in place as well. Account activity should be monitored for unusual size, volume, pattern, or type of transactions taking into consideration risk factors and red flags that are appropriate to a particular business. Red flags that indicate possible money laundering include, but are not limited to, the following:

- Customers that provide identification documents that cannot easily be verified
- Customers that "structure" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or record-keeping instrument
- Funds transfers to and from high-risk geographic locations without a business purpose
- Customer transaction patterns that show a change inconsistent with normal activities
- Multiple accounts in the names of family members or corporate entities with no clear business purpose
- Payment by third-party check or money transfer without any connection to the customer.

2. **Due diligence when accounts are opened:** Testing should occur to assess 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.

3. **Monitor customers and activity with highest risk:** An enhanced due diligence and 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 (SAR).

4. **Consider an independent assessment:** Institutions that already have an AML transaction monitoring system should consider having an independent consultant test their system at least annually in order to, at a minimum, do the following:

(1) Evaluate the overall effectiveness of the firm's AML/BSA compliance programme;
(2) Evaluate a firm's procedures for BSA reporting or record-keeping requirements;
(3) Evaluate the implementation of the firm's CIP programme;
(4) Evaluate the firm's customer due diligence requirements;
(5) Review the firm's high-risk transactions;
(6) Evaluate the accuracy of the firm's training programme;
(7) Evaluate the firm's processes for identifying and reporting suspicious activity.

As an example, an institution may learn that their AML transaction monitoring system is not capturing important patterns of suspicious behaviour and, therefore, that the 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 behaviour that are not being monitored.

Additionally, it is also important that once AML activity has been flagged, AML analysts at the institution conduct adequate due diligence to assess whether a SAR needs to be filed or a client profile needs to be updated. Often, institutions run the risk of inadequately allocating resources to review cases of suspicious activity, which can result in the institution being deemed as having a deficient AML monitoring system and subject to 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 in comparing 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 a strong foundation for a complete AML compliance programme.

If you have any questions or would like to discuss this article further, please contact:

Sareena Sawhney

E: ssawhney@markspaneth.com