Suspicious Transaction/Activity

Corruption and money laundering are areas of great concern for the Trinidad and Tobago Securities and Exchange Commission (TTSEC), particularly given our role as the Supervisory Authority for Money Laundering and Terrorist Financing in the securities sector. It is now an integral part of our work because of the negative impacts that each activity will have on national and regional economies. The International Monetary Fund has also acknowledged that the international community has made the fight against money laundering and the financing of terrorism a priority. Among the goals of this effort are: protecting the integrity and stability of the international financial system, cutting off the resources available to terrorists, and making it more difficult for those engaged in crime to profit from their criminal activities.

According to Section 6 (1) of the Securities Act 2012, one of the Commission's functions is to ensure compliance with the Proceeds of Crime Act, any other written law, in relation to the prevention of Money Laundering and combatting the financing of terrorism or any other written law that is administered or supervised by the Commission.

In our earlier features, we discussed the role of the Compliance Officer ("CO"). As the gatekeeper of the Registrant's AML/CFT (Anti Money Laundering/Counter Financing of Terrorism) compliance, the CO must ensure the systems that are required to identify and report suspicious transactions and suspicious attempted transactions, are appropriate in all relevant areas of the Registrant's business. The TTSEC AML/CFT Guidelines state that, a CO who knows, suspects or has reasonable grounds to suspect that a client's funds represent proceeds of criminal conduct; or that a transaction or activity appears to be suspicious, should report their suspicions as soon as possible but no later than fourteen (14) days from the date the transaction was found to be suspicious. This report should be submitted to the Financial Intelligence Unit of Trinidad and Tobago (FIU) in the form of a SAR/STR in accordance with the FIU Regulations.

What are the blueprints used to determine when an activity or transaction is suspicious?

According to the Financial Action Task Force ("FATF"), a Suspicious Transaction Report ("STR") or a Suspicious Activity Report ("SAR") is filed if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to Terrorist Financing ("TF"). In Trinidad and Tobago, the Anti -Terrorism Act (the ATA) and the Proceeds of Crime Act ("POCA") require that a STR/SAR be made to the FIU by Reporting Entities when they know or have reasonable grounds for suspicion of Money Laundering ("ML") or TF activities. STRs/SARs are received from financial institutions and listed businesses in accordance with the Financial Intelligence Act.

What constitutes a Suspicious Activity and Transaction?

In determining what constitutes a suspicious activity or transaction, a Registrant must pay special attention to all:

(a) Complex, unusual, large transactions whether completed or not, and all unusual patterns of transactions and to insignificant but periodic transactions, which have no apparent economic or lawful purpose; and

(b) Business transactions between individuals, corporate persons and financial institutions in or from other countries which do not comply with, or who comply insufficiently with the recommendations of the FATF.

Transaction Monitoring

A Registrant is required to pay special attention to the above transactions by having policies, procedures and systems in place for transaction monitoring. Transaction monitoring should be conducted using a risk-based approach which is consistent with the client's risk profile and the Registrant's business operations. It is insufficient to monitor only large transactions given that this would not adequately mitigate risks posed by unusual patterns of transactions and insignificant but periodic transactions as required by section 55(2)(a)(ii) of POCA. Transaction monitoring policies and procedures should allow Registrants to detect structuring of transactions, in one account, as well as across more than one related account; such as accounts that have the same beneficial owner or accounts in the name of clients, who are related or close associates. A Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

Registrants must have policies, procedures and systems in place to monitor clients based on:

(a) The client's normal course of dealings with the Registrant to enable the Registrant to detect unusual transactions or patterns of transactions relative to what has been determined to be the expected activity of the client; and

(b) Known ML/TF typologies in the securities industry.

The degree of monitoring should be in line with the customer's risk rating. Monitoring can be conducted either in real time or after the transaction has taken place through an independent review of the transaction and/or series of transactions. However, this should be undertaken within a reasonable time frame depending on the risk rating applied to the client. Transaction monitoring systems may be automated or manual depending on the size, volume and complexity of the Registrant's business operations.

Training to identify Suspicious Activity

Staff at all levels must be trained to identify suspicious activity and be aware of the proper procedure to be followed when suspicious activity is detected. A non-exhaustive list of indicators of Suspicious Activity can be found at Appendix 3 of the TTSEC AML/CFT Guidelines.

A Registrant's staff must report all unusual activities or transactions to the CO immediately upon detection. Registrants should implement a process for recording 'not filed' (closed, not suspicious) internal suspicious transactions/activity reports. Such records should be maintained

and recorded by the CO. In cases where a SAR/STR has been filed with the FIU, Registrants should continue to monitor and report any further suspicious or unusual activity in relation to that client's accounts. A Registrant and/or its employees must not disclose the existence, submission or content of a SAR/STR to any person, either directly or indirectly. To do so would amount to an offence of tipping off.

Where a Registrant is part of a financial group with common clients, consideration should be given to the Registrant's risk exposure and as far as possible information on clients should be shared to ensure that all facts are considered and consistent when decisions are made at a group wide level. Such instances must immediately be brought to the attention of the Group CO.

During the onboarding process, where a client is unwilling or unable to provide the necessary due diligence information when completing a transaction; a Registrant should not commence the business relationship or perform the transaction. In such instances, a report should be submitted to the CO and a SAR/STR sent to the FIU. A Registrant should keep copies of all customer activity SARs and STRs made to the FIU for a minimum of six (6) years. Copies of all documents released to the FIU pursuant to a court order being served upon a Registrant must be kept for a minimum of six (6) years from the date of release or until the original documents are returned, whichever is the later date.

Tipping-off

During the Customer Due Diligence ("CDD") process, if a Registrant suspects that one of its clients has been involved in ML or TF activities, and believe they can be tipped off during the CDD process, the Registrant should file a SAR/STR with the FIU. Moreover, the Registrant should abort the CDD and Employee Due Diligence ("EDD") process and ensure their filing to the FIU remains obscured from the customer.

A person who knows or suspects that an investigation is being or is about to be carried out by law enforcement authorities or supervisory authorities, must not disclose to any person information or any other matter that is likely to prejudice the investigation or proposed investigation. A Registrant must not disclose to its client that it has reported, or intends to report, any transaction, or activity to the FIU.

For more information on the TTSEC's approach to AML/CFT in the local capital market, you can visit the TTSEC's website at www.ttsec.org.tt.

END

For more information, please visit our corporate website, www.ttsec.org.tt.
You may also visit our Investor Education website at www.investucatett.com or connect with us via any of our social media handles:

Published Article – Business Express Newspaper
July 22nd, 2020