Transaction Monitoring: Fighting Corruption and Protecting National Security

In an article in the Tuesday Wall Street Journal (WSJ), entitled "More foreign banks probed for sanctions violations", Brett Wolf reported that the New York County District Attorney's Office will shortly announce additional enforcement actions against banks for sanctions violations regarding Iran and Syria. In a speech made on November 14, Manhattan District Attorney Cyrus Vance talked about payments made to persons associated with sanctioned countries as constituting a threat "to US national security."

This reminded me of the ideas that my "This Week in FCPA" colleague Howard Sklar often speaks about; that being 'compliance convergence.' One of these areas where there is convergence with anti-corruption and anti-bribery compliance programs is anti-money laundering. While many persons discuss the techniques used in anti-money laundering as techniques which can or should be used in banking and other financial institutions' compliance programs, there is one area which companies should adopt from anti-money laundering directly into their anti-corruption and anti-bribery compliance programs and that is transaction monitoring.

For some time now banks have been required to monitor transactions of Politically Exposed Persons (PEPs). Generally speaking this effort includes requiring banks to apply enhanced due diligence to bank accounts and transactions by PEPs; requiring financial institutions to assess and evaluate risk so that it can be more carefully managed; promoting transparency in all transactions and monitoring transactions which might be termed suspicious. This means more than single transaction monitoring and is a more sophisticated approach which allows cataloguing and cross-referencing transactions.

Banks begin with the need for enhanced due diligence that they can determine when dealing with a foreign governmental official. This due diligence must include procedures "reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption." Banks make some or all of the following list of inquiries: identify the stakeholder and any beneficial owners; from this identification, determine the PEP status; obtain employment information and evaluate for industry and sector risk of corruption; review the stakeholder's country of residence and evaluate for level of corruption; check references; obtain information on immediate family members to determine PEP status; and make reasonable efforts to review public sources of information.

Although not couched in terms of the compliance lingo "Red Flag", anti-money laundering requirements make clear that simply identifying a stakeholder as a PEP does not disqualify the candidate. It means that additional investigation must be performed. Therefore, if a PEP comes up in your Foreign Corrupt Practices Act (FCPA) compliance program due diligence investigation, as an owner of a Foreign Business Partner, additional investigation must be performed to determine the relationship of this governmental official; the transaction at issue;

and any potentials for conflicts-of-interest or self-dealing. The promotion of transparency requires actual knowledge of the parties who are involved in all transactions. In addition to identifying those owners and any beneficial parties as indicated above, care should be taken to identify any shell companies which a PEP might have ownership or interest in. This is a critical analysis which companies should take as part of their overall due diligence effort.

While many compliance programs do a good job of the above due diligence and attendant analysis; companies do not take the next step, that being transaction monitoring, and integrate it into their compliance function.

Generally the Treasury Department, or some other functional group in a company has a policy preventing payments to locations other than (1) where services are delivered or (2) the home country of the payee. However, this other functional department rarely works in concert with the Compliance or Legal Department, in terms of notifying other company groups of a suspicious payments or even providing documentation of such suspicious payments and storage of such information in a mutually accessible database. Contrasting this, situation most companies will have a policy regarding the retention and contracting with agents or other foreign business representatives or partners but how often are such policies found for vendors in the Supply Chain. The next step in this transaction monitoring process is monitor each transaction to determine if it is 'suspicious', that is the term generally recognized by banks in the anti-money laundering context. How many companies have systems in place to perform the same suspicious activity analysis in the normal course of transacting business? Further, there are software program and other tools which a company can utilize which will automate this monitoring process.

Wolf reported that Manhattan District Attorney Vance said that payments out of certain financial institutions had "stripped wire transfer payments of information that would have revealed that sanctioned parties were engaging in US dollar transactions." How many companies could monitor that type of information for payments they may have made to vendors in the Supply Chain or agents in the Sales Chain for that matter? Near the end of his speech, Vance said that his office was "well positioned" to pursue such claims.

As banks and other financial institutions become more robust in their anti-money laundering programs, many nefarious individuals may move their activities to companies with less robust procedures and back-up systems to detect, record, store and share any such activity with the appropriate group within a company. This may well be the next US government target for inquiry.

should consult a qualified legal advisor. The author, his affiliates, and related entities shall not be responsible for any loss sustained by any person or entity that relies on this publication. The Author gives his permission to link, post, distribute, or reference this article for any lawful purpose, provided attribution is made to the author. The author can be reached at tfox@tfoxlaw.com.