REDEFINING DUE DILIGENCE: A paradigm shift for AML/BSA compliance

Money laundering, terrorist financing and fraud pose an increasing threat to the integrity of the world's financial systems. The Bank Secrecy Act (BSA) of 1970, sometimes referred to as the anti-money laundering (AML) law, requires financial institutions in the United States to assist U.S. government agencies in the detection and prevention of money laundering by keeping records of cash purchases of negotiable instruments, filing reports on purchases of ten thousand dollars or more and reporting suspicious activity that might signify money laundering, tax evasion or other financial crime. Financial institutions must demonstrate that:

- they have implemented internal controls for BSA compliance
- there is independent testing to verify compliance
- there is a designated person(s) responsible for BSA compliance
- they provide adequate AML training for staff

Portions of the BSA were amended in 2001 under Title III of the USA PATRIOT Act to facilitate the prevention and detection of international money laundering and terrorist financing and the prosecution of perpetrators. Financial institutions active in the United States or transacting business in U.S. dollars are impacted by provisions of the USA PATRIOT Act that mandate adequate anti-money laundering and customer identification processes. The law requires financial institutions to develop a Customer Identification Program (CIP) appropriate to the size and type of its business. The CIP must be incorporated into a bank's BSA/AML compliance program.

The global nature of financial and communication networks and the ease with which they can be used as a pipeline for illicit activities make worldwide collaboration an essential strategy for combating financial crime. Internationally, the Financial Action Task Force Recommendations, Wolfsberg Principles, EU Money Laundering Directives and the UNODC are indicative of the cooperative effort to create a broad network of AML regulatory provisions and policies.

New challenges face the global community following events such as the Arab Spring uprisings of 2011, the tightening of sanctions against Iran and the persistent evasion of current AML/CTF processes by drug cartels and corrupt political officials. Financial institutions must reinforce their fight against money laundering and terrorist financing by implementing tougher controls and expanding international cooperation while remaining compliant in a rapidly evolving regulatory environment.

The changing BSA/AML regulatory landscape

Regulators around the globe are responding to criticism of failed oversight of financial institutions with a newly energized focus on anti-money laundering and related risk. The recent spate of regulatory enforcement actions, significantly higher fines and massive media attention given high-profile cases like HSBC have bolstered institutions' AML efforts in 2013.

The Office of the Comptroller of the Currency's Semiannual Risk Perspective report issued in June 2013 stated that BSA/AML threats are increasing as a result of changing methods of money laundering and an increase in the volume and sophistication of electronic banking fraud, while compliance programs are failing to evolve or incorporate appropriate controls into new products and services.

Enforcement actions by the Department of Justice and the Securities and Exchange Commission (SEC) for insufficient due diligence on international business partners have pointed to several common problems:

- lack of timely and sufficient due diligence
- inadequate verification of information provided
- ignoring red flags that have been identified

Leveraging the media attention, both the Financial Crimes Enforcement Network (FinCEN) and the SEC announced plans to introduce new proposals for more proactive AML measures for broker-dealers and investment advisors. FINRA also indicated that its examination priorities would focus on AML, citing specific concerns with the level of due diligence on foreign bond currency conversion transactions.

Early this year, the European Commission announced the Fourth AML Directive intended to prevent money laundering and terrorist financing by strengthening AML rules in the EU. In addition, a new entrant into the AML arena, The Basel Committee on Banking Supervision, is proposing requirements for banks to include AML in

their enterprise-wide risk management. The committee also refers back to the Financial Action Task Force's global AML standards issued in 2012 and more recently issued guidelines. As further evidence of the worldwide focus on AML, the UK Financial Conduct Authority, Hong Kong Money Authority, New Zealand's Reserve Bank and Department of Internal Affairs and Financial Markets Authority have all ramped up their supervision by placing greater emphasis on AML risks.

The Federal Reserve Board recently demonstrated just how far the regulators are willing to go when they delayed the planned merger of a New York-based institution due to alleged shortcomings in their BSA/AML compliance program. Under a written agreement with the Federal Reserve Bank of New York, corrective action was mandated to include a revised firm-wide written BSA/AML compliance program, a revised written customer due diligence program, a written suspicious activity monitoring and reporting program and a six month suspicious activity look-back review.

Shortcomings in the current approach to KYC/CDD/EDD

Know Your Customer (KYC) and related due diligence activities are the foundation of a sound BSA/AML program. Financial institutions and other regulated companies are obliged to verify the identity of their customers at account opening, assess their customer risk, conduct ongoing due diligence of high-risk customers and monitor transactions to detect and report suspicious activity. Although the regulatory requirements are fairly clear, organizations are left to their own devices when it comes to the details of setting up effective AML programs and selecting the systems and tools to facilitate the labor-intensive processes for KYC, Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD).

When sharing observations of industry issues at a recent ACAMS conference, representatives from the Office of the Superintendent of Financial Institutions (OSFI) presented their risk management expectations while contrasting what they actually see. EDD was of particular interest to these regulators after repeated examination findings showed EDD looking very much like standard due diligence. Their directive indicated that EDD measures should be clearly distinguishable from baseline CDD. Based on their findings, they issued the following recommendations:

- Design EDD to ensure more attention is paid to higher risk customers and the attention is commensurate with the risk level
- Build an enterprise-wide risk assessment methodology and EDD approach across all business lines for consistent and appropriate identification and monitoring of high-risk clients
- Perform enhanced monitoring not only at point of sale/account opening but also at the transaction level
- Ensure that EDD measures apply to all high-risk situations and that they address and mitigate the risk factors identified
- Update customer information and changes to products, etc. in a timely fashion
- Implement effective CAMLO oversight.

Regulatory standards call for a risk-based approach that is appropriate to an institution's business. However, more often than not, risk is viewed as a static, point-in-time snapshot rather than a dynamic activity. Although regulatory guidelines address ongoing due diligence and adjustments to risk assessments based on changes in a customer's account profile and transactions, this is not the same as dynamic risk management. There is a disconnect with the real world of continual risk which begs the need for a dynamic risk model and the technology that can support it.

Due diligence redefined

To redefine due diligence, one must consider the dynamically changing global environment in which individuals and entities operate, the relevance of their social network or six degrees of separation and the nature and frequency of any related negative media.

The traditional buckets of high, medium or low risk customers present a one-dimensional view with no further differentiation on degrees of risk. A more accurate view and ranking of risk can be determined by analyzing an individual profile in conjunction with its social network (who they are linked to) and any negative media direct or through links. This methodology assigns a value to measure the degree of risk, making it much easier to identify and focus on the highest risk first. For example, in a risk-based approach using typical assessment criteria only (products, geography, historical transaction amounts), a customer may be categorized as low risk when, in reality, once their links and newsworthiness are factored in they present a greater exposure to risk.

It becomes difficult, if not impossible, to stay ahead of the bad guys in an environment where sanctions, PEPs, news and other web information change constantly. Dynamic risk management calls for technical solutions that employ a daily surveillance model; however, finding the optimal balance of risk mitigation and alert management can be problematic. Introducing a classification or prioritization hierarchy into the screening technology orders alerts by risk and accuracy of the match. This provides a transparent framework from which thresholds can then be drawn based on an institution's requirements of what matches to review and in what order to review them.

Taking the first step forward

Globally, regulators and governments will continue to remain active in clamping down on AML failings. Institutions must now re-evaluate their programs and shore up any weaknesses. They can start the process by:

- Understanding the benefits of a shift from static to dynamic risk management
- Completing a cost/benefit analysis to assess the viability of keeping legacy systems and processes
- Exploring hosting alternatives to address budget and resource constraints
- Considering a principles-based versus rules-based methodology for entity resolution
- Implementing solutions that provide a more granular and interconnected view of risk with features for link analysis, link monitoring and news monitoring.

In a recent industry survey on the global cost of AML compliance, 66 percent of the 284 respondents in 46 countries saw an increase in their AML and OFAC compliance budgets over the last three years.[1] The option exists to continue spending money supporting traditional approaches with known gaps and shortcomings or to explore new methodologies that strengthen due diligence programs by identifying and prioritizing enterprise risk on a daily basis.

Carol Stabile, CAMS, senior business manager, Safe Banking Systems LLC, Mineola, NY, USA, carol.stabile@safe-banking.com

[1] Veris Consulting, Inc. (2013). The global cost of anti-money laundering compliance [PDF file]: http://www.verisconsulting.com.