



The Overlooked Key to Successful Transaction Monitoring – Skilled People and Effective Procedures

David B. Caruso, CEO

The Dominion Advisory Group

SUMMARY

Transaction monitoring software has become a requirement for all mid size and large banks. Many institutions are led to believe that the implementation of such systems will ensure AML compliance and protect against regulatory failures. This is not true. The implementation of transaction monitoring software, if not complimented by a well trained, experienced and fully staffed unit of analysts and investigators, will only lead to more compliance challenges.

ABOUT THE AUTHOR

David Caruso, CEO of the Dominion Advisory Group, has more than 15 years of experience creating and implementing comprehensive Anti-Money Laundering (AML) programs. As CEO, David is responsible for providing strategic leadership and industry expertise to ensure clients receive the best possible solution for regulatory compliance issues.

Effective anti-money laundering (“AML”) compliance programs rely upon the ability of an institution to identify, analyze, investigate and report suspicious activity. Without this capability an institution’s efforts to comply with regulatory requirements are likely to fail.

As a result, large and mid-sized financial institutions are moving rapidly to implement transaction monitoring software that detects suspicious activity. Purchasing software is often believed to be the key element in fulfilling obligations to ferret out customer wrongdoing. Banks are spending millions of dollars to implement monitoring software, but are often overlooking the most vital component of any monitoring program – having skilled professionals who can make meaning out of the flood of reports generated by the software. The inability of banks to effectively assess, prioritize, properly analyze and thoroughly investigate exceptions generated by monitoring systems is the primary cause of regulatory enforcement actions.

Regulatory application of the PATRIOT Act made the implementation of transaction monitoring software a de facto AML compliance requirement. In the last several years numerous software firms have developed products that assist financial institutions in their efforts to identify transactions that may be suspicious. To identify suspicious activity, most of these products operate similarly - they: (1) attempt to capture and aggregate as many of a customer’s transactions from as many different bank systems as possible and (2) pass them through filters to (3) detect anomalies based on transaction history, (4) or to identify transactions that are out of the norm when compared to peer customers, or (5) to identify transactions that match a pre-determined pattern of activity, the characteristics of which are built into the software, that is known to be a method of money laundering or terror financing.

Regardless of the software a bank selects and the time and expense of implementation, the key to success of monitoring is whether or a not an institution has developed effective procedures and processes to resolve the exceptions produced by the transaction systems and whether or not it is has trained, skillful professionals to execute those procedures.

When marketing their products, some technology firms outwardly or tacitly suggest that software provides a complete solution to an institution's need to monitor and report suspicious transaction activity. Unfortunately some banks hold the same view. The reality is much different.

Software creates numerous challenges the greatest of which may not be the likely cost overruns and delays traditionally found in large technology implementations. The challenges faced after implementation, if not addressed properly, can undermine a transaction monitoring system and actually create more problems for an institution than when no system was operating. Some post implementation challenges include:

- Validating that transaction exception thresholds in the software are properly set
- Adopting comprehensive procedures, and manuals to ensure exceptions are resolved in a consistent, methodical, and sufficiently documented manner
- Prioritizing exceptions to ensure those presenting the greatest risk are resolved first
- Ensuring staffing levels are appropriate to resolve exceptions in a timely manner
- Ensuring staff are properly qualified and trained to perform the functions required to investigate and resolve exceptions
- Adopting effective escalation processes to ensure high risk exceptions are reported to appropriate management
- Adopting thorough procedures to report suspicious activity to staff, management, a board of directors, and the government as required by law
- Implementing processes to perform enhanced monitoring on those customers whose activity is regularly identified by the software as high risk
- Implementing comprehensive programs to manage high risk customers in accordance with Enhanced Due Diligence guidelines or laws

Institutions that have not thought through and resolved these issues will surely put tremendous stress on their AML compliance operations.

Once a transaction monitoring software system is implemented it's guaranteed that the number of exceptions generated will add substantially to the work load of the AML compliance staff, especially when these new exceptions are added to the exceptions generated by existing systems.¹ This is where an institution that has not addressed the challenges listed above faces extreme difficulty, and exposes itself to regulatory criticism, or worse, regulatory violations.

The specific problem is: How does an institution make its way through all the exceptions in a way that ensures those of highest risk and those that should be reported to the government are investigated first? Compounding this problem is the likelihood that many institutions do not have staff with sufficient training and experience to provide the answer to that key question. The demand for skilled and experienced analysts and investigators has never been higher. Unfortunately the supply of people with these talents is diminishing, if it hasn't already run out. As a result, institutions are anxious to ensure they are not accused by auditors or regulators of

¹ Prior to installing software, banks should have existing means to identify unusual activity. These would include proprietary database systems to identify unusual cash and wire activity; a program to investigate the subjects of subpoenas and other government requests received by the bank; and, investigating allegations contained in referrals from employees who notice activity that needs further review.

falling behind in their investigations. In some countries, like the U.S., the reporting laws have specific requirements as to when Suspicious Activity Reports must be filed. The law reads as follows:

Time for reporting. A bank is required to file a SAR no later than 30 calendar days after the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect was identified on the date of detection of the incident requiring the filing, a bank may delay filing a SAR for an additional 30 calendar days to identify a suspect. In no case shall reporting be delayed more than 60 calendar days after the date of initial detection of a reportable transaction. In situations involving violations requiring immediate attention, such as when a reportable violation is ongoing, the financial institution shall immediately notify, by telephone, an appropriate law enforcement authority and the OCC in addition to filing a timely SAR.

Filing late SARs is among the worst regulatory transgression an institution can face.

The number of SAR filings by U.S. financial institutions has skyrocketed in the past several years. Among the reasons for this are the interests institutions have in assisting law enforcement as well as their interests in avoiding the type of severe regulatory and legal action suffered by Riggs and AmSouth. Many inside the government and from industry are concerned such increases in filings make it difficult to identify those SARs that are truly worthwhile in aiding efforts to identify terror financing from those SARs that are filed defensively and that have little value to law enforcement.

Exacerbating the problem of overfilling are the results likely found in the combination of the serious consequences of filing late SARs; the substantial number of exceptions monitoring systems produce; and, the challenges banks face hiring and retaining skilled and experienced investigators.

ABOUT THE DOMINION ADVISORY GROUP

Dominion Advisory Group is the leading provider of comprehensive and sustainable anti-money laundering programs and critical investigations services for top domestic and international financial institutions, law firms, and other organizations. Dominion Advisory Group has 15 years of extensive experience in banking, compliance, law enforcement, regulatory oversight, technology, and consulting to help financial institutions and corporations navigate the complex regulatory environment and address the needs of regulators, customers, and the institution.

5885 Trinity Parkway, Suite 220, Centreville, Virginia 20120
Main: 703.815.1550 Fax: 703.485.8012 Email: info@dominion-advisors.com