



The Most Important Issue in AML Compliance – Conducting Thorough Investigations

David B. Caruso, CEO

The Dominion Advisory Group

SUMMARY

There is no more important aspect of BSA/AML compliance than conducting accurate, complete and timely investigations. Filing Suspicious Activity Reports is arguably the sole purpose of BSA/AML compliance. There is no one, set way for institutions to comply with this requirement. This paper provides guidance on how to establish an effective suspicious activity identification and investigation program.

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.

There is no more severe a compliance breakdown than the failure to file Suspicious Activity Reports (SARs). Although AML/BSA compliance programs have many components, including training, audit, policies and procedures for things like account opening and customer risk rating, the single most important piece of an AML/BSA program is to have effective processes to identify, analyze, investigate and report suspicious activity.

The failure to file SARs when the government believes one should have been filed can lead to criminal prosecution. The cases of Riggs Bank and AmSouth prove this. How many banks have been the subjects of Department of Justice investigations because a training program was inadequate, or a piece of Customer Identification Program information was missing, or a customer wasn't risk rated properly? None. Banks are issued enforcement actions when a regulator finds strong evidence that an institution is unable to consistently and systematically identify and report suspicious activity. A prosecutor makes a decision on whether to act based upon how serious the failure to file SARs was and was it the result of willful blindness on the part of an institution.

A failure to file a SAR or the failure to file SARs accurately or timely can be considered, in the case of a national bank, a violation of Title 12, Section 21.11 of the Code of Federal Regulations. State banks, foreign banks operating in the United States, thrifts, credit unions and broker dealers of securities are bound by similar federal requirements as administered by the Federal Reserve, the Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, and the Securities & Exchange Commission.

A violation of the SAR filing requirements has the force of requiring a regulator to contemplate if such a weakness warrants the issuance of an enforcement action based upon the presence of a violation of the Code of Federal Regulation, Section 21.21 also known as a "program failure" of the BSA. If the institution's failure to file SARs is so troublesome the Department of Justice may find it necessary to investigate that institution using its investigative and prosecutorial authority under Title 31, United States Code, Sections 5322 & 5318(g).

Many argue that a financial institution's failure to file a SAR or SARs should not be a criminal matter, but instead, an issue between that institution and its regulator. Since the Riggs and AmSouth criminal pleas and recent media reports suggesting other banks may be under investigation by prosecutors in New York City, the topic of whether an institution's violation of a regulation should carry the weight of criminal culpability has been a point of some fiery

debates.

Some however, wonder why there is even a debate. After all, the text of the U.S. Code is clear and the responsibility to file SARs is well known and understood by financial institutions as are the ramifications of not filing. One could, it seems, conclude that institutions would make detecting, investigating and reporting suspicious activity the primary focus of their compliance efforts and thus implement processes that would protect them from regulatory compliance failures.

The government's view of the importance of ensuring financial institutions file SARs can be best described as written in the Government's Memorandum in Aid of Sentencing in *United States of America v. Riggs Bank N.A.*:

"The requirement to file SARs under the BSA does not exist in a vacuum; it exists to detect and prevent criminal activity. Congress enacted the Bank Secrecy Act to address an increase in money laundering criminal activity utilizing financial institutions, to require insured banks and other financial institutions to maintain an effective BSA and anti-money laundering program to detect and report suspicious activity therein that might be indicative of money laundering and other financial crimes, maintain certain records, and file reports that are especially useful in criminal, tax or regulatory investigations or proceedings. (T)he BSA regulatory regime constitutes law enforcement's first defense against the misuse of the U.S. financial system by money launderers and terrorist financiers."

Many financial institutions contend that examination procedures are too vague and leave too much room for interpretation by the regulatory agencies. However, if each enforcement action over the past several years and the underlying facts leading to them are understood, it would be clear the notion an action was issued because of a difference of opinion over some vague point during the examination is false.

With all the enforcement actions issued over the last three years and with so much media attention of AML/BSA matters one would think every institution would by now have robust and effective ways to identify suspicious activity. But do they? And how do they ensure they have it right?

Six components are necessary to make sure an institution has an effective program to identify, investigate and report suspicious activity. They are:

1. Effective ways to identify and capture potentially suspicious activity
2. A formal process of analysis, investigation, management review, and quality assurance of suspicious activity cases and SARs
3. Written standards of investigation, case documentation, and management decision making criteria
4. Ensuring the right people with the right skills and experience are executing the process of investigation and reporting
5. Proper use of case management and management reporting tools
6. The use of information obtained and assessed from investigations to better manage and predict AML/BSA risk

1. Capturing Suspicious Incidents

There are many ways in which information about potentially suspicious activity is gathered. Transaction monitoring software, employee tips, media reports, subpoenas and other government requests, and tips from other financial institutions are just a few. How these incidents are collected and prioritized is vital.

Well designed manual and technical systems to obtain and sift through numerous alerts are essential to ensure an

institution is aware of the type of data that may indicate its customers or employees are engaged in suspicious activity. Case management systems are necessary to capture, track and record data that may become investigations. Case management systems also enable institutions whose operations are wide-spread domestically and internationally to capture and track case information in a way that a small local or regional institution may not have to. Without effective case intake and tracking systems institutions may fail to gather and review potentially suspicious activity, or in the case of large complex institutions, may gather the information at multiple points, but not coordinate investigations and thus expend resources needlessly.

Once information pertaining to potentially suspicious activity is gathered and recorded into a case management system, the next step is to begin a process that may lead to a SAR filing.

2. The Investigations Process

Financial institutions are organizations where success depends upon the effectiveness of process execution. Banks collect deposits; credit them to accounts, process checks and other items, process loan requests and fund loans. A broker dealer executes trades quickly and at the best price for the customer. Financial institutions are built upon sound processes. Completing investigations should be thought of in the same way.

Commonly, investigation of suspicious activity is something considered to be outside the core practices of financial institutions. Often, those conducting investigations are either former law enforcement who may have limited knowledge and experience of banking and finance, or auditors who may try to apply auditing skills to investigations. Usually, investigation groups are a bit of a mystery to the rest of an institution. Sometimes they are part of an existing security or fraud group and sometimes they are part of a compliance department.

Regardless of where the group of individuals who investigate suspicious AML activity sit, it is essential that they approach their work in a systematic and consistent way. The investigation of suspicious activity should be designed to be a business process like any other business process. It should have documented standards that are consistently applied by a skilled and trained set of individuals who use technology and other systems to assist them in their work.

The process of investigation needs to include at least five steps:

1. **Analysis of Exceptions:** A process of analytical review must be applied to each transaction exception to determine if it merits a full investigation. The number of exceptions and incidents reported from monitoring systems is too large for each to be thoroughly investigated. The result of this step is to determine if the incident or exceptions has the attributes of potentially suspicious activity and should therefore be fully investigated.
2. **Investigation:** Only those exceptions or incidents that are determined after an analytical review to warrant an investigation are reviewed in this step. Investigations must be thorough and include historical account and transaction review, a review of CIP and KYC information, a review of other accounts and related accounts and relationships, and a review of public record information related to the customers and counterparties.
3. **Management Review:** Investigation cases files should be reviewed by management to ensure the investigative report conforms to established standards, contains cogent explanations supporting the decision to file a SAR or to not file a SAR, and is of the quality to withstand an intense review by an auditor or examiner, or in some cases a prosecutor.
4. **Quality Assurance:** During this step a SAR is reviewed, prior to it being filed, to ensure it is completed fully

and accurately. Instances where fields are left blank or contain erroneous information such as listing the wrong Social Security Number for a suspect or inadvertently transposing account numbers are considered to be technical errors and are certain to be criticized by an auditor and may be considered a violation of law by the regulatory examination team.

5. Reporting: This is the step where the SAR is actually filed with FinCEN. Many institutions still file SARs by mail, choosing not to take advantage of the electronic option offered by FinCEN. Using the electronic filing, an institution is able to receive confirmation the SAR was accepted. Using outdated methods like the U.S. mail are prone to human error, both on the part of the institution as well as the Postal Service. It would be a shame if the hard work designed to comply with the BSA failed to show up at FinCEN.

When investigations are treated as important as other fundamental day-to-day operational processes, it is then that an institution can be confident it has designed an adequate AML/BSA compliance program.

3. Written Standards

The process of investigations described above will only be as sound as the written standards established for how to conduct analysis and investigations. In addition, written standards need to exist describing how an institution documents (either through paper or electronically) its case files. This means case files should have the same or similar type contents from one investigation to the next. If the physical or electronic case files of an investigations group are inconsistent and reveal that few standards are applied, this will be the first sign to an examiner the institution's process to identify and report suspicious activity needs enhancement.

An institution's written standards should be based upon published FinCEN and other regulatory guidance.

Written standards are one way to help an organization to ensure work product from numerous analysts and investigators is of the same quality. Without these standards, each analyst and investigator will naturally create their own standards (or sub-standards) and these are certain to have varying levels of effectiveness. It is also likely that if no written standards exist, the evidence needed to support the institution's decision on whether or not to file a SAR will be lacking. It is instances such as this that cause the type of regulatory findings likely to lead to some sort of enforcement action.

Written standards need to apply to all AML/BSA analyst and investigative staff and must apply equally throughout the locations, both domestic and international, of an institution.

4. The Right People

Having staff and managers skilled and experienced in the process of analysis and investigation is the most important element of an AML/BSA program. Some may be surprised by that statement. However, when one examines the underlying circumstances that lead to enforcement actions, they always contain one glaring truth: the institution failed to detect, investigate, and report suspicious activity.

Institutions need to hire individuals who have the necessary skills and experience to conduct complex financial crimes investigations and also individuals who can manage staff who conduct less complex but, no less important, investigations. Hiring former law enforcement officers and agents to fill these investigative and management roles is common, as is hiring people from other financial institutions with similar qualifications.

Whoever an institution hires needs to have a deep understanding of financial crime, money laundering and terrorist

financing. Understanding the regulations and reviewing regulatory guidance is important, but investigators need to be able to realize how criminals act and how they manipulate others and manipulate free market economies to ply their trade. Investigators also need a good grasp on issues relating to international affairs to better understand how countries and regions of the world are impacted by issues like corruption and tyranny. These countries are often the source of narcotics and terrorism and transactions to and from them or involving certain political groups or members of a ruling elite poses a greater risk to institutions.

Investigators need to know how to write concise and cogent reports that will be meaningful to law enforcement and therefore less prone to criticism by regulators. Investigators should have access to as many customer records and as many front office staff as is necessary to complete their duties. Limiting investigator's resources and erecting processes to prevent them from interacting with front line staff and relationship officers is sure to lead to trouble.

Good investigators are the core component of all successful AML/BSA programs and institutions should treat them as such.

5. Case Management and Management Reporting

Financial institutions track many important sets of data. Most of it focuses on those things that generate revenue like; the number of new accounts opened, the number of new mortgages funded, the number of foreign ATM transactions and so on. Among the more important non-revenue generating data to keep track of are those that pertain to investigations.

Case management is a vital part of an AML compliance program, especially for institutions whose investigative staff is spread across numerous locations. The most important aspect of case management is to track the number of open investigations and their age. Age is important because of the requirements of 12 CFR 21.11 which states, in summary, that institutions must file SARs within 30 days of detecting suspicious activity. If a manager does not know what cases are open, what they are about, and how old they are, it makes complying with this requirement almost impossible. Failure to comply in this instance will have severe regulatory consequences.

Case management systems are also the data collection point of many important pieces of information that should be reported to management. For example, case management systems, at their most basic level, should track the number of cases, both open and closed, and the disposition of those cases i.e. which ones ended up in a SAR and which ones did not.

Case management systems also provide meaningful information that enables an active compliance department to better manage its AML/BSA risk.

6. Using Investigative Information to Improve a Program

Often investigations of suspicious activity and filing of SARs is considered the last part of an AML/BSA compliance program. Many hold the view that once Investigations finishes its job the matter is "over." Such a view, although common, fails to take into account the value of information investigations and SARs provide.

Most aspects of AML/BSA compliance are predictive in that they rely little on actual data, but rather on guidance from regulators, input from wise compliance officers, and a little guess work. For example, customer risk rating is an exercise which largely attempts to assign a score or value to certain attributes an institution believes present a higher AML risk. Customers from certain countries are likely "scored" higher than others. Customers who indicate they may send wire transfers may also be rated higher risk. Whether these things are true is debatable.

Investigations and SARs however provide known facts. Investigations and the information they provide can tell an institution if there are branch locations or relationship managers whose customers have a higher propensity to engage in suspicious activity. Data from investigations may also inform an institution which products and services actually do pose a higher risk for them.

In my experience very few enterprise AML/BSA risk assessments use the information from investigation files and SARs, when in fact it should be the place to start a risk assessment and if done properly, may be the only place the risk assessment needs to focus.

There is no more important component of AML/BSA compliance than completing thorough and timely investigations. A program lacking this capability is almost sure to have weaknesses that will surface and cause damage to an institution, its employees, and its customers.

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