On Alert: Designing Effective AML Monitoring Processes

SYNOPSIS: This article first appeared in ABA Bank Compliance magazine in October 2008. Co-authored by David Caruso, CEO of Dominion Advisory Group and Dan Soto, SVP, Director of AML and BSA Officer for Wachovia Corporation, the article addresses one of the most pressing needs among AML professionals: How to design and implement a transaction monitoring process that effectively identifies suspicious activity.

Among the more difficult anti-money laundering compliance challenges is managing and effectively addressing large numbers of transaction alerts produced by software monitoring systems.

Many in the AML field would say that most financial institutions are victims of transaction monitoring overload. Software programs designed to detect potentially suspicious activity and to protect the reputation of the institution, if not properly designed, produce far too many alerts, the large majority of which may provide little value in detecting suspicious activity.

However, AML experts and government officials worldwide expect most alerts, if not all, be properly researched and resolved. It's safe to say an element of fear pervades this approach ("What if one of the alerts leads to the next terror attack or a large international narcotics operation?")

So the challenge is: How to deal with a torrent of alerts whose likelihood of ending up as a SAR oftentimes is minimal? Compounding this problem is that these alerts begin to "age" the day they are produced and pressure exists to resolve them quickly. Without the quick response, the institution could find that regulators will likely express concern regarding the timely reporting of suspicious activity.

The most effective and efficient way to deal with the challenges of analyzing large numbers of alerts and aging issues is to implement a distinct and well-defined process of analysis.

This article will drill into the specifics of what that analysis is and how it's done.

First we should be clear about the purpose of analysis. The outcome of analyzing an alert is to determine if:

1. The activity is not suspicious and can be resolved relatively quickly; ***or***,
2. The activity *may* be suspicious so it should be referred for further investigation.

It's wrong to assume all alerts from a monitoring system should be investigated. No matter how good (or bad) monitoring filters are, the alerts they generate still need one more filter: a human being that is trained, skilled and experienced in analysis and who has a strong understanding of money laundering and financial crime. In addition, the analyst should have a full understanding of the business transaction that produced

the alert. Access to company documents and information is paramount in the analysis phase of the alert review process.

Some readers, at this point, may be asking themselves: "My "investigations department' is one or two people; Do I need to concern myself with this approach?"

In short, yes.

A multi-step process of detection, analysis, investigation, quality control and filing makes sense for small-to-mid-size as well as large institutions with sizeable AML departments, *and* it also makes sense to apply this approach in order to prevent unnecessary work and resolve matters quickly where able, regardless of the size of an institution.

Defining Analysis

By "analysis" we mean a process where the elements of the alert (i.e. the reasons for it) are *reviewed* and *related* to what the analyst knows of money laundering, terror financing, financial crime as well as what is known about the parties involved in the transaction(s) in order to answer some keys questions:

1. "Does this activity by itself have the appearance of being *potentially* suspicious?" (Three, $9,900 cash deposits at multiple branches on the same day or customer that receives a large wire transfer from an unknown and unrelated source).
2. "Is this activity, if it does <u>not</u> by itself have the appearance of being potentially suspicious, inconsistent with the expected activity for this customer?" (A salaried employee of a local municipal government is depositing $18,000 a month in cash).
3. "Is the activity of a nature that a reasonable explanation for it cannot be reached?" (Primarily cash transactions in a traditionally non-cash business).

If the answer is "yes" to any these questions, the matter must be further investigated according to the standards set forth by FinCEN and the FFIEC.[1]

If the answer is "no" to these questions than the matter can be resolved immediately.

"Analysis" in not "investigation." An investigation by its nature is more comprehensive requiring much more research of a customer(s), transactions, related parties; requires more evidence and documentation; and needs a comprehensive written report supporting conclusions. A proper AML investigation likely takes, on average, between 3 – 6 hours to complete.

By contrast, analysis requires less documentation, does not determine whether a SAR should be filed and should take between 15 – 45 minutes to complete.

A quick example of a common "alert" an AML professional regularly faces; Let's call

[1] See FinCEN's 2003 publication, "Guidance on Preparing a Complete & Sufficient SAR Narrative," and the FFIEC BSA/AML Examination Manual, Core Examination Procedures for Suspicious Activity Reporting and Appendix L: SAR Quality Guidance.

the alert a "large balance fluctuation." On April 10th customer Joe's account balance increases by over 1,000%. On April 14th his account balance decreases by almost the same amount.

Most so called "red flag" publications and transaction monitoring systems pick this up because perhaps it's a narco trafficker dumping $250,000 in cash into his account and then he sends out a wire (as if a money launderer would be so foolish).

The analyst open the alert and take a peak at the deposit item that led to the 1,000% balance increase and notices that the issuer of the check is "Suburban Title, Escrow Account." The analyst then looks at the outgoing wire and notices it's to Toll Brothers, one of the nation's largest homebuilders. Within a few short minutes the analyst realized they have someone who sold their house and then bought a new one. Whew, crime solved!

Conducting Analysis

To be effective, as noted earlier, an analyst must have access to all bank systems needed to research transactions and obtain customer due diligence information. An analyst should be able to view many months of statements showing deposit and withdrawal activity; wire transfer information including system notes that often accompany wire details; teller journals; images of deposit items and deposit tickets; and, any legacy system that contain customer information like dates of birth, addresses, employment, source of funds, and related accounts.

Furthermore, an analyst must have access to public record information provided by subscription databases or certain sites on the Internet. Its preferable that analysts also have access to specific AML subscription databases that compile lists of "troubling people", such as entities that have either been convicted of crimes or are alleged by reputable sources to be involved in suspicious activity.

Analysts equipped with the right tools are ready to begin their work.

The first step in transaction activity analysis is to understand the system from which the alert was generated. Was it a software-monitoring program? Contrast this from other sources of "alerts" -- An exception report from a Monetary Instrument Log? A referral from a branch employee?

The source of the alert matters because it provides the analyst with some idea of the methodology or logic used to indentify the transaction as unusual. For example:

- A software-monitoring program may have logic that detects events that deviated from a norm (i.e. customers of a certain type do X and don't do Y so this customer is doing something the software thinks is Y – in other words they may be acting differently from norms or from their peers).
- An alert from an exception report may be the result of a compliance officer scanning a printout of a monetary instrument log and something has "jumped" of the page at them (i.e. five $9,000 cashiers checks sold at one branch in one day).

- A referral from a branch may have more information than other alerts because the employee can offer their views and opinions on what occurred that led to a referral.

Understanding the nuances and peculiarities of each source of an alert helps the analyst answer a fundamental question: "Why am I looking at this alert?"

After understanding the source of the alert and why it was produced, an analyst should be asking: "Have I seen something like this before?" If "yes" than what was the outcome? Was it referred for further investigation or was it resolved? What were the reasons for that decision? Being able to recall previous alerts of a similar nature helps an analyst put the current alert in context and then asking, "Is this the same situation I have seen before?"

In the first few minutes of reviewing an alert the analyst should be determining the essential elements of the activity by discovering *who* was involved, *where* did the activity occur, *when* did it occur and, has it "happened before."

The analyst should complete the initial intake and review of the alert by looking into the case management system to see if this specific customer has had previous alerts and understand the outcome of those alerts. If previous alerts did occur, it should be determined if the current alert is related in any way. That is, does this current alert involve the same people, location, transaction types and amounts? If so, what was the decision on that prior alert(s)? However, the analyst should also be careful not to over-rely on previous decisions. The new alert may provide information that paints a clearer picture of what is occurring. Perhaps the activity now looks even more suspicious, or perhaps it now looks less so.

From the time the analyst first looks at the alert to this point in the process, somewhere between 5 – 8 minutes should have passed.

Let's assume that the customer whose activity we are reviewing has had no prior alerts and we are not able to quickly resolve the matter.

At this point a more rigorous analysis must begin. This analysis will seek to answer the *who, what, when, where, how* and *why* of the alert.

- *Who* was involved in the activity? Identify the customer and other parties involved including counterparties, originators and beneficiaries. Determine if the account has multiple authorized signors and which of the signors was involved in the activity that alerted. Does the person(s) engaged in the transactions have other accounts or relationships with the institution? Are those accounts involved?

  Customer due diligence information should be reviewed to determine how long the account has been opened, who opened it and who is the authorized to conduct activity. The purpose of the account should be understood - is it a personal checking account, a business account and if it is, what is it used for – payroll, accounts receivable, or other operating purposes?

If after reviewing the due diligence information available on the bank's systems its still unclear who the customer is or what they do, an analyst should search public records data bases for information that may be helpful (databases such as Lexis-Nexis and Choicepoint are examples of information providers). An analyst should also search trusted sites on the Internet to gather additional information, but should remember to understand the veracity of the source (i.e. information published in the Wall Street Journal is likely much more reliable than information from a blog run by a person you've never heard of).

- *What* was involved in the alert is the next question the analyst should address. By "what" we mean was it cash deposits and/or withdrawals, was it something the customer said to the teller, was it a wire transfer sent or received? The analyst needs to begin to ask, "does what I know make sense for this customer?" (An analyst needs to be asking this throughout the review process).

- *Where* did the activity occur? Was it at a branch, through Internet banking, or over the telephone? Did it occur domestically or internationally? If it was domestic was it in a market the bank serves? If it occurred internationally was it in a jurisdiction the bank considers "high risk?" Where were the other parties involved in the transaction located and does this present additional risk? For example, if the originator of a wire transaction is in Yemen and the recipient (the customer) is located in Jersey City, NJ that may present a different level of "perceived" risk than if the originator is from Las Vegas and the customer is in Dallas.

- *When* the transaction(s) occurred not only applies to the date or dates on which they occurred but also the sequence of transactions. By this we mean was a large cash deposit followed by an outgoing wire two days later. Were the suspect transactions made shortly after account opening or were they made in an account that is been relatively inactive for months?

- *How* did the activity under review take place? Were large cash deposits made by the account holder or someone else? If the activity was initiated via the Web or telephone can the originator's identity be authenticated?

- *Why* did the activity occur is the final question an analyst must answer. If after progressing through each prior step as necessary the analyst is able to provide a reasonable explanation for the activity they should record that explanation and move onto the next alert. In other words, the analyst has decided the activity in question is not suspicious and does not even warrant a more comprehensive investigation.

  If the analyst is unable to provide a reasonable answer to "why" this activity occurred, then the alert must be referred or set aside for further, more detailed, investigation. The investigation will then determine if a SAR is necessary.

Conducting analysis as described above should take between 15 and 45 minutes including documenting findings and conclusions.

Documenting Analysis

There are no requirements mandated by FinCEN or the FFIEC regarding how banks document decisions made from conducting analysis, only that they should.

We approach documentation with a simple view: An independent third party (i.e. regulatory examiner or internal auditor) should be able to read an analytical review and it's supporting evidence and be able to understand why a decision was reached.

In other words, written documentation around analysis needs to clear, concise, and supportable.

The burden of resolving large numbers of alerts may lead to shortcutting the analysis process and particularly shortcutting documentation. Only writing explanations like, "No suspicious activity found," or, "Activity consistent with customer type," or "No referral needed" is not considered acceptable.

An independent third party, such as an auditor or examiner, must be able to understand how and why a decision about an alert was reached. Examiners will look at these "no refer" alerts very closely because it is a key decision point that if not well controlled can call into question an entire suspicious activity detection program.

Work Flow

Real success of a transaction monitoring program hinges on implementing defined workflow. Workflow is defined as a controlled repeatable process carried out by people with specific roles and responsibilities; in this case a monitoring analyst.

The workflow produces decisions (resolve and alert or refer it to investigation) and produces documented analysis and case files. The workflow is not subject to the unique style or skills of any one individual, but rather is something that can be executed by any well-trained analyst over and over again. This brings consistency to how matters are resolved, a requirement for any program that wants to be considered compliant.

Workflow is a core component of transaction monitoring. It's the difference between a thoughtful, repeatable, and sustainable process and a bunch of people working alerts.

Most analytical and investigative workflow happens very quickly and is often carried out through a case management system. But, regardless of the amount of software a bank uses, the concept and realization of methodical and controlled workflow is essential. Without it, quality is difficult to maintain, reporting is unreliable, and compliance is jeopardized.

Workflow is also about how alerts are prioritized and assigned. Since most monitoring groups will almost always be fighting the problem of falling behind in their work, its vital that those alerts that appear to present the most risk are worked

first, and that they are assigned to people who have the skills and capabilities to resolve them quickly and properly.

Each institution has its own products, services, customer types and locations of operations that bring a certain amount of uniqueness to its AML risk profile. Its encumbant upon each institution to know which type of alerts present the most risk. For many it may be those alerts that involve large volumes or frequency of cash activity. For some it may be those alerts that result from international wire transfers to or from high-risk countries. For others it may be alerts emanating from high-risk customers such as politically exposed persons or international charities.

Written Procedures

The analysis process described here must be incorporated into written procedures that describe in detail *what* a monitoring analyst does as well as *how* it is done.

Procedures tell specifically what an analyst is to look for and what specifically they are to do with it. For example, a procedure describing how to identify potentially suspicious cash activity would say to look for "two or more deposits between $7,000 and $10,000 in cash or cash equivalents over two or more days" or, to look for "The aggregation of cash deposits over a 30 day period exceeding $25,000."

A procedure should also explain *how* to analyze such activity. For instance, "the analyst should retrieve cash reports for this customer for a period of 30 days prior to the activity to determine if similar patterns were present." Also, "the analyst should review the cash report to determine if the cash deposit occurred at the same or different branches. If it occurred at a different branch, the analyst should determine if the same or similar activity occurred within 30 days of the activity that generated the alert."

Well written procedures maintain consistency, reduce the amount of time it takes to train new employees and most importantly decreases the risk of non-compliance. It is also a reality that maintaining accurate and complete written procedures is challenging. As new systems are added, new monitoring methods introduced and as analysts learn how better to perform, updating procedures often get lost in the mix until a few weeks before an audit or exam, at which point a mad scramble can ensue to revise them.

Learn From Analysis

AML professionals understand the risks and challenges presented by systems that may produce too many alerts. However, it's the results of the analysis of those alerts that should then be used to better "tune" or "calibrate" monitoring tools.

A simplistic example would be to determine the percentage of alerts designed to detect potential structuring and examine which were more likely to end up being referred for further investigation and those that were resolved quickly. In many instances examination of the results may reveal that thresholds for determining potential "structuring" should be modified.

For example, perhaps an institution's methodology for detecting "structuring" includes cash transactions between $5,000 - $10,000, but results show that the benefit of including transaction between $5,000 - $7,000 is of little value. Conversely, examination of the results of alert dispositions may also show thresholds are too narrowly set, or the review may show the bank's thresholds are right where they need to be.

Institutions must find useful ways to apply what they learn from analysis of transactions, including devising ways to create prioritization processes to ensure alerts posing greater risk are resolved first and consideration should be given to incorporating the results of alert analysis into the enterprise BSA/AML risk assessment.

Summary

Detection of potentially suspicious activity is the foundation of an AML compliance program. Monitoring systems remain imperfect but necessary tools. By implementing a well-designed approach to the analysis process, institutions will be better able to manage large workloads, make sound decisions and maintain overall compliance with applicable rules and regulations.