SPIN CYCLE™

July 18, 2012

In this issue

Why AML Compliance Programs Fail – Part II

By David B. Caruso, CEO

Anti-money laundering transaction monitoring software is a necessary component of a compliance program. Unfortunately, these applications create unending hours of work that distract from compliance, or, in the worst cases, cause AML failures.

Second in a series.

The Typical AML Monitoring Analyst

Transaction monitoring software applications are costly, do not produce what is promised, and create untold hours of wasted time as staff sifts through "false positives" or low value alerts.

And yet, these systems are necessary for institutions to pass regulatory examinations.

No AML compliance issues generate more frustration, more cost, and more risk than those caused by transaction monitoring software.

AML Monitoring Systems Can Cause AML Failures

The Wachovia and HSBC enforcement actions show that the piles of work created by ineffective monitoring systems are often the root of major AML compliance failures. The same situation existed at Washington Mutual in that bank's waning days. Listen to AML directors from institutions of all sizes and you will hear their frustration with the constant struggle to handle a monthly deluge of low value alerts.

The dozen or so monitoring systems used today all produce volumes of low value alerts. Replacing one system with another that does basically the same thing is costly and likely has little benefit. Until a dramatically different software solution emerges, the best way to improve a monitoring program is by optimizing or "tuning" your current system to better detect suspicious activity and to reduce the number of low value alerts.

In our first Spin Cycle article in this series, we said the most important element of AML compliance was the identification, investigation and reporting of suspicious activity. Get that right and institutions will avoid the most serious consequences. Get it wrong and be prepared for harsh penalties.

Improving AML Monitoring Systems Through Tuning

The first step to ensure an institution properly reports suspicious activity is to detect it. To better detect suspicious activity, monitoring systems must be frequently "tuned."

Transaction monitoring software applications use "rules," "models," or "scenarios" that seek to flag potentially suspicious transactions while ignoring ordinary or expected activity.

Unfortunately the vast majority of transactions flagged are in fact ordinary, creating mountains of work for AML departments and hampering compliance.

The process to improve or tune these systems usually falls onto the AML department. Tuning strives to optimize thresholds, rules, and scenarios to better identify potentially suspicious activity and to ignore benign transactions.

Tuning combines statistical analysis, knowledge of how money is laundered, and sound judgment to craft better detection scenarios. Some key things to consider when tuning a monitoring system include:

- Not every type of transaction needs to be monitored through a vendor software application. Often institutions, using basic programming, develop better monitoring processes themselves.

- Data completeness. Perform data validation to ensure all transactions that should be monitored are in fact being processed by the monitoring system. No matter how well a system detects suspicious cash activity, missing ACH transactions means you won't pass an exam.
- The purpose of AML compliance is to file SARs. It is tempting to deploy scenarios to detect activity that sounds interesting, or is the AML issue de jour, but if these scenarios never yield a SAR, modify or retire them.
- Tuning is not something done once a year. Tune your monitoring system each month or at least each quarter.

When tuning, consider these points:

- Examine non-transactional variables: Transaction volumes and values are the most common variables to alter when tuning. However, these variables may not always be those that are best at identifying suspicious activity. Analyzing SARs filed from the scenario being tuned may reveal what is most meaningful is not transactional - it may have more to do with the duration of a customer relationship or the location of the activity.
- Micro-target scenarios: Every unit knows the frustration of seeing the same customer alert every month for normal or expected activity. Units are reluctant to suppress alerts for fear of missing something. So consider applying a subset of more narrow thresholds to these repeat customers that will identify their truly suspicious activity but not alter the thresholds and scenarios applied to the general population of customers.
- Change time line: Instead of a scenario looking at monthly activity, extend the period monitored to quarterly or semi-annually. Stored value cards and loans are products that lend themselves to longer review periods.

Once systems are better tuned the number of low value or false positive alerts should decline. Then comes the hard part - proper analysis and documentation of your work. In the next Spin Cycle we will discuss how to do that so as to avoid AML compliance failure.