AML Topics
Using analytics to get the most from your transaction monitoring system

March 2011
Contents

Components of the AML Compliance Program ................................................................. 1
Transaction Monitoring ................................................................................................... 1
Transaction Monitoring Performance Enhancement ......................................................... 2
   Structure of Performance Enhancement Efforts .......................................................... 3
   Determining the Approach ......................................................................................... 4
Conclusion ..................................................................................................................... 5
Contacts
Components of the AML Compliance Program

Through a bounty of legislation — such as the Bank Secrecy Act, the Money Laundering Control Act, the USA PATRIOT Act as well as associated supplemental legislation — financial institutions must identify and report customer money laundering activity, or face stiff penalties. As one of the regulatory bodies responsible for enforcing Anti-Money Laundering (AML) regulations, the Office of the comptroller of the currency has determined that any national bank subject to its oversight is required to “educate its employees, understand its customers and their businesses, and have systems and procedures in place to distinguish routine transactions from ones that rise to the level of suspicious activity” (Comptroller’s Handbook, September 2000). In the last two years alone, fines, civil penalties, and asset forfeitures for money laundering violations have frequently run into the tens of millions of dollars.

According to the Comptroller’s Handbook, to fulfill the requirements to “understand...customers and their businesses” and to “have systems and procedures in place to distinguish...suspicious activity,” most AML programs use a combination of two components:

- **An onboarding process** is used for new customers and involves due diligence investigation, initial verification of identity, comparison to lists of known entities, and risk assessment, and may involve profiling of potential client activity to aid in future monitoring. This initial onboarding process is generally referred to as the Know Your Customer (KYC) component of monitoring, although that term is used more broadly in certain contexts to include aspects of an ongoing monitoring process, as well.

- **An ongoing monitoring process** is used to assess activity for all customers, with emphasis on customers and activity with the highest risk. The ongoing monitoring process is used to identify suspicious activity that may ultimately result in the filing of a Suspicious Activity Report (SAR). Aspects of KYC may inform ongoing monitoring, such as risk assessment and client profiling, and those may in turn be informed by ongoing monitoring.

- When supplemented with appropriate employee training, compliance oversight, internal controls, and independent testing, these two components form the heart of the complete AML compliance program. **And while the components work hand in hand, in this paper we’ll focus primarily on how to improve the ongoing transaction monitoring process.**

Transaction Monitoring

The purpose of AML transaction monitoring is to provide ongoing identification of suspicious activity from customer transaction data. It is generally a two-stage process whereby first, instances of potentially suspicious behavior are identified or “flagged,” and then these instances of potentially suspicious behavior are reviewed by an analyst to determine if, ultimately, a SAR should be filed.

To identify potentially suspicious behavior, most large institutions have implemented an automated AML transaction monitoring system — either a proprietary application or an application from one of many AML software vendors. The monitoring system is fed transaction data from multiple internal and external data sources. It filters, compiles, and summarizes transaction data, and “flags” instances of potentially suspicious behavior.
behavior (called “cases”, “flags”, or “alerts”). Flagging is accomplished by implementation of AML “scenarios” that fall into two broad categories:

- **Rules-based scenarios** identify specific patterns of behavior by comparing transactional activity to algorithms that mimic known AML behavior patterns.
- **Statistical profiling scenarios** identify unusual activity by modeling norms of client activity or segment activity over time and identifying outliers as potentially suspicious.

Some AML monitoring systems provide the ability to apply mostly or all rules-based scenarios, some provide the ability to apply mostly statistical profiling scenarios, and yet others offer multiple scenarios of both types. Regardless of the type of scenario, the values for a number of “parameters” or “thresholds” determine which activity gets flagged for review. These parameter values are typically customizable for each application.

In the second stage of transaction monitoring (after activity has been flagged), cases are reviewed by AML analysts who investigate the activity using internal and external information sources, including, for example, transaction and party information, watch lists of known or suspected money launderers, and lists of trusted entities. The case is either cleared or escalated, potentially to the point where a SAR is filed, and client profile and risk information may be updated if necessary.

Quantitative analytics can be used to enhance the first stage of transaction monitoring by improving the ability of the automated system to efficiently and effectively identify suspicious behavior.

### Transaction Monitoring Performance Enhancement

Examiners conduct periodic examinations of AML compliance programs, prioritizing programs for review based on risk factors and law enforcement leads. When reviewing transaction monitoring, examiners aim to determine the adequacy of the monitoring system, to evaluate the reasonability of changes made to the system and policies, and to assess the adequacy of bank efforts to ensure ongoing effectiveness and integrity.

For this reason, it is important for banks to have a program in place to continually assess the performance of the Transaction Monitoring process and apply corrective action to address deficiencies. Generally speaking, performance can be evaluated in two ways.

- **Effectiveness** is the ability to properly identify suspicious activity that exists, or to minimize the number of “false negatives.” (False negatives are instances of suspicious activity that are not identified by the existing monitoring program.) The risk mitigated by improving effectiveness is compliance risk — the risk of failing to identify actual AML activity. Improving effectiveness is the bank’s obligation in order to be compliant with regulations, meet legal obligations, and protect its reputation.

- **Efficiency** is the ability to properly identify non-suspicious activity, or to minimize the number of “false positives.” (False positives are instances of benign activity improperly identified as suspicious.) The risk mitigated by improving efficiency is business risk — the risk of improperly allocating resources to review cases of non-suspicious activity. Improving efficiency allows the bank to keep costs down without increasing the risk of non-compliance.

When implementing a performance enhancement effort, banks should consider these common characteristics of successful efforts to address compliance requirements and improve effectiveness and efficiency:
• **Empirical** – Assessments of the effectiveness and efficiency of the AML monitoring program are based on observation of available data, mostly from files of transactional activity and case review outcomes. Assessments rely on expert opinion or management judgment only where necessary.

• **Proven** – Techniques that are common and accepted methods of statistical and quantitative analysis are leveraged to assess the effectiveness and efficiency of AML monitoring programs. Experimental or obscure techniques may have some intrinsic value, but their use may complicate proving the validity of enhancement efforts to examiners. Coherent communication of results to examiners is made more difficult if overly complicated or uncommon techniques are used.

• **Repeatable** – The performance enhancement process is conducted and documented in a way that sufficient evidence is retained for examiners to be comfortable that procedures were implemented correctly and in a way that facilitates re-performance. The documentation should be developed and maintained so that a knowledgeable third party could replicate the approach with limited additional information.

• **Independent** – The performance enhancement process is conducted by an entity independent from the internal functions that are responsible for ongoing monitoring. While personnel responsible for ongoing operation of the transaction monitoring system are likely to be leveraged for the performance enhancement effort, they are not key contributors to the assessment process.

• **Sustainable** – To the extent possible, the performance enhancement process is consistent enterprise-wide and requires a level of effort that is reasonable given the size of the institution and the risks associated with non-compliance.

**Structure of Performance Enhancement Efforts**

Successful performance enhancement efforts are structured around a core set of performance-related questions.

**Are there important patterns of suspicious behavior that the system is not monitoring?**

Transaction monitoring systems generally employ a finite number of scenarios, each of which represents established patterns or types of suspicious behavior. An instance of suspicious activity is flagged when the actual transaction data is similar to the established pattern or type. If a particular type of behavior that represents suspicious activity is not being monitored, the bank will undoubtedly fail to identify it within the current system. This flaw could be resolved by adding a scenario to the monitoring system. Many AML software programs are flexible enough that they provide the ability to create custom-made scenarios in addition to the core offerings. Performing a periodic, detailed, expert review of a sample of customer transaction data can help to identify risky patterns and types of behavior that are not being monitored.

**Where are scenario parameter values set relative to the overall population of transactions?**

Whether scenarios are rule based or profile based, they typically use customizable parameters that define the population of cases that is ultimately flagged for review. A comparison of the parameter value settings to the population of interest can provide a baseline from which to evaluate shifts in the population that, over time may affect monitoring performance. It may also highlight instances where parameter settings do not currently allow for appropriate monitoring of the population. (i.e., parameter settings are too high or too low given the population distribution). This is especially important for certain profile-based scenarios that rely on a methodology of outlier identification.

**Does the current set of monitoring scenarios identify all relevant suspicious activity?**

To minimize the risk of not identifying suspicious activity, parameter values need to be set at a level that allows for wide enough coverage of the transaction population. Sensitivity testing of parameter values can facilitate assessment of current parameter settings and identify adjustments that may be necessary to capture additional suspicious activity. This can be accomplished by adjusting parameters and applying scenarios either in a dual production environment or by creating an emulation of the production monitoring system and processing historical data. In either event, a statistical sample can be selected from the residual population of cases and reviewed to determine if suspicious activity was missed by using the current settings. If reviews show that suspicious activity is being missed, a risk-based evaluation can be performed to determine whether the increased work effort to capture these activities is worth the mitigation of ongoing risk.

---

2 Shifts in the underlying population could be the result of many factors, including, but not limited to segmentation changes and M&A activity.
Are resources being appropriately allocated to the identification of suspicious activity?
Using statistical techniques to compare cases that are deemed suspicious after review with those that are not can help identify whether parameter settings can be adjusted to reduce the number of cases reviewed. For example, multivariate risk scoring models can be developed using historical transaction and account data to differentiate between suspicious and non-suspicious cases. When fewer cases are flagged for review, a cost savings is associated with the reduction in resources dedicated to case reviews. Focusing investigations on high-risk activities can improve staff productivity with fewer false positives.

A performance enhancement program that addresses all four questions might include the following components:

- **Missing behavior identification:**
  - **What it is** – A review of a random sample of transactional activity
  - **Why it is done** – To identify additional types of potentially suspicious behavior not specifically targeted by current scenarios and reports

- **Distributional analysis:**
  - **What it is** – A comparison of the current parameter settings to the actual distribution of transactions
  - **Why it is done** – To determine a baseline for future assessment of changes in transactional behavior

- **Threshold sensitivity analysis:**
  - **What it is** – “Casting the net wider” by generating additional cases for review using adjusted parameters
  - **Why it is done** – To determine the effectiveness of current parameter settings at identifying potentially suspicious behavior. This tests whether the current parameter settings fail to identify any potentially suspicious behavior.

- **Threshold efficiency analysis:**
  - **What it is** – A comparison of cases deemed suspicious after review with those that are not using statistical tests, graphical analysis, and risk scoring models
  - **Why it is done** – To determine if current parameter settings can be adjusted to increase efficiency by reducing the number of false positives

**Determining the Approach**
The particular approach to performance enhancement and the appropriate combination of techniques should be determined by the circumstances in which it is being conducted. For example, circumstances may include specific regulatory examination requirements, business changes and other internal control triggers, an ongoing performance enhancement schedule, or a new system or platform implementation (see below). The approach might also need to be modified if all historical data necessary for analyses is not readily available — going forward, it is likely that data retention policies will require modification in order to facilitate a robust program.

As noted above, a new system or platform implementation requires selection of scenarios and initial parameter settings. The appropriate approach to implementation depends on risk and level-of-effort considerations. It may be appropriate to choose scenarios and initial parameter settings based on a line of business with a similar customer base where the same monitoring system has already been implemented. Another approach is to perform statistical analysis of the distribution of transaction data and set parameter values based on predetermined points in the distribution. A third approach is to stage the system for a predetermined time prior to official implementation and evaluate the ability of initial settings to differentiate between suspicious and benign activity. This approach requires cases to be flagged and reviewed as part of implementation. Whatever
the approach, it is important to assess and enhance performance of the system once it has been in place for a period long enough to produce a substantial number of cases.

The level of effort required when migrating from legacy systems depends on the level of similarity between old and new systems in the same line of business, ongoing performance enhancement efforts, level of AML risk in the particular line of business, and availability of staff with the appropriate technical skill sets.

Changes to the business through mergers and acquisitions or sales require re-assessment of scenario selection and parameter settings to ensure that the new population is being monitored appropriately. If ongoing assessment of parameter settings relative to population values has been conducted, this information is useful to determine the likely effect of business changes in a short period of time.

Ongoing performance enhancement may ultimately require the use of many different techniques — some multiple times, but not at the same intervals. For instance, it may be appropriate to conduct monthly or quarterly assessments of where the parameters are set relative to the population of transactions, since this is not typically a costly exercise once the initial analysis has been conducted. The results of these assessments can be used as triggers for additional assessment techniques, such as sensitivity testing of parameter values.

**Conclusion**

Ultimately, the decision about the type and extent of transaction monitoring performance enhancement efforts depends on an evaluation of the compliance and business risks inherent in the monitoring system, regulatory and legal requirements, and available resources. Having a program in place that continually evaluates performance and incorporates triggers to identify areas of risk and procedures for mitigating risk will facilitate the examination process, proactively address areas of likely regulatory focus, and contribute to cost reduction. Key to this effort is having staff that is trained in implementing the various statistical techniques, as well as AML analysts that can assist in interpreting the results that are being generated from the performance enhancement efforts.
Contacts

Jeff Lavine
703 918 1379
jeff.lavine@us.pwc.com

Catherine Stahlmann
305 375 6345
catherine.l.stahlmann@us.pwc.com

Monique Maranto
410 404 1905
monique.maranto@us.pwc.com