

ABA

Bank Compliance

NOV | DEC 2007

Gov

GOVERNANCE

BY BROOKTON N. BEHM, CAMS,
GREGORY B. HAHN, AND BRIAN J. KLOOSTRA

Driving Down the Costs of Transaction Monitoring

IN RECENT YEARS, financial institutions have become subject to increasingly rigorous anti-money laundering and Bank Secrecy Act (AML/BSA) rules and regulations. Regulators show no signs of easing the pressure; if anything, it appears to be on the rise.

Most financial institutions have concentrated on advancing their compliance programs to keep up with growing regulator expectations. The cost of compliance continues to climb dramatically, and few financial institutions can focus on optimizing their processes.

Much of this cost stems from retaining many skilled employees to monitor transactions. Reviewing alerts for suspicious activities and investigating high-risk customers are labor-intensive tasks. Fortunately, technology is creating the opportunity to reduce these costs without sacrificing quality.

Transaction Monitoring Challenges

Financial institutions of every size and risk profile have an increased need for resources to resolve potentially suspicious alerts that arise during transaction monitoring. Proper monitoring involves the examination of transactions running through a bank.

These transactions are typically filtered through various rules-based filters to generate specific alerts that flag potentially suspicious transactions. When these alerts are generated, an analyst must adhere to the bank's written procedures for reviewing and handling each one.

This review typically entails analyzing each flagged transaction to determine what caused the alert, using the bank's know your customer (KYC) data to understand the customer's expected activity, and then deciding whether the flagged activity is suspicious. Each of these steps must be clearly documented so that an examiner can retrace the banks' steps and review its decision-making process.

Transaction monitoring is not optional. To comply with legal requirements related to filing suspicious activity reports (SARs), banks have invested heavily in their monitoring systems. In turn, this has exponentially multiplied the number of AML red flags banks produce.

To keep up, financial institutions have expanded the number of employees dedicated to AML/BSA compliance. This compliance takes

a disproportionate percentage of banks' resources. It requires the addition of more support, such as hiring new employees, transferring staff, or obtaining external assistance.

Having the right number of personnel is not enough. Banks need to train them to investigate complex money-laundering schemes.

In several past instances, financial institutions have implemented transaction monitoring systems with minimal optimization only to find that they are producing so many alerts that a backlog prevents the bank from properly resolving each one in a timely manner.

Additionally, regulatory pressure for banks' broader scope of services has led to the ongoing increase in new scenarios, capabilities, and methodologies to capture new types of suspicious transactions. Such procedures lead to higher alert volumes, resulting in more resource allocation.

Does this mean that banks will see their transaction monitoring costs continue to skyrocket? Institutions are increasingly focused on two areas to reduce the cost of their monitoring programs:

- increasing the effectiveness of processes that generate alerts by minimizing the number of false positives;
- boosting the number of efficient ways to review and evaluate the alerts that are generated.

Through technology, a bank can generate fewer alerts and decrease the amount of time required to review and investigate each one.

Increasing Effectiveness

Many financial institutions have developed and implemented technology to monitor their transactions, but few have optimized these systems to their full potential. The looming threat of enforcement actions has prompted many banks to rush to demonstrate their progress in transaction monitoring.

But some banks' need for speedy implementation has clashed with the goal of developing an optimal end product. Such banks could greatly benefit from "tuning" their processes for generating alerts. The tuning of alerts decreases the total number of red flags needing review by reducing the amount of false positive alerts—those that are not designated as suspicious.

Typically, alerts flag transactions that, based on the application of pre-established rules, are determined to be potentially suspicious for money laundering or terrorism financing. Depending on the configuration, a bank's alerts will arrive in batches—daily, weekly, and monthly—through a computerized alert review system or printout.

Unfortunately, the number of alerts that are ultimately deemed to indicate unusual activity is very low. Sometimes analysts review hundreds of alerts to yield one that is suspicious. In the United States, those are required to be reported to the Financial Crimes Enforcement Network (FinCEN) on SARs.

By minimizing the amount of time that is spent reviewing these false positive alerts, the bank improves the effectiveness of

its transaction monitoring program. In several past instances, financial institutions have implemented transaction monitoring systems with minimal optimization only to find that they are producing so many alerts that a backlog prevents the bank from properly resolving each one in a timely manner.

A bank, however, cannot simply adjust a monitoring system's alert generation settings at will. It must be able to provide regulators and auditors with supporting documentation and business justification for accommodating thresholds and parameters. To tune out false positives, a disciplined transaction tuning methodology must be implemented. This strict approach should include the following components:

- the use of sampling and clustering data to identify opportunities for threshold enhancements;
- a formal change management process for centralizing the tuning justification documentation and management approvals;
- controls in place to ensure that the tuning process is performed in a consistent, repeatable manner.

An organization's tuning methodology can be enhanced with supporting technology. Key benefits of applying such technology include ensuring the tuning procedure is repeatable and consistent and uses automated workflows to track and document each step; eliminating the error-prone manual steps of sampling and tracking results; and enhancing the audit trail by creating and maintaining the change control process and justification documentation.

Return on Investment

When transaction alerts are generated, the focus turns to how these alerts are investigated and dispositioned. Analyzing AML red flags is considered a resource-intensive activity that dramatically increases as alerts multiply. The extra labor derives primarily from false positives and the subsequent investigations.

The amount of time spent reviewing each individual alert varies greatly depending on the bank. Besides reducing the number of alerts, banks desire to improve the following common factors:

- the accuracy and timeliness of information around customers and accounts involved in the alert, including the availability of KYC data;
- the level of detail required by the financial institution's alert review procedures to constitute a completed review;
- the ability of analysts to determine and execute the appropriate course of action to arrive at a proper disposition for each alert based on its specific conditions;
- the structure of the financial intelligence unit.

Individual analysts conduct investigations by applying subjective criteria to determine whether the alert contains potentially suspicious activity. The steps followed often depend on the type of alert that is generated along with certain criteria. For example, a red flag triggered by a wire transaction to a high-risk country will likely undergo a different review process than a basic structuring alert.

Without the proper tools in place, the analyst determines which process steps to follow for each review. Too often, analysts end up researching too little, too much, or in the wrong areas. Additionally, the injection of subjectivity often necessitates a high

level of quality assurance review to ensure consistency, thereby boosting labor costs.

Financial institutions focused on containing the cost of alert reviews are increasingly turning toward implementing a structured approach that steers analysts to the correct process steps for the specific conditions of the alert. Such an approach automates the data collection used to make decisions.

Using the right technology, a bank can ensure that each alert review is consistent with internal standards, policies, and procedures—all while decreasing the amount of time the analyst spends working on the alert.

Additionally, tools are also capturing the results of each step and relaying a consistent narrative to explain the decision-making process behind each alert disposition. While an analyst still determines the final disposition, financial institutions using these technologies are driving down the labor and cost to review alerts, as well as enhancing their processes' quality and consistency.

Implementing a lean technology procedure for review alerts gives these banks more flexibility. For example, by using predefined rules, software tools can collect all of the alerts for a given customer and present an "enterprise alert."

Typically, alerts are queued for a time period and then coupled as one review, streamlining the process and eliminating the need to repeat common steps on multiple different alerts.

A Wise Investment

Transaction monitoring carries tremendous and growing costs for financial institutions, but the proactive use of available technologies can contain some of those costs and allow for greater flexibility in response to increasing regulator expectations. Investing in tools that enhance transaction monitoring systems by improving both the tuning and alert review processes is becoming commonplace.

These technologies are driving down the cost of monitoring transactions without compromising banks' extensive AML/BSA compliance obligations. BC

ABOUT THE AUTHORS

Brookton N. Behm is an executive with Crowe Chizek and Company LLC in Grand Rapids, Mich. Reach him at (616) 233-5566 or bbehm@crowechizek.com.

Gregory B. Hahn is an executive with Crowe Chizek and Company LLC in Grand Rapids, Mich. Reach him at (616) 752-4223 or ghahn@crowechizek.com.

Brian J. Kloostra is an executive with Crowe Chizek and Company LLC in Grand Rapids, Mich. Reach him at (616) 752-4219 or bkloostra@crowechizek.com.