

BY PAUL R. OSBORNE, CPA, CPO, AMLP, AND JEFFREY A. JONES, CAMS

Transaction Monitoring: Where to Start?

CONSIDER THE FOLLOWING: Your bank examiner or bank management has strongly recommended that you purchase an automated system to monitor your customer transactions for suspicious money-laundering activity. You're thinking now that all of your institution's problems will be solved. However, these systems are complicated and are often designed to be tailored to the specific customer behavior of each bank. More than just a set of reports, they usually filter activity against a set of rules that the bank determines. Authors Paul Osborne and Jeffrey Jones discuss where to start when it comes to monitoring customer transactions for money-laundering activity.

and automated clearing house (ACH) transactions that were once used for smaller, low-risk, recurring amounts—have also been classified as high-risk because they move money quickly, in large amounts, and often with hidden identities and worldwide geographic locations.

In order to conduct a more comprehensive investigation, less-risky transactions like checks and customer-initiated transfers between accounts are also important and should be monitored to develop a foundation and general understanding of a customer's typical transaction behavior.

Historical or typical behavior is important to determine because it acts as a benchmark for setting thresholds for flagging transactions and plays a key role in minimizing the number of false-positive alerts that are generated by broad-based rules not centered on actual risk characteristics.

Timing Is a Factor

Suspicious activity can be the result of a one-time occurrence or a series of transactions occurring over a period of time that establish a pattern of unusual or unexplainable behavior. Rules that detect a variety of transaction types and multiple timing schemes need to be established. Some rules should look at customer behavior in time periods of less than one week; others should look at daily activity. And still other rules should yield no results until longer periods of time have elapsed and patterns have been established.

To avoid bank reporting or record-keeping requirements, fraudulent transactions often are split up over time, which is referred to as structur-

and divides customers into business and personal accounts. Is this enough? The answer is probably no.

As the FFIEC guidelines indicate, "The type and frequency of reviews and resulting reports used should be commensurate with the bank's BSA/AML risk profile and appropriately cover its high-risk products, services, customers, entities, and geographic locations."² At a minimum, this means adding monitoring for frequent and high-dollar transactions, significant balance changes, spikes in activity, and transactions with common originators and beneficiaries. Anything that is out of the ordinary for a particular customer peer group should be looked at more closely. Unusual behavior generally leads to investigating further transactions that are not consistent with the stated business purpose or occupation or with the source of income or geographic location in which the customer operates.

Look at All Risks

Depending on the results of the risk assessment, monitoring should include transaction activities other than cash, wires, and monetary instruments. Recently, electronically conducted transactions—including ATM



Start With Risk Assessment

As with any other part of a Bank Secrecy Act (BSA) and anti-money laundering (AML) program, a risk assessment is the starting point. The Federal Financial Institutions Examinations Council (FFIEC) examination manual states, "The level of monitoring should be dictated by the bank's assessment of risk, with particular emphasis on high-risk products, services, customers, entities, and geographic locations."¹ A transaction monitoring system might already come with a set of default rules that are typical of money-laundering activities and generally common to all banks. These would include cash structuring, transaction layering, "smurfing," and round dollar amounts. Typically, this basic monitoring focuses on cash and wire activity

Certainly you can use the expertise built into automated tools as a guide, but you still must demonstrate that you understand how to use the tools to get the best results for your bank.

ing (staying just below the reporting threshold for currency transaction reporting). Because structured transactions can be made within a short time of each other or over longer periods, both time periods should be monitored. Timing is also a risk factor when considering the movement of money. Money can be moved between accounts quickly in order to hide or cause confusion regarding the criminal intent.

How to Fill Gaps

Customer deposit accounts tend to be the most active class of accounts and make up the majority of customer activity. These accounts are rich in transaction activity and are a good source for customer behavior monitoring. What is missing is the monitoring of other types of activity, including commercial loans, mortgage loans, installment loans, credit cards, home equity loans, trust accounts, brokerage accounts, and insurance policies. These various lines of business often stand alone as subsidiaries and might not be easily integrated with other transaction monitoring. But they could contain unusual activity that represents criminal intent to hide or launder funds.

What do you do when your system does not have the capacity to monitor certain activities? The answer lies in developing alternative monitoring methods that will alert investigators to suspicious accounts based on the FFIEC red flags. For example, loan account monitoring may include reviewing loans secured by certificates of deposit with an unknown source of funds; loans paid off early in cash or by unknown third parties; payments in excess of the loan balance; or loans secured by unrelated parties.

Monitoring insurance policy purchases might involve flagging cash payments for policies with large pre-

miums, purchases of policies outside a customer's range of wealth, policy terminations without concern for penalties, or policy loans payable to unknown parties.

Too Small?

What if your bank is not big enough to warrant an automated system for transaction monitoring? The FFIEC guidelines state that "the level of sophistication of the internal controls should be commensurate with the size, structure, risks, and complexity of the bank."³ This guidance makes it difficult to determine what needs to be monitored. In this situation, the appropriate course of action would be to follow the FFIEC recommendations in light of your bank's identified risks. Following the FFIEC guidelines entails manually reviewing periodic reports generated by the bank's core accounting systems, including the following:

Currency Activity Reports

- Transactions greater than \$10,000
- Multiple transactions between \$7,000 and \$10,000
- Multiple transactions of small dollar amounts that aggregate to a substantial amount
- Transactions aggregated by customer name, tax identification number, or customer number

Funds Transfer Records

- Amounts of \$3,000 and above
- Funds transfers of large dollar amounts (varies by customer profile)
- Transfers involving high-risk countries
- Funds transfers by noncustomers

Monetary instrument Records

- Cash purchase of monetary instruments between \$3,000 and \$10,000
- Frequent purchasers
- Common payees

As your bank's risks change (as a result of acquiring additional customers, product and service offerings, or locations), the risk assessment might change, and you likely will need to expand, revise, or discontinue a portion of your transaction monitoring program. New reports and even the purchase of an automated system should be considered as the bank's risks grow or change.

Document, Explain, Review

Whether you are using manual reports to monitor suspicious activity or a sophisticated automated system to uncover unusual activity, you need to be able to explain to regulators what you are monitoring and why. Taking an approach based on the risks identified by the risk assessment is the best way to demonstrate that you understand your regulatory responsibilities and obligations to report suspicious customer activities to government agencies or law enforcement.

Certainly you can use the expertise built into automated tools as a guide, but you still must demonstrate that you understand how to use the tools to get the best results for your bank. The decisions made should be your own. **BC**

ABOUT THE AUTHORS

Paul Osborne is an executive with Crowe Horwath LLP in the Indianapolis office. He can be reached at (317) 706-2601 or paul.osborne@crowehorwath.com.

Jeff Jones is a senior manager with Crowe Horwath LLP in the Grand Rapids, Mich., office. He can be reached at (616) 752-4295 or jeffrey.jones@crowehorwath.com.

Endnotes

¹www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_015.htm.

²*Ibid.*

³www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_007.htm.