Bloomberg BNA

Securities Regulation & Law Report™

BROKER-DEALERS

Broker-Dealer AML Transaction Monitoring: The Devil's in the Details

BY DANIEL NATHAN AND ALMA ANGOTTI

Broker-dealers often face a significant challenge monitoring transactions for possible money laundering or other suspicious activity, especially given the volume of transactions they handle. Clearing firms, which often handle a substantially higher trading volume, have an even bigger challenge. Clearing firms are also expected to provide monitoring resources such as reports of wire activity, journals of funds and securities, and other transaction activity, to their introducing brokers so they can comply with their own reporting responsibilities.[1]

[1] While introducing and clearing brokers each have an independent responsibility to identify and report suspicious transactions, they may allocate monitoring responsibilities between them. FIN 2008-G002 (March 4, 2008). *See also*, NASD NTM 02-21 at 4, 11.

Daniel Nathan is a partner at Morrison & Foerster LLP and, until recently, was Vice President and Director of Regional Enforcement in the FINRA Department of Enforcement. Alma Angotti is a Director with Navigant Consulting Inc., and previously held senior enforcement positions at FINRA, the Financial Crimes Enforcement Network and the SEC.

While an automated system can dramatically improve the efficiency and effectiveness of transaction monitoring, some firms have been slow to adopt effective automated systems. Since the time when broker-dealers were first required to implement anti-money laundering (''AML'') compliance programs in 2002, the available technology for transaction monitoring has evolved, and, as with any technology, the costs have decreased. There is as yet no black-letter law requiring any firm to adopt automated transaction monitoring. But regulatory expectations for identifying and reporting suspicious transactions would make it difficult for firms with large transaction volume to take the position that a manual review system, or limited reliance on automated systems, is reasonable in view the nature and size of those firms' businesses without a large number of staff analyzing the transactions.

A precedent set by a litigated decision in a case brought by the Financial Industry Regulatory Authority's (''FINRA's'')[2] Department of Enforcement declared that a clearing firm's AML monitoring system could be effective in the absence of automation. As discussed below, the decision in that disciplinary proceeding, that accepted Sterne, Agee & Leach, Inc.'s failure to adopt an automated system, could be seen as a product of its time. The AML procedures at issue in that case are now at least seven years old.[3] In view of the technological advances and decreased cost of available systems since that decision, and enforcement actions taken by the Financial Crimes enforcement Network (''FinCEN'') and the federal banking regulators, it would be difficult today for a firm with substantial transaction volume to claim that it is reasonable to rely on a largely manual system to identify and report suspicious transactions.

[2] FINRA is the largest independent regulator for all securities firms doing business in the United States and has primary responsibility for anti-money laundering compliance for broker-dealers. All told, FINRA oversees nearly 4,435 brokerage firms, about 161,450 branch offices and approximately 630,155 registered securities representatives.

[3] *Department of Enforcement v. Sterne, Agee & Leach*, FINRA Disciplinary Proceeding No. E052005007501.

 ISSN 0037-0665

However, ultimately there is no firmly-prescribed system that firms must adopt; rather, regulators have articulated a set of principles that firms should consider in choosing the most effective system for their business models.

I. The Applicable Law and Guidance

The Bank Secrecy Act and implementing regulations[4] include a variety of provisions to require U.S. financial institutions to take steps to prevent and detect money laundering and terrorist financing. Under the BSA, financial institutions including banks and broker-dealers [5] must establish and implement anti-money laundering programs.[6] Each compliance program must, at a minimum, include what the federal banking regulators refer to as ''the Four Pillars'' of BSA compliance:

1. Written policies procedures and internal controls to assure compliance;
2. An individual responsible for managing day to day compliance;
3. Independent testing for compliance by either internal or external personnel; and
4. Ongoing training for employees.[7]

While FinCEN and banking regulatory actions are not precedent for FINRA and U.S. Securities and Exchange Commission (''SEC'') actions against broker-dealers *per se*, they are instructive. As the administrator of the BSA, FinCEN has the guidance and policy authority to determine what constitutes a reasonable AML program, and can bring and has brought enforcement actions against many types of financial institutions, including broker-dealers, for inadequate programs.

A. *Suspicious Activity Reporting*

The BSA requires all covered financial institutions, including all FINRA member firms, to have AML programs that are reasonably designed to detect and report suspicious activity. The suspicious activity reporting requirement, like all AML program requirements, is to be ''risk-based'' and tailored to the firm's business. There is no ''one size fits all'' system that is right for every firm. Precedents set by FinCEN enforcement actions help define a reasonable system for identifying and reporting suspicious activity and the circumstances that make an automated system advisable, and provide insights into the pitfalls of failing to adopt an adequate system.

A broker dealer must report any transaction or pattern of transactions over $5,000 where the broker dealer ''knows, suspects or has reason to suspect'' the transaction involves virtually any violation of law or regulation.[8] There is no explicit requirement for firms to utilize automated transaction monitoring systems to detect and report suspicious transactions. But FINRA has provided guidance to clearing firms, in Notice to Members 02-21, that in order to ''assist introducing brokers and, more importantly to satisfy their own obligations under federal law, clearing firms should establish both automated systems to detect suspicious activity and procedures to share AML information and responsibilities with introducing brokers. . . .''

B. *Sterne Agee decision*

The March 5, 2010 decision by a FINRA Hearing Panel held that Sterne Agee's AML procedures from April 2002, when broker-dealers were first required to implement AML programs, through July 2005, were reasonably designed to achieve and monitor the firm's compliance with the BSA. FINRA staff had contended, among other things, that the clearing firm could not adequately detect suspicious activity because the firm's AML compliance system was insufficiently automated.[9] The Hearing Panel disagreed, finding that the firm's program was reasonable. The Panel stated that while it is likely that an automated system would have identified patterns that would not have been picked up by a manual review, the staff had not demonstrated that during the period of time at issue there was proven, reliable software available for broker-dealers. Given that the requirement for firms to have AML procedures was new, and systems were not necessarily reliable, the Court held that Sterne Agee's system was not inherently unreasonable.

Firms with significant trading volume should not rely too heavily on *Sterne Agee*. The Hearing Panel specifically stated in a footnote that it ''makes no finding with respect to the level of automation that might be required in 2010,'' and noted that AML procedures, enforcement, and technology had continued to evolve since AML procedures first became required for the securities industry.[10] Given the advances in technology and increasing regulatory expectations in the area of transaction monitoring, it is unlikely that the larger firms could successfully argue that manual monitoring is adequate to reasonably identify potentially suspicious transactions. In addition, most clearing firms typically offer a variety of reports that even the smallest broker-dealer can leverage to identify potentially reportable transactions without an investment in technology. Whatever system a firm chooses will require periodic evaluation and optimization to make sure that over time the program will continue to effectively identify potentially suspicious activity for analysis and reporting.

II. AML Compliance and Transaction Monitoring

While technology can be an important part of an AML compliance system, a good compliance program requires people, technology, and processes to work together. An effective AML compliance program starts with an assessment of the AML risks of each part of the business, each new and existing customer, and each type and volume of transaction. Once the risks are identified, the firm needs to ensure that its AML compliance program generally, as well as its monitoring system specifically, is tailored to those risks. In some areas of the firm's business, it might be more efficient and less

[4] 31 USC 5318 *et seq*. and 31 CFR 1000 *et seq., FINRA Rule 3310 (formerly NASD Rule 3011 and NYSE Rule 445)*.

[5] 31 USC 1023.210 and FINRA Rule 3310 (formerly NASD Rule 3011).

[6] 31 U.S.C.A. § 5318(h) (l) and 31 C.F.R. § 103.120.

[7] *See BSA and FFEIC Manual, Appendix R.*

[8] 31 CFR 1023.320 (a)(2).

[9] The Hearing Panel also rejected FINRA staff's claim that the firm's AML training program for those years was inadequate. FINRA staff also claimed that for a later period, July 2006 through April 2007, there were six additional specific deficiencies in the firm's AML program, and in its decision the Hearing Panel agreed with certain of those allegations and fined the firm $40,000.

[10] *Sterne, Agee*, *supra*, fn 28.

  SRLR ISSN 0037-0665

expensive to review transactions mechanically rather than manually. The firm must have adequate staff to review potentially suspicious transactions and train employees appropriately. The AML compliance program should include a periodic review of staffing levels, the risk assessments and the monitoring thresholds, to ensure that the volume and type of transactions that were the basis for the design of the transaction monitoring system have not materially changed. Periodic evaluation of thresholds will also improve the efficiency of the system to detect potentially suspicious transactions.

A. *Risk Ranking*

The starting point for any good system for monitoring transactions is an understanding of the risks presented by the firm's particular business model and mix of customers. A firm needs to tailor its procedures and systems to its business.[11] More specifically, the firm needs to identify appropriate red flags related to the firm's business model and customer base, or otherwise provide measures to manage the heightened risk of illicit activity present in the business.[12] This means identifying operations, such as products, services, customers, entities and geographic locations that are more vulnerable to abuse by money launderers and criminals and monitoring accordingly.[13]

A firm should ''risk rank'' the areas of its operations and its customers. Recent cases have criticized not only firms' failures to conduct due diligence with respect to particular customers and transactions,[14] but the failure to risk rank customers based on that due diligence when they first open accounts and to refresh periodically thereafter. For example, FinCEN sanctioned Pinnacle Capital Markets, LL, a broker-dealer, for violating the BSA by failing to tailor its procedures to its business and known risks.[15] Specifically, FinCEN charged that Pinnacle failed to conduct a BSA/AML risk assessment to evaluate and distinguish correspondent accounts with heightened BSA/AML risks, including accounts from countries in regions that had been classified by the International Narcotics Control Strategy (''INCSR'') as ''Jurisdictions of Primary Concern'' or ''Jurisdictions of Concern'' known for heightened money laundering risk.[16] FinCEN found that Pinnacle violated the BSA because it failed to identify the risks, implement risk-based monitoring for suspicious activity, and review transactions originating from these customers.[17]

In addition, broker-dealers should pay special attention to high-risk customers, products and services. Regulators have also found transaction monitoring systems to be inadequate when the firms have not refreshed the due diligence for high-risk customers. In a recent cease-and desist action, the Office of the Comptroller of the Currency found that Citibank, among other things, failed to develop adequate due diligence on high risk customers and failed to periodically review and refresh that due diligence.[18]

B. *Choosing a System*

Once a firm has considered its business model, and the risks created by the nature of its customers and transactions, it must decide what type of system is appropriate. All firms should implement a system that is adequate to detect unusual activity.[19] For smaller or lower risk firms, a largely manual system that leverages the comprehensive reports that many clearing firms provide could be effective. For the larger firms, an automated system might be indispensable. Not all potentially suspicious activity can be identified through transaction monitoring. A good suspicious activity reporting program will also include methods for identifying red flags that cannot be automated, such as employee referrals of suspicious customer behavior and suspicious account opening documentation or letters of authorization, in addition to appropriate manual and automated systems.[20] Employee training on what red flags they are likely to encounter and how to escalate those red flags is critical. The firm must have a sufficient number of appropriately trained analysts or compliance staff to review and evaluate the transactions identified by either type of monitoring system.

1. *The System Should Capture all Parts of the Business*

The monitoring system implemented by a broker-dealer should capture all the relevant transactions. FinCEN found that Eurobank's automated system was deficient because it failed to adequately capture numerous services provided by the Bank, including lending, trade financing, pouch activities, and check deposits, and did not monitor for suspicious activity based on customers' risk profiles, or the type and/or volume of customers' transactions.[21] Consequently, the bank relied predominantly on manual processes to monitor these transactions for suspicious activity. FinCEN found that the Bank's use of manual processes for suspicious activity monitoring was particularly inadequate given the Bank's customer base, geographic risk and business lines, as well as the volume, scope, and types of transactions conducted at the Bank.

FinCEN has also been concerned about the failure of some financial institutions' AML monitoring systems to obtain critical information on remote deposit capture deposits for compliance purposes. As a consequence, these firms might have failed to file suspicious activity reports (''SARs''). For example, in the Citibank order discussed above, the OCC found that the bank failed to file timely SARs on its remote deposit capture and international cash letter activity because of inadequate transaction monitoring systems.[22]

Similarly, in an enforcement action against a clearing firm, FINRA found that its automated systems failed to include some important high-risk products and ser-

[11] *In the Matter of Pinnacle Capital Markets, LLC*, FinCEN Case No. 2010-4 (Aug. 26, 2010)

[12] *Id.*

[13] FFIEC BSA/AML Examination Manual at 33; For a comprehensive, although not exclusive list of red flags for broker-dealers, *see* FINRA's AML Template for Small Firms, http://www.finra.org/Industry/Issues/AML/p006340.

[14] In addition, FinCEN recently issued an Advanced Notice of Proposed Rulemaking to announce that it is considering an explicit rule requiring financial institutions to perform customer due diligence and obtain beneficial ownership information. 77 Fed. Reg. No. 43 (March 5, 2012).

[15] *Pinnacle Capital Markets*, *supra*.

[16] *Id.*

[17] *Id*.

[18] *In the Matter of Citibank, NA*, Dept. of Treasury Consent Order #2012-052 (April 5, 2012).

[19] FFIEC Manual at 68.

[20] *Id*.

[21] *In the Matter of Eurobank, San Juan, Puerto Rico*, FinCEN Case No. 2010-02 (May 4, 2010)

[22] *Citibank, NA*, *supra*.

vices, such as check writing.[23] Broker-dealers that offer banking-type services such as checking accounts, also need to monitor those transactions to look for, for example, suspicious cash flows that cut across several lines of business

It is not enough for a firm to implement an automated system. Indeed, a firm that switches to an automated system from a manual system or another automated system that had been working effectively could be taking a step backwards if it does not adapt the new system to its business model. FinCEN found that when Eurobank replaced its old monitoring system in favor of a new one in November 2008, it failed to conduct appropriate system validation and parameters testing to ensure that the new system could adequately identify suspicious activity. Procedures established for the new system were neither risk-based nor tailored to the Bank's customer base, geographic risk, or business lines.[24]

2. *Threshold Levels Should be Appropriate*

Firms need to set the parameters for their review of transactions at an appropriate level based upon risk and the anticipated activity, and regularly reevaluate those parameters based upon actual experience with the customers. If the threshold is set so high that it misses a large number of potentially suspicious transactions, then the firm should consider lowering it to an appropriate level.[25] Similarly, if it is set so low that it generates a large percentage of alerts that after analysis involve normal or non-suspicious activity, it might be too low.

The transaction monitoring system should capture all accounts owned by the same customer, including those at correspondent and affiliated financial institutions, and monitor all types of activity conducted by a customer for trends and patterns, including wire transfers[26] and international money transfers.[27] For example, FinCEN brought an enforcement action in which it found that the bank's automated account monitoring system covered only 15 percent of the Bank's total accounts, those classified as ''high risk.'' As a result, more than 97,000 accounts were monitored manually, and that system, based on the scope, volume, and magnitude of transaction activity within the accounts, was not sufficient to ensure compliance with the BSA.[28]

The dictates of adequate transaction monitoring should determine the firm's resource needs, rather than the firm gearing the extent of its monitoring to its current level of staff and systems. A firm should not limit its devotion of resources to transaction monitoring when its risk assessment indicates the need for an improved system, lower monitoring thresholds or more personnel. FinCEN findings as to Wachovia National Bank Association are instructive. Confronted with alerts generated by the Bank's automated transaction monitoring system that were comprised of as many as 30,000 individual transactions, the bank routinely made the monitoring system manageable by increasing the threshold so that the number of alerts generated by the system with respect to international correspondent banks remained constant at around 300 each month. ''As a result, the Bank instituted arbitrary limits on the flagging and review of transactions for suspicious activity based solely on the inadequate number of staff available to review these alerts.''[29]

While there is no objective number of alerts that should be generated by any system, a very low number of alerts relative to the number of transactions may suggest that the firm has set the threshold too high, particularly if the firm's business involves higher risk customers, products or services. Indeed, in the Wachovia case, FinCEN found that although Wachovia conducted in excess of six million wire transfers for international correspondent bank customers per month, at times the monitoring system dedicated to those transactions generated as few as 80 alerts per month. Most of the foreign correspondent accounts did not generate any alerts and were not subject to detailed transaction review, despite the high-risk business profiles and geographies associated with many of the customers.

All set parameters and any changes made to them should be documented, with the rationale for them made clear. In Wachovia, FinCEN found that management failed to document or explain filtering criteria, thresholds, and how both were appropriate for the Bank's risks. In another case, FinCEN also found that the bank had failed to document or explain account filtering criteria or thresholds, and how both were appropriate for the Bank's risks.[30]

The proof of the adequacy of a firm's systems is in the pudding – in how many unusual transactions are identified, how they are processed, and whether SARs are filed appropriately. For that reason, while there is no right number of SARs that a particular institution should file, FinCEN decisions often look at the firm's overall rate of identifying transactions for review, and the number of SARs filed relative to the number of transactions overall. In a number of cases, FinCEN found that when a firm finally adjusted its review parameters, the number of suspicious transactions identified skyrocketed. In the Wachovia case, FinCEN found further support for the inadequacy of the threshold in that once the caps were removed from the Bank's transaction monitoring system, the system began to generate a higher and fluctuating number of alerts with respect to those types of transactions, and an increase in the number of suspicious transactions.[31]

The reviews work both ways and can also provide the basis for narrowing a firm's parameters or lowering its thresholds. For example, if a review of particular alerts

[23] *Department of Enforcement v. Penson Financial Services, Inc.*, FINRA Case No. 2008011615801 (December 14, 2009).

[24] *Eurobank*, *supra*.

[25] *See In the Matter of Pacific National Bank*, FinCEN Case No. 2011-5 (March 24, 1011) (''Pacific's dollar amount threshold for monitoring the two BPE correspondent bank accounts, set at $50,000 per day, was arbitrarily high. In those two accounts, the Bank did not adequately monitor transactions in amounts less than $50,000 per day for suspicious activity.'').

[26] *Pacific National Bank*, *supra*.

[27] *In the Matter of Wachovia Bank, National Association*, FinCEN Case No. 2010-1 (March 17, 2010)

[28] *Oceans Bank*, *supra*.

[29] *Id.*

[30] *Oceans Bank*, *supra*. *See also Citibank, N.A., supra.* The OCC ordered Citibank to undertake a comprehensive review of its automated transaction monitoring systems. The bank must ensure, among other things, that the transaction monitoring system is properly optimized, that the data feeds to that system have integrity, and that the system is sufficiently tailored to the bank's business. The OCC also required the bank to ensure that it fully utilizes the system's functionality and that the system's scenarios or rules are appropriate and effective.

[31] *Wachovia Bank*, *supra*.

   ISSN 0037-0665

shows that very few or no transactions within the parameters result in the filing of SARs, a firm might have a reasonable basis to adjust those parameters without a significant loss of yield, or alerts that are likely to result in SARs. This continual ''tweaking'' of parameters based on yield should refine transaction monitoring to hone in on those transactions that really present the most risk and are mostly likely to require a SAR.

3. *Manual Review Remains a Component of Any System*

It is clear that even the best automated systems cannot function without a manual component – the review of transactions identified by the automated system by a sufficient number of experienced and well-trained personnel. In its *Oceans Bank* decision, FinCEN found that the alerts identified by the bank's automated system were reviewed by Bank staff members who were inadequately trained and inexperienced in reporting suspicious activity. Consequently, the overwhelming majority of the alerts generated by the automated system were subsequently cleared when the bank should have filed SARs. A general AML training program often is not enough; a firm needs to provide those AML compliance employees who have greater exposure to financial transactions (e.g., wire transactions and journal activity) with specialized or enhanced AML training.[32]

Similarly, FINRA found that another firm's system relied on a limited number of employees to conduct primarily manual reviews of alerts generated by its automated monitoring system, despite the fact that at the time the firm cleared hundreds of thousands of trades per day for over 200 correspondent firms. Specifically, either one or two individuals were responsible for reviewing approximately two dozen different AML exception reports, some very lengthy, for suspicious activity. The firm's failure to allocate sufficient resources to the firm's AML compliance program resulted in, at times, inadequate and untimely reviews. Given the limited resources allocated to conduct these reviews, these exception reports were not consistently reviewed or, in some instances, reviewed at all.[33]

[32] *Penson*, *supra*.
[33] *Id*.

III. Recommendations

The decision to implement an automated transaction monitoring system is only one piece of the matrix of considerations required of a firm in assessing its AML system needs. Once a firm makes that decision it must consider, among other things, the extent of the firm's business that the system will monitor, the thresholds the firm will apply to the transactions monitored, and the extent of human and other resources it needs to apply to the system.

What a firm can do to make the most of its transaction monitoring:

A. Refresh due diligence and related risk ranking of accounts on a regular basis using a risk-based approach. Any identified changes in risk should correlate to necessary changes in the transaction monitoring system or its application.

B. Review its risk assessment to ensure that the program continues to address the risk of new customers, products, services or lines of business.

C. If the firm is using reports provided by its clearing firm, review any new reports offered to determine if they better suit the firm's monitoring needs.

D. Check to see that all appropriate data that needs to be monitored by the automated system is captured.

E. Optimize its transaction monitoring regularly to ensure that its automated systems are working efficiently and effectively.

F. Review alerts relative to SARs filed to determine whether the firm is reviewing those transactions that actually result in the need to file suspicious activity reports.

G. Make sure that reports generated by other automated systems that might show potentially suspicious transactions, such as consumer fraud or suspicious trading, are considered for SAR filing if those reports are reviewed by another department.

H. Document any changes to transaction monitoring thresholds or alerts.

I. Regularly review the process of reviewing alerts or manual monitoring to determine if there are any backlogs that suggest the need to hire additional staff, and that decisions to file or not to file SARs are appropriate.

J. Conduct training regularly and provide specialized training as appropriate.