New York State of Mind

December 21, 2016 ACAMS Exclusive
Author: Maleka Ali

"It comes down to reality and it's fine with me 'cause I've let it slide"[1] might be lyrics from our favorite Billy Joel song, but to many of us a New York state of mind is a reality.

Recently, the New York Department of Financial Services (NYDFS) passed a transaction monitoring regulation known as Section 504. Many might say, "I'm not in New York, so this will not affect me." However, many of the requirements in the final rule are expectations already in place by examiners across the country. What makes this new regulation unique is that the NYDFS will also require an annual certification from each institution they regulate. The growing concern from those not in New York is that this is the first time the examiners' expectations for model validation have been put to pen and paper in a regulation specifically addressing anti-money laundering (AML) monitoring programs. I predict New York's ruling will not be isolated and other states and regulators will quickly follow suit. The new rule will be effective January 1, 2017, and the first annual confirmation of compliance will be due starting April 15, 2018.

How did we get here?

FinCEN started the ball rolling in 2014 with a guidance outlining the need for financial institution leaders to promote a culture of compliance that is specific to AML compliance obligations. The guidance stressed that compliance is not just about policies, procedures or the compliance department. The implied emphasis was that compliance needs to be obvious at the very core and culture of an organization and without the institutions' leaders showing strong support for compliance with a tone at the top mentality, the program is more likely to fail than succeed.

Soon we saw increased focus coming from all directions:

- In a speech, Thomas Curry said that the Office of the Comptroller of the Currency (OCC) is extensively focused on the Bank Secrecy Act/anti-money (BSA/AML) compliance and highlighted that there will be increased focus on BSA/AML compliance in their exams.

- Deputy Attorney General Sally Yates issued a memo known as the Yates memorandum called "Individual Accountability for Corporate Wrongdoing" that expands the threat of civil enforcement and civil penalties against individuals.
- Benjamin Lawsky, former superintendent of NYDFS, introduced the proposed new regulation for New York and emphasized that he wants senior bank executives to attest to the adequacy of their institutions' BSA/AML monitoring programs.

The NYDFS' proposed rule clarifies the minimum attributes necessary in a transaction monitoring and a watchlist filtering program. Each of their regulated institutions must maintain either a manual or automated "monitoring program that is reasonably designed to monitor transactions for potential BSA/AML violations and suspicious activity reporting."[2] The final rule clarifies the minimum attributes. Even though your institution might not be in New York, these attributes—excluding the certification requirement—are expected by examiners and regulators across the nation, not just New York.

The following attributes are for both transaction monitoring and watchlist filtering programs[3]:

- Must be based on a comprehensive and ongoing risk assessment that includes size, staffing, governance, businesses, products and services, operations, and geographies
- Requires end-to-end and before-and-after implementation testing
- Needs to identify all relevant data sources, validate the integrity and quality of this data, and ensure the data is accurately mapped and transferred from sources to all automated systems
- Needs to provide and certify governance and management oversight of programs and all changes. Programs must be appropriately funded and staffed by qualified personnel or outside consultants and include appropriate and periodic training for all participants
- It is also critical that when an institution has identified areas, systems or processes that require material improvement, updating or redesign, (including internal identification or auditor, consultant or examiner), the institution is required to document the area needing improvement, along with any remedial efforts that are planned or currently in process and make this documentation available for inspection by the examiners

Additional Attributes for Transaction Monitoring Programs:

- Must be periodically reviewed and updated at risk-based intervals to reflect changes to any BSA/AML laws or regulations, regulatory warnings, and other relevant events
- Must match the AML risks at the institution. All institutions are unique and should not rely on default settings or mirror what that bank down the street is doing
- While it is universally accepted that you cannot catch everything, the program must include detection scenarios with threshold values and amounts that are reasonably designed to identify potential money laundering and other suspicious or illegal activities. In other words, is it doing what it is supposed to do?
- Reviews of governance, data mapping, transcodes, scenario logic, data input and program output
- Maintain documentation that details current detection scenarios and underlying assumptions for parameters and thresholds
- Needs procedures that detail the investigation and decision-making process for the alerts that are generated by the program
- Will also require ongoing analysis of the continued relevance of the scenarios, rules, thresholds, parameters and assumptions

Additional Attributes for Watchlist Filtering Programs

Each covered institution must maintain a manual or automated filtering program reasonably designed to catch transactions that are in violation of the Office of Foreign Assets Control (OFAC) sanctions. Unlike the proposed rule which applied to screening against "other sanctions lists," the final rule applies only to OFAC. Below are the listed attributes for the watchlist filtering program:

- Must be based on technology, processes or tools that are reasonably designed for matching names and accounts, based on the particular risks, transaction and product profiles of the institution
- Must review data matching, whether the OFAC sanctions list and the system's settings map to the institution's risks, must evaluate the logic of the matching technology or tools, as well as test the data input and program output
- Requires ongoing analysis of the logic and performance of the technology or tools used for matching names/accounts, and requires a continued assessment of whether the OFAC sanctions list and settings continue to map to the institution's risks
- Must maintain program documentation that articulates the reasoning and design of the filtering program tools, processes and/or technology

Under NYDFS Section 504, a regulated institution must submit to the NYDFS by April 15 of each year, (either by a board of directors' resolution or a senior officer(s) finding), that they are certifying compliance with the final rule in a form provided in Attachment A of the final rule. They are certifying that they have reviewed documents, reports and certifications, along with any opinions of officers, employees, outside vendors or other individuals as necessary, to confirm that their institution has a transaction monitoring and filtering program that complies with the provisions of the final rule and to the best of their knowledge, that the programs comply with Section 504.3 of the final rule as of the date of the compliance finding for the specified year.

Message for Compliance Professionals

In an effort to highlight the importance of AML compliance, regulators are sending a very strong message. Institutions face an increasing threat of cease-and-desist orders, consent orders or worse. What is most likely to earn penalties for compliance failures is a lack of systems that are capable of flagging suspicious activity, or well-trained people capable of analyzing what those systems spit out. Not only is the institution at risk, but individuals may also be found personally liable. Last January, in the U.S. Department of Treasury v. Haider,[4] a federal district court ruled that compliance officers of financial institutions can be held civilly liable for failures with the Bank Secrecy Act's provisions. This action upheld a FinCEN $1 million fine against Thomas Haider, MoneyGram's former chief compliance officer.

As mentioned previously, examiners (and not just those in New York) are expected to take an aggressive approach in enforcement. Institutions need to take necessary precautions to make sure they are not found deficient. Examiners will be looking to see if you have done reviews to ensure your program is adequate and that your systems are performing correctly and producing reliable alerts and accurate reports. Data integrity from end to end is one concern, but there is more to validation.

Validation

We have all become very familiar with the term model validation. In order to simplify a BSA model validation let us break it down and review its three main components: software system algorithm validation, data integrity validation and a program evaluation/efficiency review.

Software System Algorithm Validation

The software system validation piece is the test of the actual software algorithms to ensure they work as designed. If it is bank built and proprietary, it will need to be independently validated. If it is provided by a software vendor, you may discover that it was already independently validated by a third party and you should request a copy of this validation.

Data Integrity

It is critical to ensure you are not missing significant data in your AML program. Data usually comes from multiple sources, including your host core processors and other sources like teller, wire transfer, ACH, ATM and monetary instrument systems. It is crucial to identify all data sources and ensure they are mapped appropriately into the AML system.

Common data problems include:

- NAICS codes or business type codes. Often times, codes are missing or inaccurate, leaving the AML department in a dilemma of not knowing whether the activity they see makes sense for the business. In another scenario, an institution may have created their own codes and do not use NAICS codes. This might cause complications in a merger/acquisition situation requiring major clean up. In addition, FinCEN uses NAICS codes. Thus, if an institution created their own codes they run the chance of incorrectly filing currency transaction reports (CTRs) or suspicious activity reports (SARs).
- Signer information and relationship codes need to be mapped into AML systems. This information is not only critical in the filing of CTRs and SARs but relationship codes tell the system what that "name line's" relationship is to the account. With increased focus on customer due diligence, it is more important than ever for there to be a code to identify relationship and beneficial owners.

Often there is critical missing data. It is important to keep lists of all types of essential data and run regular checks on this data. Essential data that are often missing includes:

- International wires: Most institutions have more than one source for wires. Often auxiliary sources are forgotten and are not imported into the AML systems or international wires that are processed through a domestic bank may be overlooked as having an international source or beneficiary.
- Activity on loans and certificates (especially cash and wire transfers): This activity is often processed to a suspense or clearing account and as a result is not properly reflected in the AML systems. It is critical that testing be done to ensure that a work-around is established to ensure higher risk activity is imported.
- Monetary instrument sales: Critical to include all types offered including: Cashier's checks, prepaid cards, money orders and traveler checks.
- Capture the "real" purchaser—not just the name on the account.
- Import all monetary instruments—not just the items purchased with cash aggregating between $3,000 and $10,000. It is imperative for the identification of suspicious activity for all monetary instrument activity to be imported.

Program Efficiency Reviews

Program efficiency reviews are the part of the model validation where you evaluate and identify the filtering criteria most appropriate for your institution. Many institutions have proactively had efficiency reviews conducted to catch issues. Automation is great and brings powerful tools, but are they all turned on and are the rules up-to-date in recognition of evolving crime trends? It is important to have someone review and test system capabilities and parameters on a periodic basis and focus on specific parameters or filters in order to ensure that suspicious or unusual activity will be captured if it is happening. Optimization and tuning are

scary words to many. It is difficult to determine things like “What is a meaningful investigation?” or “When is a rule or scenario effective?”

When conducting program efficiency reviews it is important to consider the following:

- A meaningful investigation could result in a no-SAR decision**.** Institutions often conduct a full investigation on all alerts and only pass items to a case investigation once they are sure it will need a SAR. This actually slows down the process**.** It makes more sense to use the alert stage as triage. When looking at an alert, if the analyst cannot make a quick decision and document their reasoning in five to 15 minutes, then it is time to pass it on to a case investigation. Once the investigation is complete**,** you may find a reasonable explanation and clear it with a no-SAR decision.
- The effectiveness of a scenario and the resulting investigation will differ based on the intended purpose of the scenario. Some scenarios will produce lots of hits and reviews will be fast to clear. There will be others that hardly ever produce an alert and each one results in a SAR. It is important to treat each scenario separately and not compare and/or rate their effectiveness against each other.
- Some institutions report they were advised to turn certain scenarios off or lower the threshold because they were not producing alerts. The problem with this logic is two-fold. First, a scenario might never get hits because that type of suspicious activity is very rare for the institution. However, it should be reviewed if it ever happens. Second, many times, if you lower the threshold it becomes such a low dollar amount that it does not even seem suspicious anymore or is not SAR reportable.

It is important for institutions to have regular independent reviews conducted, keep up-to-date with criminal trends, understand new technology and keep tuning and adapting their AML programs to keep up with the crooks. New York might be the first state to require their institutions to certify that they are keeping up, but the basic requirements are universal, as are the expectations from regulators in all states.

It comes down to reality and unlike the Billy Joel song, some folks will not be able to take a holiday or hop on a flight to Miami Beach or to Hollywood. We are in a New York state of mind.

Maleka Ali, CAMS-Audit, president, Arc-Serv, Burbank, CA, USA maleka@arc-serv.com

1. From Billy Joel’s song “New York State of Mind.”
2. “New York Banking Regulator Issues Anti-Money Laundering Rules for Transaction Monitoring and Filtering Programs,” Sidley, July 7, 2016, http://www.sidley.com/~/media/update-pdfs/2016/07/20160707-banking-and-financial-services-update-1.pdf
3. Ibid.
4. “United District Court, Southern District of New York” https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Haider,%20Thomas%20Complaint.pdf