

Client Alert

NYDFS Requires Board or Senior Officers to Certify AML and Sanctions Compliance; Issues Additional Program Rules

August 23, 2016

On June 30, 2016, the New York State Department of Financial Services (NYDFS) adopted a final rule imposing new anti-money laundering (AML) and economic sanctions requirements on banks and other financial institutions regulated by the agency.

The rule applies to: (1) banks, trust companies, private bankers, savings banks, and savings and loan associations chartered under the New York Banking Law; (2) all branches and agencies of foreign banking corporations licensed under the Banking Law to operate in New York; and (3) check cashers and money transmitters licensed under the Banking Law (collectively, Regulated Institutions).

The rule requires Regulated Institutions to:

1. Maintain a “Transaction Monitoring Program” that is “reasonably designed” for post-transaction detection of violations of AML laws and to allow appropriate filing of suspicious activity reports as required under the Bank Secrecy Act (BSA).
2. Maintain a “Filtering Program” reasonably designed to interdict transactions prohibited by the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC).
3. Provide an annual board resolution, or finding by one or more “senior officers,” that the Regulated Institution complies with all Transaction Monitoring and Filtering Program requirements.

Both the Transaction Monitoring Program and the Filtering Program are required to have specific attributes detailed in the rule (and described below). NYDFS explained that it adopted the final rule after an investigation in which it found shortcomings in the existing transaction monitoring and filtering efforts of Regulated Institutions, which it attributes to “a lack of robust governance, oversight, and accountability at senior levels.”

Financial institutions strongly criticized the original version of the rule when it was first proposed in December 2015. The final rule adopts a number of significant changes that appear intended to address these criticisms.

The rule is effective January 1, 2017, and the first annual certification of compliance is due to the Superintendent of NYDFS on April 15, 2018.

Transaction Monitoring Program Requirement

The rule requires Regulated Institutions to maintain a program “reasonably designed for the purpose of monitoring transactions after their execution for potential BSA/AML violations and Suspicious Activity Reporting,” which must include the following attributes “to the extent they are applicable”:

- Be based on an ongoing, enterprise-wide Risk Assessment of the institution and its businesses.
- Be reviewed and updated at risk-based intervals to reflect current law and guidance, and other company information determined by the institution to be relevant.
- Appropriately match BSA/AML risks to the institution's businesses, products, services, customers and counterparties.
- BSA/AML detection scenarios with threshold values and amounts designed to detect potential money laundering or other suspicious or illegal activities.
- End-to-end, pre- and post-implementation testing of the program including, as relevant, a review of governance, data mapping, transaction coding, detection scenario logic, model validation, data input and program input.
- Documentation that articulates the institution's current detection scenarios and the underlying assumptions, parameters and thresholds.
- Protocols explaining (a) how alerts generated by the system will be investigated, (b) the process for deciding which alerts will result in a filing or other action, (c) the operating areas and individuals responsible for making such a decision, and (d) how the investigative and decision-making process will be documented.
- Be subject to on-going analysis to assess the continued relevancy of the detection scenarios, the underlying rules, threshold values, parameters, and assumptions.

Filtering Program Requirement

Regulated Institutions also must maintain a Filtering Program "reasonably designed for the purpose of interdicting transactions that are prohibited by OFAC," which must include the following attributes, "to the extent applicable":

- Be based on an ongoing, enterprise-wide Risk Assessment of the institution and its businesses.
- Be based on technology, processes or tools for matching names and accounts, in each case based on the institutions' particular risks, transaction and product profiles.
- End-to-end, pre- and post-implementation testing of the program, including, as relevant, a review of data matching, an evaluation of whether the OFAC sanctions list and threshold settings map to the risks of the institution, the logic of matching technology or tools, model validation, and data input and Program output.
- Be subject to on-going analysis to assess the logic and performance of the technology or tools for matching names and accounts, as well as the OFAC sanctions list and the threshold settings to see if they continue to map to the risks of the institution.
- Documentation that articulates the intent and design of the Filtering Program tools, processes or technology.

The rule also requires that both the Transaction Monitoring Programs and Filtering Programs contain the following elements, "to the extent applicable":

- Identification of all data sources that contain relevant data.
- Validation of the integrity, accuracy and quality of data to ensure that accurate and complete data flows through the programs.
- Data extraction and loading processes to ensure a complete and accurate transfer of data from their source to automated monitoring and filtering systems, if automated systems are used.
- Governance and management oversight, including policies and procedures governing changes to the programs to ensure that changes are defined, managed, controlled, reported, and audited.
- Vendor selection process if a third party vendor is used to acquire, install, implement, or test the programs or any aspect of them.
- Qualified personnel or outside consultants responsible for the design, planning, implementation, operation, testing, validation, and on-going analysis of the programs, including automated systems if applicable, as well as case management, review and decision making with respect to generated alerts and potential filings.
- Periodic training or all stakeholders with respect to the programs.

The new rule includes a number of new qualifiers, such as “to the extent applicable,” “as determined to be relevant by the institution,” “at risk-based intervals,” and “as relevant,” which soften these requirements and make them more risk-based as compared to the original, proposed rule.

The Transaction Monitoring Program and the Filtering Program provisions also now require programs that are “reasonably designed” to detect violations or suspicious activity or to interdict transactions prohibited by OFAC, respectively. However, although this too can be read as a move toward a risk-based approach to these programs, such language arguably gives NYDFS greater discretion than it had in the proposed rule to find violations in a program even where the program includes all of the specific features enumerated in the Transaction Monitoring Program and Filtering Program provisions (on the basis that the program, despite having these features, contains other failings that make it not “reasonably designed” to accomplish its required purpose). There is also the risk that regulators considering what is reasonable will apply “20-20 hindsight” to problems that emerge later, which can be a challenge to counter.

Both the Transaction Monitoring Program and the Filtering Program must be based on a “Risk Assessment,” which the rule specifically defines as “an on-going comprehensive risk assessment, including an enterprise-wide BSA/AML risk assessment, that takes into account the institution’s size, staffing, governance, businesses, services, products, operations, customers, counterparties, other relations and their locations, as well as the geographies and locations of its operations and business relations.” This raises the question of whether banks with foreign parents or affiliates will be held responsible for sharing BSA/AML risk information globally across affiliated entities. Recent guidance and enforcement actions by the Financial Crimes Enforcement Network (FinCEN), federal banking agencies, and the Department of Justice already can be read to suggest an expectation for such an approach at the federal level. This can create challenges for U.S. institutions with limited access to information from overseas affiliates, and legal issues under international data privacy laws, and it may require affected institutions to seek clarification about their responsibilities from NYDFS.

Requirement to Document Remedial Efforts

The new rule now contains a provision that requires Regulated Institutions, in cases where they identify aspects of their programs that “require material improvement, updating, or redesign,” to “document the identification and remedial efforts planned and underway” and to make such documentation available for inspection by the Superintendent of the NYDFS.

This replaces a much-criticized provision in the proposed rule that would have prohibited Regulated Institutions from making changes to their programs “to avoid or minimize filing suspicious activity reports, or because the institution does not have the resources to review the number of alerts generated ... or to otherwise avoid complying with regulatory requirements.” Financial institutions commented that this prohibition would have punished legitimate efforts to adjust alert programs to avoid false hits, causing a substantial waste of compliance resources dedicated to reviewing such alerts as well as an increase in defensive SAR filings that would reduce the utility of such reports to law enforcement. Although the new provision removes this prohibition, it does add a new compliance burden associated with documenting, in a form suitable for inspection by the NYDFS, changes to these programs, and applies to all improvements, not just changes to SAR reporting.

Required Annual Certification

The most criticized provision of the proposed rule would have required the chief compliance officer for Regulated Institutions to certify to NYDFS each year that the institution’s Transaction Monitoring Program and Filtering Program met the specific requirements for such programs laid out in the rule, and provided for criminal penalties in the event of an “incorrect or false” certification.

The new rule now requires each Regulated Institution to adopt and submit to NYDFS, by April 15 of each year, a resolution of the institution’s board, or a finding by one or more “Senior Officer(s),” that includes certain certifications about these programs spelled out in a standard form attached to the rule. This includes a certification that: (1) the board or Senior Officer(s) have “reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors, and other individuals or entities as necessary to adopt” the resolution or finding; (2) the board or Senior Officers have “taken all steps necessary to confirm that” the Regulated Institution has a Transaction Monitoring Program and Filtering Program that comply with the rule; and (3) “to the best of the [Board’s or relevant Senior Officers’] knowledge,” these programs comply with the rule. Regulated Institutions also must maintain for examination by NYDFS all of the records relied on for the board or Senior Officer certification, for a period of five years. As noted above, the first certification is due to NYDFS on April 15, 2018.

Although this provision seems to allow the certifying parties some reliance on facts developed by more junior officers or by counsel, the required certification that the Board or Senior Officers “have taken all steps necessary to confirm” that the programs comply with the rule, in a provision separate from the one providing for reliance on information provided by others, suggests that any reliance on information prepared by others must be reasonable. In response to criticism that the proposed rule would discourage qualified professionals from serving as chief compliance officers, the final rule now defines “Senior Officer(s)” to include not only compliance officials but also persons responsible for the management or operations of the institution. It also allows more

than one such officer to be responsible for the finding, or in the alternative to have the certification made through a resolution of the board. It remains to be seen how many Regulated Institutions will take advantage of this increased flexibility as to who makes the required certification.

The final rule also responds to heavy criticism of the proposed rule's provision for criminal penalties for "incorrect or false" certifications, which fueled concerns by compliance officers that they would be punished for inadvertent mistakes. It now provides generically that the rule will be enforced according to the "Superintendent's authority under any applicable laws." One of the laws cited as authority for the rule that presumably qualifies as an "applicable law" is Section 672 of the New York Banking Law, which establishes that it is a felony for "[a]ny officer, director, trustee, employee or agent of any corporation to which the banking law is applicable [to make] a false entry in any book, report or statement of such [...] with intent to deceive any officer, director or trustee thereof, ... or any public officer, office or board to which such corporation is required by law to report, or which has the authority by law to examine into its condition or into any of its affairs[.]" However, the removal of language about penalties for "incorrect or false" certifications does provide some comfort for inadvertent violations.

One issue that likely will need clarification is what Regulated Institutions should do in cases where an institution has identified deficiencies in its programs and is in the process of remediation at the time that the annual certification is due. As discussed above, the final rule now clearly contemplates situations where Regulated Institutions will identify deficiencies in their programs and undertake initiatives to remedy them, and requires documentation of these efforts, but says nothing about how such identified issues affect an institution's annual obligation to certify that its programs satisfy all of the requirements in the rule. In the absence of clarification, Senior Officers or board members could be caught between the threat of penalties against the institution for failing to certify that it is compliant, and the threat of individual penalties in the alternative for a false certification.

Practical Considerations

Changes to compliance programs take time, and Regulated Institutions should start assessing now what they will need to do to come into compliance with the rule by its January 1, 2017 effective date. Regulated Institutions likely already follow many of the practices required in the rule based on guidance from federal regulators or industry best practices. However, given the specificity of the new requirements, Regulated Institutions should begin a gap analysis now to identify areas where they may need to add new procedures, technology or personnel to their AML and sanctions programs to satisfy the requirements of the new rule.

This gap analysis should include in particular: (1) a review of the institution's risk assessments for these programs to determine whether they meet the standard called for in the rule, and whether any updates to such assessments require changes in the programs; (2) a review of the institution's detection or interdiction scenarios and logic for AML and sanctions, and the documentation for these, against the requirements of the rule; (3) considering whether additional procedures are needed to meet the new requirement in the final rule that institutions document the identification and remediation of improvements to their programs; and (4) a consideration of who in the institution will make the annual certification of compliance called for in the rule,

what documents those persons will rely on to make the certification, and how these documents will be preserved for review by NYDFS.

The new rule also comes at a time when banks subject to BSA regulation are preparing to comply, by May 11, 2018, with new FinCEN rules which require banks to obtain and incorporate into their AML programs beneficial ownership information about their legal entity clients (see our analysis of FinCEN's beneficial ownership rule [here](#)). Regulated Institutions should consider whether and how they will implement anticipated beneficial ownership information into their Risk Assessments, detection scenarios, and other aspects of their Transaction Monitoring Programs and Filtering Programs.

Regulated Institutions should expect aggressive enforcement of the new rule. The NYDFS in the past has taken a very aggressive approach to enforcing sanctions and AML-related violations committed by financial institutions, and the new rule provides the agency more bases for additional enforcement. Although Maria Vullo, the recently-confirmed Superintendent of the agency, has demonstrated some responsiveness to industry concerns regarding the proposed rule, in particular the concern about a “strict liability” standard for the annual certification, she also has indicated a willingness to impose accountability at high levels.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Carlton Greene

Partner – Washington, D.C.

Phone: +1.202.624.2818

Email: cgreene@crowell.com