NYDFS Issues New AML/Sanctions Program Requirements

By V. Gerard Comizio, Lawrence D. Kaplan & Amanda M. Kowalski

Introduction
The New York Department of Financial Services (“NYDFS”) recently promulgated a highly-anticipated regulation, to become effective January 1, 2017, imposing new anti-money laundering, anti-terrorism, and economic and trade sanctions requirements on financial institutions regulated by the NYDFS (the “Final Rule”). The Final Rule is the latest example of the NYDFS’ increased activity in the BSA/AML arena, following several years of enhanced supervision and enforcement of Bank Secrecy Act/anti-money laundering laws (“BSA/AML”) as well as the economic and trade sanctions administered by the U.S. Department of the Treasury’s Office of Foreign Assets Control (“OFAC”). As result of such actions, NYDFS has indicated that it “has reason to believe that financial institutions have shortcomings in their transaction monitoring and filtering programs.” The Final Rule, therefore, imposes regulatory requirements for all institutions operating in New York and emphasizes the increased regulatory focus on BSA/AML issues, although it does not impose transaction monitoring and filtering program requirements beyond what most sophisticated financial institutions have already implemented.

The Final Rule clarifies and implements the requirement that financial institutions regulated by the NYDFS maintain a Transaction Monitoring and Filtering Program, and adopts the controversial mandate that a certificate of compliance be executed by a Senior Officer.

The Final Rule broadly applies to all “Regulated Institutions,” defined to include:

(i) banks, trust companies, private bankers, savings banks, savings and loan associations, and all branches and agencies of foreign banking corporations licensed to conduct banking operations in New York, and

(ii) New York-licensed check cashers and money transmitters.

The rule, however, does not apply to federally-chartered depository institutions or those not chartered or licensed by the NYDFS, as well as certain other institutions subject to separate AML requirements.

The Final Rule significantly departs from the NYDFS’ December 2015 proposed rule. As noted, the Final Rule retains the requirement that a Regulated Institution’s Board of Directors adopt a resolution or a Senior Officer execute a certification of compliance, modeled on certifications required under the Sarbanes-Oxley Act of 2002. While the Final Rule removed an explicit reference to criminal liability for Senior Officers who must certify as to an institution’s compliance with the Final Rule, the certification
requirement is consistent with the NYDFS’ recent focus on imposing liability in appropriate circumstances for violations of the banking laws, not only on banking organizations but also on responsible officers, directors, and/or employees. Further, it should be noted that the NYDFS reserves the authority to enforce the Final Rule “under any applicable laws.”7 Thus, while the explicit reference to criminal liability has been removed from the Final Rule, it may be argued that the NYDFS has retained the right to pursue actions under New York criminal law. Accordingly, compliance with the Final Rule by Regulated Institutions will likely draw significant compliance attention, as directors or Senior Officers could still face significant personal liability.

Requirements of the Final Rule

The key requirements of the Final Rule include the following:

**Maintain a Transaction Monitoring Program**

Each Regulated Institution is required to maintain a Transaction Monitoring Program reasonably designed to identify potential BSA/AML violations and trigger Suspicious Activity Reporting. The system, which may be automated or manual, must include the following components, to the extent applicable:

- be based on the Risk Assessment of the institution;
- be reviewed periodically updated to reflect changes to BSA/AML laws and any other relevant information;
- appropriately match BSA/AML risks to the institution’s businesses, products, services, and customers/counterparties;
- include BSA/AML detection scenarios with threshold values and amounts designed to detect potential money laundering or other suspicious or illegal activities;
- involve comprehensive pre- and post-implementation testing of the Transaction Monitoring Program (as described below);
- require documentation that articulates the institution’s detection scenarios and underlying assumptions, parameters, and thresholds;
- implement protocols setting forth how alerts generated by the Transaction Monitoring Program will be investigated and related documentation; and
- be subject to an ongoing analysis to assess the continued relevancy of the detection scenarios and underlying values, parameters, and assumptions.

A “Risk Assessment” means “an ongoing 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.”8 Thus, the Final Rule reiterates regulatory expectations that an institution’s BSA/AML program be tailored to its specific risk areas.
Maintain a Watch List Filtering Program

Each institution is also required to maintain a Filtering Program, reasonably designed to interdict transactions that are prohibited by OFAC. This is a departure from the Proposed Rule, which would have extended these requirements to include the vague "other sanctions lists, politically exposed persons lists, and internal watch lists."^9

The OFAC filtering program may be automated or manual and must include the following attributes, to the extent applicable:

- be based on the risk assessment of the institution;
- be based on technology, processes or tools for matching names and accounts, in each case based on the institution’s particular risks, transaction, and product profiles;
- include end-to-end, pre- and post-implementation testing of the Filtering 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 ongoing 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; and
- Require documentation that articulates the intent and design of the Filtering Program tools, processes, or technology.

These requirements underscore that all U.S. persons, including financial institutions, are subject to OFAC’s regulations and program requirements. This generally includes all U.S. persons regardless of where located, all persons and entities within the U.S., all U.S.-incorporated entities and their foreign branches, and all U.S. financial institutions. Although the Final Rule does not require that a filtering program screen against non-U.S. sanctions lists, fully-functional programs likely would also filter against sanctions programs outside the U.S., such as those administered by the European Union.

Additional Requirements for Transaction Monitoring and Filtering Programs

In addition to the requirements enumerated above, each Transaction Monitoring and Filtering Program must require the following, to the extent applicable:

- include identification of all data sources that contain relevant data;
- provide for validation of the integrity, accuracy, and quality of data;
- include data extraction and loading processes to ensure complete and accurate transfer of data to automated filtering systems, if used;
- impose governance and management oversight, including policies and procedures governing changes to the Transaction Monitoring and Filtering Program;
- be subject to a vendor selection process if a third-party vendor is used to acquire, install, implement, or test the Program or any aspect of it;
require sufficient funding to design, implement, and maintain a Transaction Monitoring and Filtering Program;

utilize qualified personnel or outside consultant(s) responsible for the design, planning, implementation, operation, testing, validation, and on-going analysis of the Transaction Monitoring and Filtering Program, including automated systems if applicable, as well as case management, review, and decision making with respect to generated alerts and potential filings; and

conduct periodic training of all stakeholders with respect to the Transaction Monitoring and Filtering Program.

Additionally, to the extent an institution has identified areas of the Program that require material improvement, updating, or redesign, the institution is required to document such efforts and make the documentation available to the Superintendent of the NYDFS.

Annual Certification

To ensure compliance with the Final Rule, Regulated Institutions are required to submit by April 15th an Annual Board Resolution or Senior Officer Compliance Finding addressing the Regulated Institution’s compliance with the Final Rule. The required compliance certification must provide that the Board of Directors or a named Senior Officer:

(1) has reviewed necessary documents, reports, certifications, and opinions of such officers, employees, representatives, outside vendors, and other individuals or entities as necessary to adopt the certification;

(2) took all steps necessary to confirm the Regulated Institution is in compliance with the Final Rule; and

(3) to the best of their knowledge, as of the date of the certification, the Transaction Monitoring and Filtering Programs are in compliance with section 504.3 of the Final Rule for the prior year.

The certification requirement was the most highly-anticipated aspect of the Final Rule and differs from the Proposed Rule in two material respects. First, the certification no longer must be submitted by the institution’s chief compliance officer—it may be submitted by any “Senior Officer,” defined to mean the senior individual(s) responsible for the management, operations, compliance, and/or risk of a regulated institution. Second, as noted, the Final Rule removes the Proposed Rule’s explicit reference to criminal liability for officers who file an incorrect or false certification. This is a notable difference because certifying officials will no longer be personally subject to criminal penalties under the Final Rule merely for misstatements in the document. However, the enforcement provision of the rule emphasizes that it will be enforced pursuant to, and is not intended to limit, the Superintendent’s authority "under any applicable laws." This authority includes New York Banking Law § 672, which makes it a felony for “any officer, director, trustee, employee or agent” of an institution subject to New York banking law to make a false entry in “any book, report or statement” of such financial institution with the intent to deceive. Thus, criminal liability may still apply in cases of willful intent, including omission of information.
Each regulated institution must also maintain all records, schedules, and data supporting adoption of the Board Resolution or Senior Officer Compliance Finding for a period of five years.

**Action Items for Regulated Institutions**

Regulated institutions operating in New York, including New York-chartered and foreign financial institutions, should review their existing BSA/AML and OFAC compliance programs to ensure they comply with the explicit requirements of the Final Rule in advance of the January 1, 2017 effective date. This should include:

- reviewing and updating the institution’s specific Risk Assessment to ensure it encompasses enterprise-wide operations and risks;
- reviewing and updating the institution’s OFAC screening system, including when changes to OFAC regulations or the List of Specially Designated Nationals are made;
- identifying a Senior Officer to provide the annual compliance certification and ensure there are adequate procedures, processes, and oversight in place to ensure the certification is made without risk of omission;
- taking steps to ensure that the Board of Directors has sufficient information to authorize a Senior Officer to accurately certify as to the financial institution’s compliance with the Final Rule. Boards and Senior Officers should now highly incentivized to:
  - review and update compliance policies to ensure best practice policies that take into account the obligations now imposed on Senior Officers under the certification requirement and New York Banking Law;
  - cause adoption and implementation of updated policies, systems, and procedures that successfully execute their company’s AML compliance policies, and thus, mitigate potential liability;
  - conduct a full review of the scope of relevant indemnification provisions in corporate governance documents, as well as applicable laws; and
  - review existing director and officer insurance policies, and seek expanded coverage as needed to address perceived deficiencies.

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings Washington, D.C. lawyers:

- V. Gerard Comizio  
  1.202.551.1272  
  vgerardcomizio@paulhastings.com

- Lawrence D. Kaplan  
  1.202.551.1829  
  lawrencekaplan@paulhastings.com

- Scott M. Flicker  
  1.202.551.1726  
  scottflicker@paulhastings.com

- Amanda M. Kowalski  
  1.202.551.1976  
  amandakowalski@paulhastings.com

Stay Current is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2016 Paul Hastings LLP.

“Transaction Monitoring Program” means a program that includes the attributes specified in Subdivisions (a), (c), and (d) of Section 504.3. See § 504.2(i). “Filtering Program” means a program that includes the attributes specified in Subdivisions (a), (c), and (d) of Section 504.3. See § 504.2(j).

See Final Rule at § 504.2(g).

Final Rule § 504.2(b).


Final Rule at § 504.5.

Final Rule at § 504.2(f).


Final Rule at 504.2(a).

Final Rule at § 504.2(g).

Final Rule at § 504.5.