NOW + NEXT

REGULATED FINANCIAL INSTITUTIONS ALERT | NIXON PEABODY LLP

MARCH 2, 2016

Proposed regulation regulating transaction monitoring by banks, check cashers and money transmitters

By Lawrence D. Fruchtman

A pending rulemaking by the New York State Department of Financial Services (NYSDFS) would add potential New York State criminal liability to the burdens of chief compliance officers of New York chartered banks, trust companies, savings banks, savings and loan associations, New York licensed branches and agencies of foreign banks, as well as all New York licensed check cashers and money transmitters (but not credit unions).

The rulemaking was announced in December 2015 by New York's Governor Cuomo as "a new anti-terrorism and anti-money laundering regulation that includes—among other important provisions—a requirement modeled on Sarbanes-Oxley that senior financial executives certify that their institutions have sufficient systems in place to detect, weed out and prevent illicit transactions."[1] It was published in the *New York State Register* on December 16, 2015, and is open for public comment until March 31, 2016. If adopted, it would be codified as a new Part 514 of the Superintendent's Regulations.

Although the proposed rule purports not to alter existing federal requirements, but only to provide "more granular guidance," it substantively changes New York law by imposing New York-specific non-risk based standards over and above federal standards governing Bank Secrecy Act, Anti-Money Laundering and Office of Foreign Assets Control (BSA/AML/OFAC) compliance, which are risk based and allow for reasonable management judgment.

New York financial institutions subject to these rules will find it difficult to meet the New York standards, and compliance officers will likely resist providing certifications that risk criminal prosecution. The rule may also require New York institutions to rely extensively on outside consultants, or detailed sub-certification processes, to enable compliance officers to provide the mandatory certifications. Accordingly, the proposed rule, if adopted in its present form, will

[1] See NYSDFS Press Release dated December 1, 2015, available here. The proposed rule and related material can be found here.

significantly disadvantage New York chartered and licensed financial institutions, make it harder for them to maintain effective BSA/AML/OFAC compliance programs and make it more difficult to attract and retain competent compliance officers.[2]

Certifications by the chief compliance officer

The proposed rule would require the chief compliance officer (or functional equivalent official) to certify, to the best of his or her knowledge, that he or she has reviewed, or caused to be reviewed, the institution's suspicious activity transaction monitoring program and the OFAC watch lists filtering program and that such programs comply with all the requirements set forth in the rule. The certification must be filed by April 15 of each year. The rule specifically warns that a senior compliance officer who files *an incorrect or false* certification *may be personally subject to criminal penalties*.

The proposed rule thus potentially criminalizes decisions that, under federal law, involve risk-based requirements that involve significant management discretion. As pointed out in a recent Financial Action Task Force Report: "The [risk based approach] . . . is not a "zero failure" approach; there may be occasions where an institution has taken reasonable . . . [anti-money laundering/counter-terrorist financing] . . . measures to identify and mitigate risks, but is still used for [money laundering or terrorist financing] purposes in isolated instances."[3] A senior compliance officer for a New York financial institution who believes that the firm's transaction monitoring systems do not completely fulfill the rule's requirements, even if they fully meet federal standards, would have the choice of providing the certification and risking criminal prosecution, or withholding certification and causing his or her employer to be targeted for violation of the proposed rule.

As a practical matter, given the complexity of the systems involved, it may be virtually impossible for a senior compliance officer to avoid being second guessed by an examiner or prosecutor for a BSA/AML or OFAC error. Looming as well is the growing concern of senior compliance officers with personal liability of corporate officers and employees under the new U.S. Justice Department's policy as articulated in the Yates Memo,[4] as well as the massive civil penalties for BSA and OFAC violations levied by New York State, through the NYSDFS and the Manhattan District Attorney's Office, among others, against a number of foreign banks with New York licensed branches and agencies in recent years.

Certifications based on matters outside the control of the senior compliance officer

The proposed rule would require the senior compliance officer to certify as to several matters that are outside his or her control. For example, BSA/AML/OFAC monitoring systems are built upon each regulated institution's customer identification program and related customer risk assessments. The customer identification program may be carried out by numerous and, in large institutions, hundreds or thousands of branch personnel, private bankers and lending and trust officers, who do not report to, and whose priorities appropriately differ from, the senior compliance officer. Similarly, systems work will be the responsibility of the institution's information technology

---

[2] Any comments on the draft regulation should be submitted to the NYSDFS at comments@dfs.ny.gov. by March 31, 2016.

[3] See Guidance for a Risk-Based Approach Money or Value Transfer Services, February 2016, p. 15, available here.

[4] See memorandum dated September 9, 2015, from Deputy Attorney General Yates, available here.

department or outside vendors. In this connection, the proposed rule requires the senior compliance officer to account for "other relevant areas, such as security, investigations and fraud prevention."

The federal interagency *BSA/AML Examination Manual*[5] for example, states that: "When multiple departments are responsible for researching unusual activities . . . . the lines of communication between the departments must remain open." However, the responsibility of ensuring that these lines of communication remain open is on senior management, not the senior compliance officer. In order for the compliance officer to provide the mandated certification, he or she may need assurance from outside consultants, or from sub-certifications from all relevant areas, or both.

Likewise, the proposed rule requires the senior compliance officer to certify that the transaction monitoring systems are, in effect, adequately funded, which is also a matter that will be ultimately determined by senior management and the Board of Directors rather than the senior compliance officer.

Substantive changes to AML/BSA/OFAC monitoring requirements.

The proposed rule creates a series of requirements, either explicit or implicit, that fail to acknowledge the significance of management's risk-based approach to its BSA/AML/OFAC monitoring systems, as contemplated by federal law.

100% interdiction standard; barring adjustments to monitoring systems

The proposed rule appears to require OFAC monitoring systems to interdict *all* unlawful transactions and also bars institutions from making "changes or alterations" to their transaction monitoring 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 by a Program . . . "*. However, the federal regulators recognize that the OFAC screening system does not require a "zero failure" approach and should have thresholds consistent with an institution's risk assessment that may not identify all potential transactions subject to OFAC sanctions. The *BSA Manual* states that "Decisions to use interdiction software and the degree of sensitivity of that software should be based on a bank's assessment of its risk and the volume of its transactions. In determining the frequency of OFAC checks and the filtering criteria used (e.g., name derivations), banks should consider the likelihood of incurring a violation and available technology."

The *BSA Manual* also states: "The bank's policies, procedures[] and processes should also address how the bank determines whether an initial OFAC hit is a valid match or a false hit. *A high volume of false hits may indicate a need to review the bank's interdiction program.*"[6] The NYSDFS has recognized this issue in a recent enforcement action, requiring the institution to include within its written plan to enhance compliance with OFAC regulations: "procedures to ensure that *the processes used to suppress repetitive false positives* are periodically reviewed and updated to ensure appropriateness and relevance.[7]

---

[5] The *BSA Manual* is issued by the Federal Financial Institutions Examination Council and is available here.

[6] *BSA Manual* at p. 147.

[7] See Written Agreement among the Industrial Bank of Korea, its New York Branch, the FRB and the NYSDFS dated

(Footnote continued on next page)

An institution's transaction monitoring systems both at implementation, and thereafter, need to be adjusted to reduce the number of false alerts, which detract from an institution's ability to address "true" alerts. Implementation of any transaction monitoring system is an iterative process that uses the risk-based settings of the system to minimize the number of false alerts and maximize the number of "true" alerts. Accordingly, given that this iterative process is found in the development and ongoing or periodic maintenance of every monitoring system, it is hard to see how a senior compliance officer can certify compliance with the foregoing prohibition. A senior compliance officer may also find it difficult to certify to the funding that supports the transaction monitoring systems, knowing that their settings have been optimized, and continue to be optimized, in this manner.

Continuous risk monitoring and watch list updates

The proposed rule appears to require each regulated institution to continuously revise its BSA/AML/OFAC risk assessments on which its monitoring systems are based. In contrast, federal requirements, embodied in the *BSA Manual*, state that unless there are changes in the institution's risk profile, such as a merger, or the introduction of new products or services, "*it is a sound practice* for banks to periodically reassess their BSA/AML risks at least every 12 to 18 months."[8]

The proposed rule also requires that the firm's suspicious activity monitoring system "reflect all current BSA/AML laws, regulations and alerts, as well as any relevant information available from the institution's related programs and initiatives, *such as 'know your customer due diligence,' 'enhanced customer due diligence' or other relevant areas, such as security, investigations and fraud prevention . . .* ". Regulated institutions and their senior compliance officers will certainly seek to meet this requirement; however, the sheer volume of these issuances and the number and timing of changes render a certification that the monitoring systems fully comply with the foregoing, even subject to a knowledge exception, difficult to provide.

Easy to understand documentation

The rule would require that BSA/AML/OFAC monitoring systems include "*easily understandable*" documentation. However, even the simplest of these systems is highly complex and requires trained individuals to understand how they operate. The systems' documentation will reflect this complexity and, while they can be well written and easily understandable by a person reasonably acquainted with bank operations and money laundering tools, it is doubtful that they will be "easily understandable" by a lay person. Accordingly, without clarification, a senior compliance officer could not certify to this aspect of the regulation, even with the best drafted documentation.

Real-time monitoring

Among other things, the Proposed Regulation appears to require "real-time" interdiction of transactions on the basis of watch lists, including OFAC or other sanctions lists, politically exposed person lists and internal watch lists. However, much transaction processing is still handled on a batch basis either at various times during the day or at night rather than on a "real time" basis. Under the current federal requirements, financial institutions can make a reasonable business judgment as to the most effective way of processing such transactions and a risk based judgment as

February 24, 2016, available here.

[8] *BSA Manual* at p. 22.

to the manner in which they identify transactions required to be frozen or rejected under the OFAC rules. The key is that the transactions are properly handled, not how the processing occurs.

Use of manual monitoring systems

Finally, while the proposed rule gives a nod to the possibility of using manual monitoring systems, its language and very specific requirements strongly suggest that manual systems will not likely be compliant. This could jeopardize the business of very small community banks and thrifts, and small check cashers and money transmitters, adding to the tension between societies' desire to provide banking and financial services to as many people of varied economic conditions as possible, and the costs and risks of failing to comply with BSA/AML/OFAC rules.

For more information on the content of this alert, please contact your regular Nixon Peabody attorney or:

- Lawrence D. Fruchtman at **lfruchtman@nixonpeabody.com** or (212) 940-3015
- Raymond J. Gustini at **rgustini@nixonpeabody.com** or (202) 585-8725