Banking and
Finance Law Daily

Wolters Kluwer

February 8, 2018

# New York Cybersecurity Regulations Could Affect Foreign Banks

By Michael E. Leiter William J. Sweet, Jr. Donald L. Vieira
Skadden, Arps, Slate, Meagher & Flom LLP

Financial institutions covered by the New York State Department of Financial Services' (NYDFS) new Cybersecurity Requirements for Financial Services Companies must file their first annual certification by February 15, 2018. The regulations also require covered institutions to complete additional tasks throughout the remainder of 2018.

## What Are the Regulations?

The regulations, the majority of which became effective in August 2017, require certain banks, insurance companies and other financial services institutions — including foreign banks operating New York branches and agencies — to establish and maintain a cybersecurity program. The regulations set forth general minimum standards for firms' cybersecurity programs and codify certain best practices into law. These regulations signify the first significant prescriptive rules on a state level in the cybersecurity space. State regulators have otherwise preferred to reference guidelines such as the National Institute of Standards and Technology Cybersecurity Framework and various industry-specific procedural and governance best practice standards. With the institution of these cybersecurity regulations, covered entities may face penalties for noncompliance.

> ***"These regulations signify the first significant prescriptive rules on a state level in the cybersecurity space."***

## Who Do the Regulations Cover?

Entities covered by the regulations include those operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization according to New York state banking, insurance or financial services laws. (See our September 15, 2016, client alert "New York State Proposes Cybersecurity Regulation for Financial Institutions.") While the regulations do not apply to national banks and federal branches of foreign banks, they do apply to the information systems that support the New York-licensed branch. As a practical matter, significant segments of a bank's global information system may be covered by the regulations if they cannot be logically separated from those that support the New York-licensed branch. Foreign banks face an additional compliance burden, considering they are subject to multiple foreign and domestic regulators' expectations. Prescriptive rules such as the NYDFS regulations will necessarily impact cross-border systems and operations as other jurisdictions adopt this type of cybersecurity regulation.

> *"Foreign banks face an additional compliance burden, considering they are subject to multiple foreign and domestic regulators' expectations."*

Foreign banks also should be aware that the cybersecurity regulations' definition of "nonpublic information" is more expansive than many other regulatory definitions of personally identifiable information and includes certain nonpublic business information. Accordingly, the set of NYDFS-covered systems containing such information may be meaningfully broader than those included in other regulatory frameworks. As a result, during a cyber event, covered entities must consider whether nonpublic business information was accessed in addition to traditionally targeted personally identifiable information.

Importantly, a foreign bank's New York branch can adopt an affiliate's cybersecurity program, rather than create one specifically to comply with the rules, if it meets the requirements.

## What Is Required in the February 15, 2018, Certification?

In February 2018, covered entities must submit their first annual certification attesting to their compliance with the regulations to the NYDFS superintendent. The certification, a format for which is available from the NYDFS, requires the chairperson of the board of directors or a senior officer of the institution to certify that the board has reviewed the institution's policies required under the regulations and, to the best of their knowledge, that the program complies with the regulations' requirements.

Importantly, a certification of compliance indicates that the board member and/or senior official has determined to the best of their knowledge that the institution is prepared to notify the department of a covered "cyber event" within 72 hours of its discovery. Specifically, covered entities must report any act or attempt, successful or unsuccessful, to gain unauthorized access to, or disrupt or misuse, a covered system or the information stored on it. In practice, many covered entities likely already prepare for a cyber event, but reporting the event to the NYDFS within the specified time frame will be an added compliance burden.

If, during the process of implementing the plans and procedures required by the regulations, the covered entity identifies areas, systems or processes that require "material improvement, updating or redesign," then the entity is required to document the "identification and the remedial efforts planned and underway to address such areas, systems or processes" and maintain such documentation.

Finally, covered entities must maintain for examination by NYDFS all records, schedules and data supporting the certification for a period of five years.

## What Additional Requirements Become Operative in 2018?

By March 2018, all covered entities, including covered foreign banks, must complete the following tasks:

- submit to the board (or a senior officer) the chief information security officer's report on the covered company's cybersecurity program;
- conduct an annual penetration test and vulnerability assessment;
- conduct an annual written risk assessment;
- implement multifactor authentication; and
- provide regular cybersecurity awareness training to personnel.

By late 2018, the covered entity must further expand its cybersecurity program to include:

- an audit trail;
- written procedures, guidelines and standards for the security of in-house or externally developed applications;
- data retention policies and controls to protect nonpublic information;
- policies and procedures to monitor the activity of authorized users; and
- controls, including encryption, to protect nonpublic information.

## Should We Expect Robust Enforcement by NYDFS?

To date, NYDFS has been active in the use of its regulatory authority in the cybersecurity space, including conducting a series of surveys of covered entities that contributed to the development of the current regulations. Therefore, while it remains unclear how NYDFS will enforce its new regulations and remedy noncompliance, given the novel nature of their implementation, it is likely that it will move to aggressively audit compliance as contemplated under the regulations. Critically, given the importance that regulators, including NYDFS, have placed on cyber issues, it is likely that any negative action by NYDFS will be coupled with negative media attention and the potential for legal action by third parties, including customers and other regulators.

## Key Takeaways

With 2018 underway, effective dates for additional portions of the cybersecurity regulations are approaching, and boards and senior officers of covered entities should begin to actively and meaningfully inquire into their institutions' progress in complying with the new rules. That inquiry should include an evaluation of their systems' security posture and existing risks and vulnerabilities. One important example is the institution's ability to meet the short 72-hour deadline for reporting cyber events. Given the scope of the reporting requirement and the continuous attacks to which they are subject, banks may bear a large reporting burden. Ultimately, while instituting new compliance measures may be time-consuming, banks should weigh the costs against not only the financial implications of a breach and government response but also the expense of negative publicity from a public NYDFS enforcement action.

*Associates Katherine A. Clarke, Jennifer Ho and Joe Molosky contributed to this article.*

*This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.*