Westlaw Journal
BANK & LENDER LIABILITY
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 22, ISSUE 19 / FEBRUARY 6, 2017

EXPERT ANALYSIS

The New York State Department Of Financial Services Issues Revised Cybersecurity Regulations

By Daniel A. Cotter, Esq.,
Butler Rubin Saltarelli & Boyd

On December 28, 2016, the New York Department of Financial Services (the "NYDFS") issued revised cybersecurity regulations addressing comments submitted by interested industry members to the NYDFS's September 13, 2016, draft. The press release from New York Governor Andrew Cuomo that accompanied the September draft announced the proposal of "a new first-in-the-nation regulation" requiring banks, insurance companies and other financial institutions regulated by NYDFS to "establish and maintain a cybersecurity program designed to protect consumers."[1]

The December 28th revised regulations make several changes to the September draft,[2] reacting to comments from the industry[3] and with some adjustments made to permit more flexibility for covered entities to design their cybersecurity program.

Governor Cuomo's September 13, 2016, press release announcement followed a November 9, 2015, letter from NYDFS Acting Superintendent Anthony J. Albanese to the members of the New York Financial and Banking Information Infrastructure Committee ("FBIIC"),[4] notifying those agencies that the NYDFS was considering "potential new NYDFS Cybersecurity Regulation Requirements" (the "NYDFS Cyber Letter").[5]

These proposed regulations are the most extensive that have been put forward issued by any agency to date and will have a major impact on the cybersecurity practices of financial services companies as well as those with whom they interact. This article addresses the newly published, revised "Cybersecurity Requirements for Financial Services Companies"[6] and what financial services companies will need to do to comply with them.

THE NYDFS SURVEYS

The NYDFS conducted surveys of its regulated banking organizations in 2013 and of its regulated insurers in 2013 and 2014. The surveys requested that the banks and insurers respond to questions about their cybersecurity programs, the costs of those programs, and their future cybersecurity plans. In May 2014, the NYDFS issued its "Report on Cyber Security in the Banking Sector" (the "Banking Report"), which contained the results of 154 banking institutions' responses.[7]

In February 2015, the NYDFS issued its "Report on Cybersecurity in the Insurance Sector" (the "Insurance Report"), which included survey responses from 43 insurance providers with combined assets of approximately $3.2 trillion.[8] The findings and conclusions of the Banking Report and the Insurance Report were similar, with a few major exceptions.

First, whereas the Banking Report noted that corporate governance for cyber was primarily within the IT framework, the Insurance Report found that "a majority of insurers reported involvement from a number of different departments within their organizations." The other major difference related to

The proposed regulations are the most extensive that have been put forward issued by any agency to date and will have a major impact on the cybersecurity practices of financial services companies.

the frequency of cybersecurity incidents and breaches. The Insurance Report noted that "58% of insurers reported that they experienced no cyber security breaches in the three years preceding the survey, excluding failed attempts." In contrast, the Banking Report stated that most banking institutions had experienced actual or attempted intrusions into their IT systems in the three years prior to the survey.

The Insurance Report concluded that the NYDFS was "considering the use of various security technologies in financial institutions" and discussed its meetings with the insurance industry to learn more about the cyber insurance market.

As a follow up to the May 2014 Banking Report, the NYDFS issued a letter in October 2014 to 40 banking organizations to try to obtain more information regarding banking organizations' practices with respect to third-party service providers and how the banking organizations managed this process (the "Vendor Management Report").[9]

THE NYDFS CYBER LETTER

On November 9, 2015, Acting Superintendent Albanese issued the NYDFS Cyber Letter to the FBIIC Members (*endnote 3 provides a list of FBIIC Members*). Albanese informed the FBIIC Members that his hope was to lead to "new, strong cyber security standards for financial institutions." Citing the Banking and Insurance Reports, Albanese noted "several additional actions" the NYDFS had undertaken to address cybersecurity, including: 1) expanding its IT examination procedures "to focus more attention on cybersecurity," and 2) focusing on "the financial industry's reliance on third-party service providers for critical banking and insurance functions."

After making a number of conclusions and observations based on the surveys and other interactions by the NYDFS with the financial services industry, the NYDFS Cyber Letter set forth "the key regulatory proposals that [the NYDFS is] currently considering" and requested the FBIIC Members' collaboration and cooperation. Specific requirements were outlined in the following areas:

- Cybersecurity Policies and Procedures — The proposed regulations contained twelve areas that a financial institution's written cybersecurity policies and procedures would be required to cover.[10]
- Third-party Service Provider Management — Regulated entities would be required to have policies and procedures to ensure the security of sensitive data, with "minimum preferred terms" for third-party service providers.[11]
- Multi-Factor Authentication — Regulated entities would be required to implement multi-factor authentication for certain data access and transmission.
- Chief Information Security Officer — Regulated entities would be required to designate a qualified employee.
- Application Security — Regulated entities would be required to have written policies and procedures to ensure security of all applications utilized.
- Cybersecurity Personnel and Intelligence — Regulated entities would be required to employ adequate personnel to manage cyber risks of the entity.
- Audit — Regulated entities would be required to conduct annual penetration testing and quarterly vulnerability assessments, and
- Notice of Cybersecurity Incidents — Regulated entities would be required to "immediately notify" the NYDFS of any cybersecurity incident "that has a reasonable likelihood of materially affecting the normal operation of the entity."

The eight areas of potential regulations outlined above went beyond the survey results and reports that had been issued by the NYDFS, and NYDFSFBIIC Members and other interested parties provided feedback on the regulations to the NYDFS.

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

Governor Cuomo's September 2016 press release proposing "Cybersecurity Requirements for Financial Services Companies" (the "NY Cyber Regulation")[12] described the proposed regulation as "first-in-the-nation," stating:

> New York, the financial capital of the world, is leading the nation in taking decisive action to protect consumers and our financial system from serious economic harm.... This regulation helps guarantee the financial services industry upholds its obligations to protect consumers and ensure that its systems are sufficiently constructed to protect cyber-attacks to the fullest extent possible.[13]

The revised regulation is currently subject to a 30-day notice and public comment period before final issuance, with NYDFS Superintendent Maria T. Vullo noting that only comments not received during the initial comment period will be considered before finalization. The regulation will require annual certification of compliance by any "covered entity."[14]

The NY Cyber Regulation is designed to provide "certain regulatory minimums" while not "being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances." The NYDFS recognized that many covered entities "have proactively increased their cybersecurity programs with great success," but noted that some entities had not adopted a cybersecurity program and concluded that all financial institutions must adhere to minimum standards to protect against cybercriminals. The revised version of the Regulation "requires each company to assess its specific risk profile and design a program that addresses its risk in a robust fashion."

The NYDFS concluded that all financial institutions must adhere to minimum standards to protect against cybercriminals.

The industry expressed initial encouragement that the revised NY Cyber Regulation includes a more risk focused approach than found in the initial draft.[15]

Both the September 13, 2016, draft and the revised NY Cyber Regulation generally follow the framework that was contained in the NYDFS Cyber Letter, requiring every covered entity to "establish and maintain a cybersecurity program" that takes into account the covered entity's risk assessment and that must perform the following core functions:

- Identify and assess internal and external cyber risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems.
- Use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts.
- Detect Cybersecurity Events.
- Respond to identified or detected Cybersecurity Events to mitigate any negative effects.
- Recover from Cybersecurity Events and restore normal operations and services, and
- Fulfill all regulatory reporting obligations.[16]

The NY Cyber Regulation would require the covered entity's board of directors to review the cybersecurity policy and that the cybersecurity policy be approved by a Senior Officer. Once the Regulation is effective,[17] a financial institution must review how its board addresses cybersecurity and, if not currently part of the process, will be required to ensure that the board reviews the cybersecurity policy periodically. The organization's Chief Information Security Officer ("CISO") will be required to prepare and present, at least annually, a report to the board of directors that identifies the entity's cyber risks and assesses the effectiveness of the organization's cybersecurity program.

The proposed NY Cyber Regulation addresses and provides regulatory direction as to each of the eight areas included in the NYDFS Cyber Letter. In addition to the fourteen cybersecurity coverage areas required by the proposed regulations *(see* endnote 10*)*, the NY Cyber Regulation will require "systems and network monitoring" and "risk assessment." Every cybersecurity program must include penetration testing and vulnerability assessment and include an audit trail system.

Financial institutions will also need to provide minimum necessary access privileges to users and "periodically review such access privileges." Organizations subject to the NY Cyber Regulation must employ appropriate levels of cybersecurity personnel with the required level of expertise and at least annually conduct a risk assessment of their information systems. Financial institutions must "include policies and procedures for the timely destruction of any Nonpublic Information."

Finally, the NY Cyber Regulation will generally require encryption of "all Nonpublic Information held or transmitted by the Covered Entity both in transit and at rest," however, if a company finds such encryption to be infeasible, the revised regulations permit a covered entity to take other steps to address security of its information at rest and in transit. As noted, the Vendor Management Report indicated that only 38% of respondents encrypted data at rest.

The revised NY Cyber Regulation has also been updated from the initially issued regulation to make it more risk-focused and permit each covered entity to have flexibility in the cybersecurity program it implements based on the covered entity's risk profile. For example, in addition to the encryption alternatives noted above, the revised NY Cyber Regulation also provides:

The NY Cyber Regulation would require the covered entity's board of directors to review the cybersecurity policy.

- Audit trails may be relaxed depending on the covered entity's risk assessment.
- Multi-factor authentication is no longer mandatory, depending on the covered entity's risk assessment and alternatives available to the covered entity.
- Small entities (less than 10 employees, less than $5 million in revenues or less than $10 million in assets) and some other entities are exempt, and
- Covered entities have a 180-day transitional period within which they may become compliant with the revised NY Cyber Regulation, with longer timelines that include the following:
- One year to hire a CISO, and
- Two years to comply with third party vendor requirements outlined in the NY Cyber Regulation.

WHAT FINANCIAL INSTITUTIONS/COVERED ENTITIES SHOULD BE DOING

The good news reflected in the Banking Report, Insurance Report and the Vendor Management Report is that many entities subject to the NY Cyber Regulation have already taken some significant steps to address cybersecurity risks and to protect sensitive information. However, given the "minimum standards" set forth in the NY Cyber Regulation, all entities subject to the regulation should review it carefully for the details it will require in every cybersecurity program. For any entity that has not established a cybersecurity program,[18] it must take immediate steps to implement a program that complies with the minimum standards outlined in the proposed regulation.

Any financial institution licensed or authorized in New York by the NYDFS to operate within the state will be subject to the NY Cyber Regulation; although there is a "small entity" exception[19] that will exempt only a small number of institutions from compliance. One protocol that the regulated entities must implement if the proposed regulation goes into effect is to encrypt data, or to take other steps to ensure that data is adequately protected, both at rest and in transit.[20] Regulated entities will also have to review their board of directors' interaction and communications regarding cybersecurity.

CONCLUSION

The revised NYDFS regulation is likely to go into effect and apply to Covered Entities as of March 1, 2017. NYDFS Superintendent Maria Vullo noted in her December 28, 2016, press release accompanying the revised regulations:

> New Yorkers must be confident that the banks, insurance companies and the other financial institutions that they rely on are securely handling and establishing necessary protocols that ensure the security and privacy of their sensitive personal information. This updated proposal allows an appropriate period of time for regulated entities to review the rule before it becomes final and make certain that their systems can effectively and efficiently meet the risks associated with cyber threats.

In light of the statement in the NY Cyber Regulation that "[a]doption of the program…is a priority for New York State" and the work that the NYDFS has done over the last three years assessing the current state of cybersecurity for financial institutions, the NY Cyber Regulation is likely to be adopted.[21] Other state regulators likely will follow suit once the regulation is final, given the influence that NYDFS has in the financial services sector and also based on other activity taking place in associations such as the National Association of Insurance Commissioners.[22]

The final regulation issued at the end of the 30-day notice period may reflect some limited revisions to address new concerns raised by affected financial institutions, but its adoption appears likely in 2017. All covered entities should review in detail their current cybersecurity program and policies and procedures and take steps to ensure by the various timelines beginning with March 1, 2017, they have policies and procedures sufficient to meet the requirements of the NY Cyber Regulation "minimum standards." Failure to take steps to comply with the NY Cyber Regulation may create challenges for the covered entity, which must annually certify compliance with the final regulation.

NOTES

1 September 13, 2016, Press Release, "Governor Cuomo Announces Proposal Of First-In-The-Nation Cybersecurity Regulation To Protect Consumers and Financial Institutions," available at http://www.dfs.ny.gov/about/press/pr1609131.htm.

2 NYDFS Superintendent Maria Vullo noted in a December 28th press release: "DFS carefully considered all comments submitted regarding the proposed regulation during the 45-day comment period, which ended on November 14, 2016, and has incorporated those suggestions that DFS deemed appropriate in an updated draft that will be subject to an additional final 30-day comment period. DFS will focus its final review on any new comments that were not previously raised in the original comment process." http://www.dfs.ny.gov/about/press/pr1612281.htm.

3 See "Industry Groups Encouraged by Latest Draft of New York Cybersecurity Rule," December 30, 2016, available at http://www3.ambest.com/ambv/bestnews/newscontent.aspx?AltSrc=105&RefNum=196950.

4 November 9, 2015, Memo from NYDFS acting Superintendent Anthony J. Albanese to Financial and Banking Information Infrastructure Committee (FBIIC) Members regarding "Potential New NYDFS Cybersecurity Regulation Requirements," available at https://www.manatt.com/uploadedFiles/Content/4_News_and_Events/Newsletters/BankingLaw@manatt/DFSletter.pdf.

5 The FBIIC Members include the following: Federal Reserve Board of Governors; Office of the Comptroller of the Currency; Commodities Futures Trading Commission; U.S. Department of the Treasury; Securities and Exchange Commission; Federal Deposit Insurance Commission; Federal Housing Finance Agency; Consumer Financial Protection Bureau; National Credit Union Administration; Federal Reserve Bank of New York; Federal Reserve Bank of Chicago; National Association of Insurance Commissioners; Conference of State Bank Supervisors; American Council of State Savings Supervisors; Farm Credit Administration; National Association of State Credit Union Supervisors; North American Securities Administrators Association; and, Securities Investor Protection Corporation.

6 Available at http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

7 Available at http://www.dfs.ny.gov/reportpub/dfs_cyber_banking_report_052014.pdf.

8 Available at http://www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf.

9 Available at http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf.

10 The areas are (new items in bold from September 13 draft, with one item having been deleted from the September 13th draft): (1) information security; (2) data governance and classification; (3) asset inventory and device management: (4) access controls and identity management; (5) business continuity and disaster recovery planning and resources; (6) systems operations and availability concerns; (7) systems and network security; (8) systems and network monitoring; (9) systems and application development and quality assurance; (10) physical security and environmental controls; (11) customer data

privacy; (12) vendor and third-party service provider management; (13) risk assessment; and (14) incident response.

[11] The provisions would require, among other things: (1) the use of multi-factor authentication to limit access to sensitive data and systems; (2) the use of encryption to protect sensitive data in transit and at rest; (3) notice to be provided in the event of a cybersecurity incident; (4) the indemnification of the entity in the event of a cybersecurity incident that results in loss; (5) the ability of the entity or its agents to perform cybersecurity audits of the third party vendor; and (6) representations and warranties by the third party vendors concerning information security.

[12] Available at http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

[13] http://www.dfs.ny.gov/about/press/pr1609131.htm.

[14] According to the issued regulation, a "covered entity" means "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law."

[15] See "Industry Groups Encouraged by Latest Draft of New York Cybersecurity Rule," December 30, 2016, available at http://www3.ambest.com/ambv/bestnews/newscontent.aspx?AltSrc=105&RefNum=196950.

[16] http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

[17] The proposed effective date of the NY Cyber Regulation is now March 1, 2017.

[18] From the cyber surveys and reports, the number of such entities would appear to be relatively small. However, the number of survey respondents were relatively small, so there may be a number of entities without cybersecurity programs.

[19] Only entities with "fewer than 1000 customers," "less than $5,000,000 in gross annual revenue" and "less than $10,000,000 in year-end total assets" are exempted from the NYDFS Regulation.

[20] The Vendor Management Report indicated that only 38% of respondents encrypted data at rest.

[21] The National Association of Insurance Commissioners ("NAIC") is also working on a model law, "Insurance Data Security Model Law," that addresses many of the same issues and would require insurance companies to implement many similar policies and procedures, including enhanced board of directors interaction.

[22] California regulators are working on similar regulations and the NAIC's Cybersecurity Task Force is developing an "Insurance Data Security Model Law," available in its current redlined form at http://www.naic.org/documents/committees_ex_cybersecurity_tf_exposure_mod_draft_redline.pdf.

Daniel A. Cotter is a partner at **Butler Rubin Saltarelli & Boyd** in Chicago, where he chairs the insurance regulatory and transactions practice and is a member of the cyber and privacy practice. In 2016 he obtained his CIPP/US, a certified information privacy professional designation for the U.S. private sector from the International Association of Privacy Professionals. He can be reached at dcotter@butlerrubin.com. Republished with permission.