June 28, 2018

The NY Department of Financial Services Cybersecurity Regulations: An Update

Barry R. Temkin
Kenneth M. Labbate

New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 259—NO. 124
THURSDAY, JUNE 28, 2018

Outside Counsel

Expert Analysis

The NY Department of Financial Services Cybersecurity Regulations: An Update

By **Barry R. Temkin**

And **Kenneth M. Labbate**

The New York State Department of Financial Services has promulgated 17 new cybersecurity regulations which apply to regulated entities doing business in New York. The new DFS rules apply to all entities under its jurisdiction, including insurance companies, insurance agents, banks, charitable foundations, consumer lenders, mortgage brokers, holding companies and premium finance agencies.

These regulations require encryption of all non-public information held or transmitted by the covered entity, require each regulated company to promulgate a written cybersecurity program, and appoint a chief information security officer ("CISO"), who must report directly to the board of directors and issue an annual report, setting forth an assessment of the company's cybersecurity compliance and any identifiable risks for potential breaches. See New York 23 NYCRR Section 501 et. sec..

The purpose of the new regulations is to enhance data security, and to prepare for and prevent cybersecurity attacks against financial institutions that hold confidential customer information. According its preamble, "this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities." .

With the possible exception of Massachusetts, which implemented a wide-reaching cybersecurity law in 2010, the DFS regulations are the first in the nation to require specific state-wide cybersecurity measures for an entire industry. Given New York's status as a financial center, the DFS regulations are expected to have wide-ranging effects and influence insurance and financial services practices throughout the country.

The DFS rules require each covered company to establish a comprehensive written cybersecurity policy addressing specific areas, including information security, data governance and classification, a business continuity and disaster recovery plan, systems operations and availability concerns, network security, customer data privacy, risk assessment, and related topics. The written cybersecurity policy should also contain a proposed plan of response to a potential data breach or other cyber event, which must be reviewed and approved by the board of directors and chief executive on an annual basis.

As a practical matter, compliance with the new regulations imposes some hurdles. In the first instance, determining the compliance dates of the regulations is not a simple matter. The implementation dates of these regulations are

BARRY TEMKIN *and* KENNETH LABBATE *are partners at Mound Cotton Wollan & Greengrass in New York, where their practice includes professional liability defense.*

staggered; some went into effect in 2017, others became active on March 1, 2018, and still others are being implemented on September 1, 2018. The final regulation, which requires registrants to attest to the cybersecurity practices and policies of their third-party vendors, goes into effect on March 1, 2019.

Registrants which have missed the March 2018 deadline for filing a cybersecurity plan with DFS may have received a notice of non-compliance, warning them that they should file their plans, and get to work on preparing for cybersecurity compliance. While at the time of writing, the authors have not seen any major enforcement actions by DFS, this is likely to change in the not-too-distant future.

The 17 regulations, and their compliance dates, can be summarized as follows (*see Table 1)*:

Limited partial exemptions are available for a number of regulated entities. For example, a smaller registrant with fewer than ten employees, less than $5 million in gross revenue (including affiliates) from business in New York, or less than $10 million in total assets (including affiliates) is exempt from nine of the seventeen regulatory requirements, including the need to appoint a chief information security officer, maintain an audit trail, use and hire qualified cybersecurity staff, implement multi-factor authentication, encryption or a written incident response plan. A partially exempt registrant must still file a notice of exemption and comply with the remaining regulations.

A different limited exemption is available for a risk retention group which is licensed under New York Insurance Law Section 5904, as well as a charitable annuity or a reinsurer. There is also an exemption for registrants which do not use or access non-public information.

While employees of covered entities are themselves considered covered entities under the rules, these individuals are exempt from compliance and need not develop their own cybersecurity programs to the extent they are covered by the cybersecurity programs of their employer.

In addition, covered entities which do not operate, maintain or control information systems and do not receive non-public information are exempt from 12 of the 17 specified requirements of the regulations. Non-public information is defined as business information of the covered entity, including, presumably trade secrets; personal identifying information about an individual, and any information or data regarding medical or health care treatment of an individual.

A registrant's cybersecurity program should comply with the seventeen requirements of the DFS regulations. These are summarized as followed, bearing in mind that the actual text of the regulations contains additional details. The registrant should:

1. Maintain a cybersecurity program; This may be adopted from an affiliate, and should detect and prevent cybersecurity risks, and use defensive infrastructure.
2. Prepare a written cybersecurity policy approved by a senior officer or the board. This policy should meet 14 factors outlined in the regulations, including information security, data governance and classification, asset inventory and device management, access controls, business continuity and disaster recovery planning; systems operations; systems and network security; systems and network monitoring; systems and application development and quality assurance; physical security and environmental controls; customer data privacy; vendor and third party service provider management, risk assessment and incident response.
3. Designate a Chief Information Security Officer, who should maintain cybersecurity policies and procedures and issue an annual written report to the board of directors about the firm's cybersecurity program and any lapses. The CISO may be an independent contractor or work for an affiliate. Engage in penetration testing by continuous monitoring or

by annual testing, plus biannual vulnerability assessments.
4. Engage in penetration testing by continuous monitoring or by annual testing, plus biannual vulnerability assessments.
5. Maintain an audit trail designed to reconstruct material financial transactions and designed to detect and respond to cybersecurity events.
6. Limit and periodically review access privileges.
7. Engage in periodic risk assessments designed to anticipate potential cybersecurity threats.
8. Use and train qualified cybersecurity personnel.
9. Institute written guidelines for maintaining the security of internal and external applications used by the company.
10. Prepare a written policy and procedure for third-party providers' data security, including risk assessment; minimum cybersecurity practices; periodic assessment of cyber-risk provided by third party providers; guidelines for due diligence; third parties' use of encryption and related issues.
11. Prepare written limitations on data retention.
12. Multi-factor authentication for any person accessing the company's internal networks from an external network.
13. Encryption of nonpublic information, to the extent feasible.
14. Training and monitoring of company personnel regarding cybersecurity.
15. Preparation of a written incident response plan, including internal roles, goals, remediation, etc.
16. A registrant should include notice to the superintendent in the event of a data breach.
17. Maintain the confidentiality of non-public information.

As mentioned, the DFS regulations require registrants to certify, by March 1, 2019, that third party vendors with whom they do business have adequate cybersecurity programs in effect. Of particular interest to law firms who represent financial institutions is Section 500.11 of the new DFS regulations, which requires each covered entity to "implement written policies and procedures designed to ensure the security of information systems and non-public information that are accessible to, or held by third-parties doing business with the covered entity."

> The purpose of the new regulations is to enhance data security, and to prepare for and prevent cybersecurity attacks against financial institutions that hold confidential customer information.

Thus, covered entities, including insurance companies, which provide access to personal identifying information to third-party vendors must certify not only that their own information systems are adequate, but that the information security systems of vendors with whom they do business are also secure and protected. In other words, vendors who do business with regulated financial service companies will eventually be expected to comply with the cybersecurity standards of their represented clients.

Conclusion

The New York DFS cybersecurity regulations are being implemented on a staggered schedule, with additional compliance dates scheduled for September 2018 and March 1, 2019. The requirements of the DFS regulations should be noted not only by registrants, but also by vendors who do business with them.

Registrants should act diligently to ensure their compliance with DFS cybersecurity requirements. Cybertechnology experts are expecting enforcement action from the DFS, and no company wants to be the first case.