WHITEMAN OSTERMAN & HANNA LLP
ATTORNEYS AT LAW

WOH LEGAL ALERT – FEBRUARY 28, 2017 UPDATE

FINAL CYBERSECURITY RULES FOR NEW YORK'S FINANCIAL SERVICES INDUSTRY

The Issue

New York's "first-in-the-nation" financial services cybersecurity rules have been finalized and will go into effect on **March 1, 2017**.

Who Is Affected?

The final regulations cover every business regulated by the New York State Department of Financial Services ("DFS"), including but not limited to banks, credit unions, insurers, and mortgage companies ("Covered Entities").[1] The final regulations also indirectly affect non-regulated third parties who have access to a Covered Entity's information systems and/or Nonpublic Information,[2] including but not limited to IT service providers, accountants, auditors and law firms.

Smaller covered entities (generally those with fewer than 10 employees, less than $5 million in annual revenue derived from New York business operations, or less than $10 million in total assets) are required to comply with only a portion of the regulations. A small number of entities, including those that do not have access to a Covered Entity's information systems and/or access to Nonpublic Information are not required to comply with the regulations, but must file a notice of exemption.

Compliance Dates

Covered Entities have until **August 28, 2017** to comply, although longer compliance dates are applicable to some specific provisions, as discussed below.

---

[1] The regulations define a Covered Entity as "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." 23 NYCRR § 500.01(c).

[2] For purposes of the proposed regulation, Nonpublic Information generally includes (1) business information that would have a "material adverse impact to the business, operations or security of the Covered Entity" if disclosed, accessed, tampered with or improperly used; (2) personal information of an individual that would allow identification of the individual in combination with that individual's social security number, driver's license number, account number or other sensitive information; or (3) certain individual health-related information. 23 NYCRR § 500.01(g).

Background

On September 13, 2016, DFS announced what it described as "new first-in-the-nation" cybersecurity rules that would require DFS-regulated firms "to establish and maintain a cybersecurity program designed to protect consumers and ensure the safety and soundness of New York State's financial services industry." The September 2016 proposed rules also required a Covered Entity to ensure that third parties with access to a Covered Entity's information systems and Nonpublic Information implement and follow minimum cybersecurity requirements.

The September 2016 proposed rules, which originally were scheduled to go into effect on January 1, 2017, were met with intense public criticism. While numerous aspects of the proposed rules were questioned, the main criticism concerned the conflict between the compliance-based "regulatory minimum standards" set forth in the proposed rules and "risk-based" cybersecurity models used by other regulators and standards organizations.

DFS acknowledged the criticism and, on December 28, 2016, issued revised rules that modified many provisions to allow more tailored risk-based compliance. Nonetheless, the December 2016 revised rules retained many prescriptive "regulatory minimum standards" and raised concerns that the rules remain focused more on compliance than security.

DFS provided a new notice and comment period following issuance of the December 2016 revised rules. DFS received additional comments, but few changes have been made in the final rules. The principal changes involve modification of the exclusions from coverage, including minor expansion of the small business limited exemption and creation of a new exemptions for captive insurance companies, charitable annuity societies, out-of-state risk retention groups, and certain reinsurers that do not have other operations that would make them Covered Entities.[3]

The final regulations create three principal compliance tiers: (1) all non-exempt DFS-regulated entities;[4] (2) large covered entities; and (3) third party service providers.

The first tier sets a minimum baseline for cybersecurity compliance. The second (more burdensome) tier applies only to large Covered Entities, which includes entities with: (1) 10 or more employees; (2) $5 million or more in gross annual revenue derived from New

---

[3] 23 NYCRR § 500.19(d) and (f).

[4] Certain entities are exempted from the regulation, including: (1) covered entities covered by the cybersecurity plan of another covered entity (i.e., employees, agents and representatives of covered entities); (2) Covered Entities that do not handle nonpublic information, such as personal information of customers (except such entities must still complete a risk assessment); and (3) the newly added exemption for captive insurance companies, charitable annuity societies, out-of-state risk retention groups, and reinsurers covered by 11 NYCRR §125 that are not also Covered Entities. 23 NYCRR § 500.19 (c), (d) and (f).

York business operations in each of the last three fiscal years;[5][5] and (3) $10 million or more in year-end total assets. The third tier affects third party service providers, but only indirectly. Under the final regulations, Covered Entities are responsible for confirming that the third party's cybersecurity protections are sufficient before providing access to the Covered Entity's information systems and nonpublic information.

Summary of Provisions Applicable to Non-Exempt Covered Entities

The following provisions apply to all non-exempt DFS-regulated entities, regardless of size.

- ***Implement a cybersecurity program*** that is "designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems." 23 NYCRR § 500.02.

- ***Create a written cybersecurity policy*** approved by a senior officer or board of directors that sets forth the Covered Entity's policies and procedures for protecting its information systems and Nonpublic Information based on the organization's "Risk Assessment." 23 NYCRR § 500.03.

- ***Limit user access privileges to Nonpublic Information*** and periodically review those access privileges. 23 NYCRR § 500.07.

- ***Perform a periodic risk assessment*** to evaluate the effectiveness of the Covered Entity's cybersecurity program, which "shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations." 23 NYCRR § 500.09.

- ***Develop a third-party service provider security policy*** to ensure third parties will provide adequate security for the Covered Entity's information systems and Nonpublic Information. 23 NYCRR § 500.11.

- ***Securely dispose of Nonpublic Information*** when no longer needed for legitimate business purposes, unless the information is otherwise required to be retained by law or regulation or it is not feasible to dispose of such information. 23 NYCRR § 500.13.

- ***Mandatory reporting of cybersecurity events within 72 hours*** that "have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity" or where notice is required to be provided to another government body, self-regulatory agency or any other supervisory body. 23 NYCRR § 500.17.

---

5 This provision has been changed. Originally, the $5 million exemption applied to an organization's total revenue. As a result of this change, more out-of-state entities will qualify for the small business limited exemption.

- ***Annual certification of compliance*** covering the prior calendar year to be filed with DFS on or before February 15 of each year. 23 NYCRR § 500.21.

Summary of Provisions Applicable Only to Large Covered Entities

In addition to the provisions described above, DFS-regulated Covered Entities that do not qualify for the small firm limited exception also are required to comply with the following provisions:

- ***Appointment of a qualified individual to perform the functions of a Chief Information Security Officer ("CISO")*** responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy. Formal designation of a person with the title "CISO" is not required and the CISO function may be performed by any qualified person in the organization or may be outsourced. 23 NYCRR § 500.04.

- ***Monitoring, testing and/or vulnerability assessments*** to detect threats and vulnerabilities to the Covered Entity's information systems. 23 NYCRR § 500.05.

- ***Maintenance of audit trails and other records*** that allow for the reconstruction of all material financial transactions and allow the organization to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the organization's normal operations. 23 NYCRR § 500.06.

- ***Development of application security guidelines*** to ensure use of secure development practices for internally developed applications and for assessing and testing the security of externally developed applications. 23 NYCRR § 500.08.

- ***Employ and train cybersecurity personnel*** to fulfill core cybersecurity functions for the organization. This requirement can be satisfied through internal resources or outsourcing arrangements. 23 NYCRR § 500.10.

- ***Utilize "effective controls" for access to non-public information*** including multi-factor authentication where appropriate or necessary based on the organization's risk profile. 23 NYCRR § 500.12.

- ***Risk-based monitoring*** of the entity's authorized users to detect unauthorized access, use or tampering with Nonpublic Information. 23 NYCRR § 500.14.

- ***Cybersecurity awareness training*** for all organization personnel that is updated to reflect risks identified by the organization's risk assessment. 23 NYCRR § 500.14.

- ***Utilize encryption*** or "alternative compensating controls" for protection of Nonpublic Information in transit and at rest. 23 NYCRR § 500.15.

- ***Create a written incident response plan*** designed to allow a Covered Entity to promptly respond to and recover from any material cybersecurity event "affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations." 23 NYCRR § 500.16.

Key Components of the Proposed Revised Rules Affecting Third Party Service Providers

Non-regulated third parties are indirectly affected by the proposed regulations, because DFS-regulated Covered Entities must ensure that the third parties with whom they contract have adequate cybersecurity protections.

Third parties that deal with Covered Entities' information systems or Nonpublic Information likely will be required to comply with contractual provisions requiring them to meet many of the minimum cybersecurity requirements set forth in the final regulations, including but not limited to (1) access controls; (2) encryption; and (3) notice of cybersecurity events.

Third Parties that fail to meet these requirements in advance may find themselves at a significant competitive disadvantage in bidding for new business with Covered Entities.

Compliance Deadlines and Certification

The final regulations require compliance with most provisions within 180 days from final adoption **(August 28, 2017)**, with longer compliance periods for some provisions as follows:

- ***One year (March 1, 2018):*** report to the board or other governing body; monitoring, penetration testing and/or vulnerability assessments; risk assessment; multi-factor authentication (or other effective controls); and cybersecurity awareness training for staff.

- ***Eighteen months (September 1, 2018):*** audit trails; application security policies; limits on data retention; risk-based monitoring; and encryption of Nonpublic Information (or implementation of other effective controls).

- ***Two years (March 1, 2019):*** implementation of a third party service provider policy.

Enforcement

The final regulations give the DFS superintendent enforcement discretion under the various laws granting DFS's general enforcement authority. The regulations do not provide any specific penalty ranges or any indication as to how DFS intends to enforce the regulation once it goes into effect.

Conclusion

180 days will go quickly and all organizations should review the regulations and address any shortcomings in their cybersecurity programs as soon as possible.
The impact of these regulations on individual Covered Entities will vary greatly. Some organizations already have robust cybersecurity compliance programs in place; other organizations will be starting from scratch. In addition, uncertainty remains due to the fact that the standards for compliance and the potential penalties for noncompliance have not been clearly defined.

Over the next few weeks, we will be providing additional in-depth analysis of individual provisions that are likely to create questions or compliance concerns for covered entities.

Contact

Chris Meyer, cmeyer@woh.com, 518-487-7712, or any other Whiteman Osterman & Hanna LLP attorney.