New York Issues Proposed Cybersecurity Regulations That Could Set a New Standard

November 01, 2016

On September 13, 2016, the New York State Department of Financial Services (NYDFS) issued a press release announcing a proposed cybersecurity regulation (Proposed Regulation) that will require covered entities to design a cybersecurity program that addresses their risks "in a robust fashion." Proposed 23 NYCRR Part 500. Although the Proposed Regulation contains requirements similar to those found in existing guidance from the Federal Financial Institutions Examination Council, it goes much further with its prescriptive requirements.

The Proposed Regulation is subject to a 45-day notice and public comment period that ends November 12, 2016. The Proposed Regulation would become effective as-proposed on January 1, 2017, but it provides for a 180-day transitional period for covered entities to come into compliance.

In contrast to existing cybersecurity frameworks, the Proposed Regulation is highly prescriptive in nature. Unless revised before being finalized, it will be extremely difficult for financial institutions to implement a cybersecurity program that complies with all of the Proposed Regulation. Compliance with the third-party requirements will be particularly difficult. Since the NYDFS currently requires that applicants for licensure submit policies and procedures in connection with their applications, applicants should anticipate that they will need to submit their cybersecurity policies as a part of the licensing process.

It is also likely that other states will follow New York and issue their own cybersecurity regulations. This rulemaking could very well result in a landscape of varying and conflicting state cybersecurity regulations similar to the patchwork of data breach notification requirements that financial institutions currently face.

Scope

The Proposed Regulation generally applies to 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." There is a partial exemption for smaller regulated entities.

Requirements

The Proposed Regulation establishes several onerous requirements for covered entities. Among other things, the requirements include the following:

***Cybersecurity Program*.** Covered entities must establish a cybersecurity program designed to ensure the confidentiality, integrity, and availability of the covered entity's information systems. The program must be able to identify internal and external threats, use defense infrastructure to protect the covered entity, detect and respond to cybersecurity events, and recover from cybersecurity events.

***Cybersecurity Policy*.** Covered entities must implement a cybersecurity policy addressing how the covered entity protects its information systems and nonpublic information stored on those systems. The policy must be reviewed and approved annually by the covered entity's board of directors. The policy must, at a minimum, address the following:

- Information security;
- Data governance and classification;
- Access controls and identity management;
- Business continuity and disaster recovery planning and resources;
- Capacity and performance planning;
- Systems operations and availability concerns;
- 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.

***Chief Information Security Officer*.** Covered entities must designate a Chief Information Security Officer ("CISO") to oversee and implement the cybersecurity program and enforce the cybersecurity policy. The CISO is required to provide the board of directors with a biannual report assessing the confidentiality and integrity of the covered entity's information systems, assessing the effectiveness of the covered entity's cybersecurity program and policies, and summarizing all cybersecurity events that occurred during the time period covered in the report.

***Third-Party Information Security Policy*.** Covered entities must establish written policies and procures designed to ensure the security of information systems and nonpublic information that is accessible to, or held by, third parties doing business with the covered entity. At a minimum these policies must establish cybersecurity practices to be followed by third parties and provide for periodic cybersecurity risk assessments of third parties. In addition, covered entities must include certain "preferred provisions" in their third-party contracts. These include provisions for the following:

- Multifactor identification;
- Encryption;
- Breach notification systems;
- Availability of identity protection services for customers impacted by the third-party service provider's negligent or willful conduct;

- Representations and warranties that service or product provided to the covered entity is free of mechanisms that would compromise the security of the covered entity's information systems or nonpublic information; and
- Authorization for covered entity to perform cybersecurity audits on third-party service provider.

***Incident Response Plan and Reporting*.** Covered entities must notify NYDFS within 72 hours of the discovery of "cybersecurity event" that either compromises nonpublic information (including unauthorized access of such information) or is likely to materially affect the business. In addition, covered entities must establish a written incident response plan to respond to cybersecurity events.

***Data Encryption*.** Covered entities must encrypt all nonpublic information held or transmitted by the covered entity both in transit and at rest. The encryption requirements for in-transit data must be met by January 2018, while compliance for at-rest data must be met by January 2022. However, prior to those dates, NYDFS expects that organizations secure nonpublic information using alternative controls that have been reviewed and approved by the CISO.

***Penetration Testing and Vulnerability Assessments*.** Covered entities must perform annual penetration tests and quarterly vulnerability assessments.

***Audit Trails*.** Covered entities must track and maintain audit trails for certain data with logs maintained for 6 years.

***Annual Certifications*.** A covered entity's senior officer must submit an annual certification to the NYDFS stating that the entity is complying with the Proposed Regulation's requirements. This requirement would begin in January 2018.

Limited Exemption

There is a limited exemption for entities that have: (1) fewer than 1,000 customers in each of the three preceding calendar years; (2) less than $5 million in gross annual revenue in each of the three preceding fiscal years; and (3) less than $10 million in year-end total assets (including affiliate assets).

Entities qualifying for this limited exemption are still required to implement several of the Proposed Regulation's provisions, including establishing a cybersecurity program and policy, conducting risk assessments, vetting third-party information security practices, and providing notices of cybersecurity events to the NYDFS.