Client Alert: New York Department of Financial Services Proposed Cybersecurity Regulation: Comment Period Open Until November 12

Related Attorneys

Scott M. Guttman

Related Services

Data Strategy, Privacy and Security

Litigation

Related Industries

Financial Institutions

CLIENT ALERT | 10.10.2016

Recently, the New York State Department of Financial Services (NYDFS) published its "first-in-the nation cybersecurity regulation" to impose cybersecurity requirements on NYDFS regulated entities such as banks, consumer lenders, money transmitters, insurance companies and other financial service providers. The draft regulation is open for comment until November 12, 2016, and, unless modified as a result of the comments, will become effective January 1, 2017. Entities subject to this cybersecurity regulation will have 180 days thereafter to comply with the final regulations. Given New York's importance in the financial services industry, this regulation may serve as a template for other state regulators aimed at protecting consumers and financial institutions.

Covered Entities

The proposed regulation applies to any entity "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" and, therefore, covers a broad range of entities in the banking, insurance and financial services industries, including insurance producers and premium finance companies (each a covered entity). However, the draft regulation provides an exemption for certain smaller entities that may otherwise have difficulty complying with some aspects of the law, such as the requirement to appoint a Chief Information Security Officer (CISO). This limited exemption applies to entities with: (1) fewer than 1,000 customers in each of the last three calendar years; (2) less than US$5,000,000 in gross annual revenue in each of the last three fiscal years; and (3) less than US$10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates.

Cybersecurity Program

For covered entities, the regulation requires establishment of a cybersecurity program that ensures the confidentiality and integrity of information systems. The new cybersecurity program must address the

following:

- identification of cyber risks;
- implementation of policies to prevent unauthorized access/use or malicious activity;
- detection of cybersecurity events, response to and mitigation of cybersecurity events; and
- recovery from restoration to normal operations following cybersecurity events.

Covered entities must also employ cybersecurity personnel to manage the cybersecurity program, and these persons must undergo training to stay abreast of cybersecurity threats and best practices. Further, covered entities must provide all personnel with cybersecurity training targeting threats and best practices, and establish written incident response plans that address internal processes for responding to cybersecurity events, provide clear roles and levels of decision-making, and external and internal communications and information sharing.

Cybersecurity Policies

Covered entities must adopt written cybersecurity policies that outline their cybersecurity programs. At a minimum, the written policies must address: 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. The board of directors or a senior officer is responsible for the cybersecurity program, and must review the cybersecurity program at least annually.

Appointment of CISO

A CISO must be appointed or designated by each covered entity. The CISO will be responsible for overseeing the entity's cybersecurity program and enforcing its cybersecurity policies. As part of his or her duties, the CISO will be required report bi-annually to the board of directors about threats or vulnerabilities to the network, and this report must include:

- the confidentiality and integrity of the entity's information systems;
- the entity's policies and procedures;
- the cybersecurity risks;
- the effectiveness of the entity's cybersecurity program;
- the incident response and remediation plans; and
- a summary of any cyber events during the reporting period.

Moreover, the CISO is required to conduct penetration testing on an annual basis to identify vulnerabilities to the entity's network security systems, and must also conduct vulnerability testing on a quarterly basis.

Limited Access

The draft regulation requires limited access to information and systems. For example, covered entities will be required to limit access to nonpublic information solely to those persons who require such access to perform their jobs. They will also be required to conduct due diligence on their third-party providers' policies and procedures to assess the risk accompanying utilization of those third parties. The regulation requires "multi-factor authentication" for any person accessing the entity's internal systems or data from an external network and for privileged access to database servers that allow access to nonpublic information. Moreover, covered entities will be required to monitor their authorized users' activity and detect unauthorized access, use or tampering with nonpublic information.

Cybersecurity Event Reporting

The draft regulation also contains a potentially burdensome notification requirement, requiring notification to the superintendent of any attempt or attack, whether or not successful, "that has a reasonable likelihood of materially affecting the normal operation" of the covered entity or affecting nonpublic information within 72 hours after the regulated entity becomes aware of the event. Any notice the covered entity provides to any government or self-regulatory agency must also be given to the superintendent. This 72 hour timeline may force covered entities to provide notice before gaining a full understanding of the event or the nature of the data involved in the event.

Annual Certification

Beginning Jan. 15, 2018, entities subject to the cybersecurity regulation are required to have the chair of the board (or other senior officer where the entity has no board) certify in writing that that the entity is in full compliance with the draft regulation to the superintendent. In addition to this certification, a written report that details all remedial efforts planned or underway and all attempts or attacks that occurred in the prior year requiring reporting to the superintendent must be provided. All records that support the certification must be maintained for at least five years and made available to the superintendent upon request.

Conclusion

In some regards, the draft regulation is consistent with cybersecurity principles and requirements set forth by other regulators such as the Cybersecurity Assessment Tool released by the Federal Financial Institutions Examination Council and the Cybersecurity Framework released by the National Institute of Standards and Technology, as well as industry standards like the Payment Card Industry Data Security Standard. However, the draft regulation contains a level of detail beyond what other regulators have required. For example, it defines the term "nonpublic information" broadly to include any information that would be considered nonpublic personal information under the Gramm-Leach-Bliley Act or its regulations. This means that more information is subject to the regulation than "personal information" as defined under existing New York laws. Its requirement that this broad category of data be encrypted at rest as well as in transit may pose compliance challenges to many covered entities. Moreover, since the regulation requires notification to the superintendent of any cybersecurity event that affects nonpublic information or its operations, covered entities will likely need to report events that are otherwise not reportable under

New York law. Given the current Jan 1, 2017 effective date and 180 day compliance period thereafter, entities subject to this regulation should start evaluating their cybersecurity programs and policies for compliance with the regulation.