What You Must Know about New York's Proposed Cybersecurity Regulation for the Banking, Insurance, and Financial Services Sectors

CONSUMER FINANCE | CYBERSECURITY AND PRIVACY | TECHNOLOGY | SEPTEMBER 20, 2016


Steven Blickensderfer


Nora A. Valenza-Frost


Joseph W. Swanson

Last week, New York's Department of Financial Services released its long-awaited proposed cybersecurity regulation, which promises to deliver sweeping protections to consumers and financial institutions alike. The proposed regulation, titled "Cybersecurity Requirements for Financial Services Companies" (23 NYCRR Part 500), if implemented, would be a first-of-its-kind state provision that creates mandatory cybersecurity and risk management regulations for companies in the banking, insurance, and financial services industries licensed in New York. The proposed regulation would take effect January 1, 2017, and will be open for public comment for 45 days beginning September 28, 2016. Given New York's prominence in the financial services sector, other states are likely to follow its lead in promulgating similarly sweeping regulations.

Background. The proposed regulation arose out of surveys of regulated banking institutions and insurance companies the Department conducted in recent years.

Based on those surveys' findings, the Department identified five key elements of cybersecurity programs, all of which can be seen in the proposed regulation: (1) a written information security policy; (2) security awareness and education and training for employees; (3) information security audits; (4) risk management of cyber risk (including the identification of key risks and trends); and (5) incident monitoring and reporting.

Here's what you need to know about New York's proposed cyber regulation.

Scope. The proposed regulation is broad in scope. It applies to *any individual* or *entity* operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under New York banking, insurance, or financial services laws, subject to certain limited exemptions for smaller entities. Smaller entities – which the regulation defines as having (1) fewer than 1,000 customers in each of the last three calendar years; (2) less than $5 million in gross annual revenue in each of the last three fiscal years; and (3) less than $10 million in year-end total assets as calculated by GAAP – are still expected to comply with many of the regulation's requirements.

The broad scope of the proposed regulation continues with its definition of "nonpublic information," which is defined to include *any information* that an individual provides to a covered entity in connection with seeking or obtaining a financial product or service.

Cybersecurity Program. The proposed regulation's primary purpose is to ensure that all companies, large and small, in the banking, insurance, and financial services industries have a cybersecurity program in place. While an increasing number of companies already do, the proposed regulation makes this mandatory across-the-board and requires it to be in writing. Among the requirements, the proposed regulation requires companies to have a program that achieves the following:

- identifies internal/external cybersecurity risks;
- uses defensive infrastructure to protect covered information;
- detects "cybersecurity events" such as a breach; and

- fulfills regulatory reporting obligations.

Third Parties. If a company uses a third party to handle its information systems or retain its data, the proposed regulation further obligates the third party to ensure that certain minimum cybersecurity practices are being met. This includes mandatory periodic assessments and requiring third parties to have written policies that, in some instances, may include warranties that the entity is free from viruses and other security vulnerabilities.

Chief Information Security Officer. For larger companies, the proposed regulation will require the designation of a Chief Information Security Officer (CISO), who will be tasked with implementing, overseeing, and enforcing the cybersecurity program. In particular, the CISO will review the cybersecurity policy annually and bi-annually report on the program to the company's governing body. Again, while such reporting mechanisms may already be in place at some companies, the proposed regulation will make this standard.

Multi-Factor Authentication & Encryption. Until now, multi-factor authentication has generally been a best-practice, not a requirement. The proposed regulation would require large companies to use multi-factor authentication for access to internal systems or data from an external network or to servers that contain nonpublic information, as well as risk-based authentication for individuals accessing web applications that contain the same. The proposed regulation likewise requires encryption for all nonpublic information, with limited exceptions.

Limits on Data. Another key provision of the proposal is its limit on data retention. Companies subject to the regulation will be required to destroy all nonpublic information that is no longer necessary for the provision of products and services for which the information was originally provided.

App Development. The proposed regulation also encompasses app security, requiring companies to ensure the use of secure development practices for in-house developed apps.

Reporting & Certification Requirement. When a "cybersecurity event" such as a breach occurs, the proposed regulation requires companies to notify the Department within 72 hours. The regulation further requires companies certify to the Department annually that their cybersecurity programs are in compliance and maintain all supporting documentation for a five-year period.

Staff & Training. The proposed regulation further requires companies to employ cybersecurity personnel to manage the program, as well as to provide for mandatory and regular cybersecurity education and training.

The Takeaway. New York's proposed cybersecurity regulation is consistent with the shift toward greater regulation in the cybersecurity space, particularly for the financial services sector. As previously discussed (here), the Federal Financial Institutions Examination Council recently issued similar-sounding guidelines to help examiners evaluate the risk management and mitigation processes of financial institutions and third-party service providers. New York's proposed regulation, however, would be different because it is mandatory.

For some ahead-of-the-curve companies, this "new" cybersecurity regulation may not seem all that new. But for most, the imposition of its mandatory cybersecurity standards, including the designation of a CISO and ongoing staff training and education, may have significant cost implications that may require advanced discussion and planning.

Indeed, the biggest impact of the regulation may be felt on smaller entities that, unlike their larger counterparts, do not already have many of these policies and procedures in place. Under the new regulation, smaller entitles will still be required to have a cybersecurity program and written policy in place, limit access privileges to nonpublic information, conduct annual risk assessments, and comply with the notices and certification requirements.

Further, the broad definition of nonpublic information, data limit regulation, and mandatory multi-factor authentication may require some companies to reassess their existing data storage and retention policies. What’s more, because New York is considered a leader for the financial services industry, this regulation may be a harbinger of things to come for other states as well.