Cooley

New York Wants Its Cybersecurity Regulation to Reach Nationwide

April 13, 2017

On April 9, 2017, Maria Vullo, the New York Department of Financial Services (NYDFS) superintendent, pronounced to state insurance commissioners that New York's new cybersecurity regulation could be the model for other states.

The new cybersecurity regulation went into effect on March 1 and requires certain financial services companies licensed under New York law, including insurance companies, to maintain a robust cybersecurity program. This mandate applies far and wide to a range of licensed entities. Various commenters have expressed concerns over how burdensome the requirements can be for small businesses. Notwithstanding this objection, Superintendent Vullo expressed that states should have a "consistent framework" and the "New York regulation is a road map with rules of the road."

As cybersecurity regulation advances at the state level, we summarize the coverage and basic requirements of the New York regulation, which may stretch nationwide if other states agree with the NYDFS.

Who is covered

In New York, the new regulation splits the world of regulated entities into "Covered Entities" and "Non-Exempt Covered Entities."

A Covered Entity is 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." This means licensed insurance companies, money transmitters, virtual currency companies, lenders and other licensed entities under those laws must abide by the cybersecurity requirements.

A Non-Exempt Covered Entity means a company with:

- 10 or more employees (including independent contractors),
- $5,000,000 or more in gross annual revenue (for the past three fiscal years from New York business operations) and
- $10,000,000 or more in year-end total assets (calculated using generally accepted accounting principles, excluding assets of affiliates).

Most entities licensed in New York would not meet these criteria. For those that do, the regulation imposes stringent requirements such as penetration testing on an annual basis, vulnerability assessments on a quarterly basis, use of multi-factor authentication, hiring of a chief information security officer, encryption of specific data and development of a written incident response plan.

What is required

For the majority of licensed entities, the regulation requires companies to establish and maintain a cybersecurity program that has a written cybersecurity policy and a third-party information security policy.

It also requires Covered Entities to limit access privileges to information systems that provide access to nonpublic information. This would require determining who should and should not have access to nonpublic information and tiering that access. Companies subject to the regulation would also have to perform a periodic risk assessment and develop policies and procedures for the secure disposal of nonpublic information no longer necessary for business operations.

In addition, these companies would have to notify NYDFS within 72 hours if certain cybersecurity events occur.

Implications

The regulations place the highest burdens on Non-Exempt Covered Entities, which covers the larger financial institutions licensed in New York. However, it reaches beyond those large institutions to cover the smallest licensed outfits, including startups with thin operating budgets. Many requirements may prove overly burdensome for new entities operating in New York, as compliance often presents an unexpected and expensive line item on the budget.

For any questions regarding the new rules in New York, please reach out to one of the attorneys listed here. We encourage you to read the **New York regulation**.