MINTZ

New York Proposes First-Ever Cybersecurity Regulation for Financial Institutions

September 19, 2016 | Blog | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

The New York Department of Financial Services recently announced a new proposed rule, which would require financial institutions and insurers to implement strong policies for responding to cyberattacks and data breaches. Specifically, the rule would require insurers, banks, and other financial institutions to develop detailed, specific plans for data breaches; to appoint a chief privacy security officer; and to increase monitoring of the handling of customer data by their vendors.

Until now, various regulators have been advancing similar rules on a voluntary basis. This is reportedly the first time that a state regulatory agency is seeking to implement mandatory rules of this nature.

"New York, the financial capital of the world, is leading the nation in taking decisive action to protect consumers and our financial system from serious economic harm that is often perpetrated by state-sponsored organizations, global terrorist networks, and other criminal enterprises," said New York Governor Cuomo. He added that the proposed regulation will ensure that the financial services industry upholds its commitment to protect customers and take more steps to prevent cyber-attacks.

The rule would go into effect in 45 days, subject to notice and public comment period. Among other detailed requirements, it will mandate a detailed cybersecurity program and a written cybersecurity policy. While larger financial institutions already likely have such policies in place, the rule puts more pressure on them to fully comply. It also mandates the hiring of a Chief Privacy Officer at a time when privacy professionals are already in a very high demand. To attract top talent, the financial institutions will need to allocate appropriate budgets for such hiring.

Additionally, the rules outline detailed requirements for the hiring and oversight of third-party vendors. Regulated entities who allow their vendors to access nonpublic information will now have to engage in appropriate risk assessment, establish minimum cybersecurity practices for vendors, conduct due diligence processes and periodic assessment (at least once a year) of third-party vendors to verify that their cybersecurity practices are adequate. More detailed specifications can be found **here**. Other requirements include employment and training of cybersecurity personnel, timely destruction of nonpublic information, monitoring of unauthorized users, and encryption of all nonpublic information. As DFS Superintendent Maria Vullo explained: "Regulated entities will be held accountable and must annually certify compliance with this regulation by assessing their specific risk profiles and designing programs that vigorously address those risks."

Among other notable requirements, the regulations further mandate that banks notify New York's Department of Financial Services of any material data breach within 72 hours of the breach. The regulations come at the time when cybersecurity attacks are on the rise. The proposed rules also follow on the heels of recent legislative initiatives in 4 other states to bolster their cybersecurity laws, as we previously **discussed**.

The regulations are sweeping in nature in that they potentially affect not only New-York-based companies but also insurers, banks, and financial institutions who conduct business in New York or have customers who are New York residents. If you are unsure about your company's obligations and the impact of the proposed rules on your industry, contact Mintz Levin privacy team for a detailed analysis.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.