Articles + Publications | September 15, 2022

New York Department of Financial Services Looks to Raise the Floor — Again — on Cybersecurity Regulation

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Alexander R. Cox

Already considered among the most rigorous cybersecurity requirements for financial services companies, the existing New York Department of Financial Services ("NY DFS") Cybersecurity Regulation (the "Regulation") set the standard for a scalable and prescriptive framework for cybersecurity. Its provisions inspired the various state insurance data security requirements of other states, and the new updates to the Federal Trade Commission's Safeguards Rule promulgated under the Gramm-Leach-Bliley Act. On July 29, 2022, NY DFS proposed draft updates to the Regulation that incorporate the following big-picture changes:

- New rules for large companies (2,000+ headcount or over $1 billion in revenue);
- New expertise requirements for company boards and engagement requirements from senior leadership;
- New penalties and enforcement tools for the NY DFS;
- New ways to certify to "non-compliance" to avoid the not-quite-compliant issue;
- New compliance requirements for everyday security such as risk assessment requirements and requirements to inventory assets; and
- New notification requirements expanding to ransom payments, deployment of ransomware, and unauthorized access to certain privileged accounts.

These updates will both clarify existing issues with the Regulation, and generally raise the bar for compliance. Unlike the existing Regulation, these changes substantially ramp up the "mandatory" sections of the Regulation and make it less scalable for smaller covered entities. This is mitigated to an extent by many of the most stringent new requirements only being applicable to large companies, but many small shops will need to make a serious reinvestment in their cybersecurity programs to meet and document compliance with the new standards.

Once the proposed rule is published in the New York State Register, there is a 60-day comment period, after which the amendment will become effective following the publication of the Notice of Adoption in the State Register. After that publication, covered entities will have a 180-day grace period before the new requirements kick in. That being said, NY DFS has specifically carved out changes to the cybersecurity event notice requirements, so that they are required much more quickly at only 30 days after the amendment's effective date. On the other hand, the new requirements for large companies to implement sophisticated monitoring tools in 500.14(b), the new mandatory requirement for multi-factor authentication with privileged accounts in 500.12(c), and new password requirements in 500.7(b), will all be given a year-long grace period from the effective date of the final rule.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber