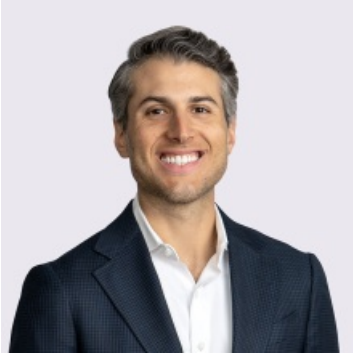
Legal Update Article

New York's Department of Financial Services Moves to Further Bolster Cybersecurity Requirements

By Damon W. Silver & Melissa Pascualini

December 11, 2024

Meet the Authors



Damon W. Silver
Principal
(212) 545-4063
Damon.Silver@jacksonlewis.com

Melissa Pascualini
Associate
631-247-4676
Melissa.Pascualini@jacksonlewis.com

Related Services

Financial Services
Privacy, Data and Cybersecurity

The New York Department of Financial Services (DFS) has been increasingly active in enforcing the rigorous cybersecurity requirements imposed on "covered entities" under 11 NYCRR Part 500 (Reg 500). DFS has published an updated proposal for amendments to Reg 500 with new obligations.

Reg 500 has broad application, covering entities "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."

In addition to expanding or modifying the obligations imposed on all covered entities, the proposed amendments would subject "Class A Companies" to heightened requirements. "Class A Companies" are those that, over the past two fiscal years and inclusive of affiliates, had (a) at least $20 million in New York-based gross annual revenue, and (b) either an average of 2,000 employees or over $1 billion in global gross annual revenue.

The proposed amendments would impose a number of new or modified requirements on covered entities relating to, among other things:

- The responsibilities of a covered entity's chief information security officer and "senior governing body" (*e.g.,* board of directors);
- Cyber risk assessments;
- Penetration testing and vulnerability assessments;
- Cybersecurity policies and procedures, including those addressing data retention, end-of-life management, remote access, security awareness and training, systems and application security, access privileges, multi-factor authentication, and encryption;
- Asset inventories;
- Business continuity and disaster recovery (BCDR) plans;
- External reporting requirements, including reporting of unauthorized access to privileged accounts, ransomware events (including a detailed justification for making ransom payments), and service provider incidents; and
- Annual certification of compliance.

Additional requirements would apply to Class A Companies. For instance, these companies would need to subject their cybersecurity programs to independent audits at least annually, monitor privileged account access activity and implement privileged access management solutions, utilize endpoint detection and response solutions, and maintain heightened password controls.

The proposed amendments also would expand the enforcement provision by clarifying that a single act, or failure to act, constitutes a violation.

Once the amendments are adopted, covered entities will generally have 180 days to comply with the updated requirements, although there will be alternative transition periods for cybersecurity event notification and annual compliance certification (30 days after adoption); incident response and BCDR planning, governance, and encryption (one year); vulnerability scanning, password controls, and enhanced monitoring controls for Class A Companies (18 months); and asset inventory and multi-factor authentication (two years).

Jackson Lewis' Financial Services and Privacy, Data and Cybersecurity groups will continue to track this development. Please contact a Jackson Lewis attorney with any questions.