New York Cybersecurity Regulation Amended and Expanded

December 08, 2023

On November 1, 2023, the New York Department of Financial Services (NYDFS) adopted amendments to its Cybersecurity Regulation, 23 NYCRR Part 500 (Cybersecurity Regulation). This is the second amendment (Amendment) to its Cybersecurity Requirements for Financial Services Companies, which adds and expands requirements for "covered entities" regulated under the NYDFS' existing cybersecurity regime. The Amendment follows the proposed amendments to the Cybersecurity Regulation that NYDFS issued a year ago on November 9, 2022, and is the most significant expansion since its enactment in 2017.

By way of background, a "covered entity" is defined under the Cybersecurity Regulation and the Amendment to mean "any person operating or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the [NY] Banking Law, the [NY] Insurance Law or the [NY] Financial Services Law **regardless of whether the covered entity is also regulated by other government agencies.**" Note that the Amendment adds the bolded clarifying language.

Reporting Requirements: Expanding and Clarifying Scope

The Amendment expands and clarifies the scope of the requirement for covered entities to report certain cybersecurity events to NYDFS. Prior to the Amendment, the cybersecurity regulations required a covered entity to report a "cybersecurity event" to the New York Superintendent of Financial Services no later than 72 hours after a determination of an event has occurred. The Amendment retains the 72-hour reporting timeline but adds that the notification must be made electronically through the New York NYDFS website.

New Term: Cybersecurity Incident

The Amendment creates a newly defined term, "cybersecurity incident," and ties the reporting requirement to this term rather than to a "cybersecurity event." Under the Amendment, a "cybersecurity incident" means "a cybersecurity event that has occurred at the covered entity, its affiliates, or a third-party service provider that:

1. impacts the covered entity and requires the covered entity to notify any government body, self-regulatory agency, or any other supervisory body;
2. has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity; or

3. results in the deployment of ransomware within a material part of the covered entity's information systems."

The Amendment retains the prior definition for a "cybersecurity event," but the reporting requirement now only applies to a cybersecurity incident. The Amendment also adds an ongoing obligation to provide NYDFS with any material change or new information associated with the cybersecurity incident that was previously unavailable. Further, the Amendment extends the reporting obligation to include cybersecurity incidents that occur at a covered entity's affiliates or a third-party service provider.

Additional Compliance: Senior Governing Body

The Amendment also creates additional compliance obligations for covered entities, including a requirement for the covered entity to have a "senior governing body" to provide oversight of the covered entity's cybersecurity risk management. The senior governing body must have a sufficient understanding of cybersecurity-related matters and develop, implement, and maintain the covered entity's cybersecurity risk management program. Further, the senior governing body is obligated to receive timely reports of material cybersecurity issues from the entity's Chief Information Security Officer (CISO).

Additional Compliance: Miscellaneous

The Amendment also supplements existing compliance requirements, including those related to written policies and procedures, vulnerability management, passwords, multi-factor authentication, asset management and data retention, ongoing monitoring, and encryption of nonpublic information.

New Category: Class A Companies

The Amendment also creates a new category of covered entities, "Class A companies," which have enhanced compliance requirements. A "Class A company" is a company that has at least $20,000,000 in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and the business operations in New York of the covered entity's affiliates and either: (a) has over 2,000 employees averaged over the last two fiscal years, or (b) has over $1,000,000,000 in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and all of its affiliates no matter where located.

Class A companies are subject to all the compliance obligations applicable to covered entities but also are required to:

(1) design and conduct independent audits of their cybersecurity program based on their risk assessments;

(2) monitor privileged access by implementing both "a privileged action management solution" and "an automated method of blocking commonly used passwords" for "all accounts" on company systems and "all other accounts wherever feasible"; and

(3) implement "an endpoint detection and response solution to monitor anomalous activity," including but not limited to lateral movement, as well as a "solution that centralizes logging and security event alerting."

Effective and Compliance Dates

The effective and compliance dates of certain provisions of the Amendment will occur in a phased approach. The reporting of certain cybersecurity incidents to NYDFS will take effect on December 1, 2023. For many requirements, covered entities will have until April 29, 2024, to come into compliance with the Amendment. However, the Amendment sets forth longer timeframes for certain other compliance provisions.

The Takeaway

The existing Cybersecurity Regulation has had a significant influence on other federal and state cybersecurity regulations and enforcement actions, and we expect these amendments to similarly serve as a model for additional regulatory action at both the federal and state levels.

As always, please reach out to the authors or any member of McGlinchey's Cybersecurity and Data Privacy team if you have any questions.

Related people

David Tallman

Rachael L. Aspery

Paul J. Lysobey