Armstrong Teasdale

July 24, 2023 • Advisory • www.atllp.com

NYDFS UPDATES PROPOSED AMENDMENT TO CYBERSECURITY REGULATIONS

As mentioned in our Jan. 9, 2023, client advisory, the New York Department of Financial Services (NYDFS) proposed amendments to its Cybersecurity Regulations (23 NYCRR Part 500) on Nov. 9, 2022. A 60-day comment period followed the publication of the proposed amendments, which resulted in the NYDFS publishing an updated proposed Second Amendment (Amendment) to the regulations on June 28, 2023.

As a result of the Amendment, amendments to the Cybersecurity Regulations, which could have taken effect as early as the summer of 2023, will be delayed until at least early 2024. A 45-day comment period began when the updated Amendment was published and will last until Aug. 14, 2023. If no additional updates are proposed, the majority of the Amendment's provisions will take effect in February 2024, 180 days after the comment period ends.

The following is an overview of the key changes to the NYDFS Amendment and a timeline for compliance. With new obligations under the Cybersecurity Regulation expected to take effect in February 2024, companies should begin preparing now.

OVERVIEW

There are two sets of obligations under the NYDFS Amendment: one applies to all covered entities and the other applies only to Class A Companies. A covered entity is any individual or entity operating under NYDFS licensure, registration or similar authorization (insurance companies, banks and other regulated financial institutions). Class A Companies are covered entities with at least $20 million in gross annual revenue during each of the last two years from operations in New York and:

1. an average of 2,000 employees over the last two years (including affiliates); or
2. over $1 billion in gross annual revenue in each of the last two fiscal years from all business operations (including affiliates).

The Amendment clarifies that only entities that share information systems, cybersecurity resources or any part of a cybersecurity program with the covered entity are considered affiliates for purposes of the Class A applicability

PEOPLE
Jeffrey Schultz, CIPP/US

SERVICES AND INDUSTRIES
Data Innovation, Security and Privacy
Financial Services and Banking

analysis.

KEY CHANGES

Obligations for Class A Companies

While Class A Companies are subject to more strenuous obligations, the Amendment changes, and in some cases tempers, their duties under the Cybersecurity Regulations. For example:

- The requirement that Class A Companies conduct annual independent audits of their cybersecurity programs has been relaxed to allow internal auditors to perform the audit, provided they are not influenced by interested parties within the company.
- Class A Companies are no longer required to use external experts to conduct their annual risk assessments.
- The obligation to implement an automated method of blocking common passwords on accounts that are not maintained on systems controlled by the company has been eliminated.

Obligations for Covered Entities

The Amendment changes several obligations imposed on covered entities:

- The requirement that covered entities submit a written statement to the superintendent certifying their compliance with the Regulations was changed to require that covered entities certify *material* compliance with the Regulations.
- Multi-Factor Authentication (MFA) requirements were expanded to align with the FTC Safeguard Rules' MFA requirements. The scope of these heightened MFA requirements was also expanded from applying only to privileged accounts to any access of the entity's system.
- Incident Response Plans (IRP) must now contain a root cause analysis describing how and why the event occurred, the business impact it had, and the steps being taken to prevent recurrence.
- The definition of "Privileged Account" was narrowed to include only accounts that can be used to perform security-relevant functions that ordinary users are not authorized to perform. Thus, the heightened obligations will apply to fewer accounts if a breach occurs.
- The obligation that Senior Governing Bodies (the board of directors or an equivalent group) provide direction on the entity's cybersecurity risk management was reduced to providing effective oversight of the entity's cybersecurity risk management.
- Covered entities must test their IRP and Business Continuity and Disaster Recovery Plan (BCDRP) on an annual basis and with the participation of senior officers and the covered entity's highest-ranking

executive. Further, the BCDRP must ensure that the covered entity's information systems and material services remain available and functional, as well as able to protect personnel, assets and nonpublic personal information in the event of a cybersecurity incident.

- Backups must be maintained and annually tested to ensure the covered entity can restore its critical data and information systems in the event of an incident.
- The threshold for cybersecurity event reporting can now be triggered regardless of whether the incident occurred at the covered entity or at one of its service providers.
- Covered entities no longer need to update the NYDFS within 90 days of providing a cybersecurity event notice; instead, the entity must promptly provide information related to the incident if requested by the NYDFS.

TIMELINE FOR COMPLIANCE

Covered entities have 180 days from the effective date of the Amendment to comply with most of the new requirements. However, several obligations have different timelines for compliance.

On the effective date:

- Entities may apply to the superintendent for an exemption to the filing and submission requirements.
- Exempt entities must file a notice of exemption on the NYDFS' website within 30 days of the determination that the entity is exempt.
- Entities must annually prepare and submit a certification of compliance with this regulation to the superintendent.

30 days from the effective date: Entities must comply with the requirements for providing notice to the NYDFS (including notice of a cybersecurity incident and notice of an extortion payment).

One year from the effective date:

- Comply with all requirements for designating a Chief Information Security Officer (CISO) and ensure all duties placed on the CISO are being fulfilled.
- Implement a written encryption policy that conforms with industry standards.
- Establish written incident plans that describe the proactive measures being taken to investigate and mitigate cybersecurity incidents and ensure operational resilience (including IRPs and BCDRPs).

18 months from the effective date:

- Conduct automated scans of information systems and manually review systems that are not covered by automated scans.
- Limit access privileges to information systems that provide access to nonpublic information and access functions of privileged accounts that are not necessary for the user to perform their job.
- Implement a password policy that meets industry standards.
- Class A Companies must monitor privileged access activity and implement a privileged access management solution and an automated method of blocking common passwords for all accounts on information systems owned or controlled by the Class A Company.
- Implement risk-based controls designed to protect against malicious code.

Two years from the effective date:

- Establish MFA for any individual accessing any of the covered entity's information systems.
- Implement written policies and procedures to ensure complete asset inventory of information systems and ensure the secure disposal of nonpublic information that is no longer needed for a legitimate business purpose.

Our Data Innovation, Security and Privacy team is actively monitoring for developments in this space and has deep experience helping clients navigate complex regulatory issues related to cybersecurity. Contact your regular AT lawyer or one of the authors listed below for proactive guidance specific to your organization.