ROCHESTER BUSINESS JOURNAL
Part of the BRIDGETOWER MEDIA network
JANUARY 8, 2024

New cybersecurity requirements for financial services companies

BY ANNA MERCADO CLARK, ADELYN BURNS

On March 1, 2017, the New York State Department of Financial Services (DFS) enacted 23 NYCRR 500 (Part 500), or "cyber regulations," with the intent to combat the growing risk of cybersecurity threats. N.Y. Comp. Codes R. & Regs. tit. 23, § 500.0 (2023) (eff. Mar. 1, 2017). The DFS cyber regulations were amended as of November 1, 2023, which include changes to cybersecurity incident reporting, oversight of cybersecurity protocol, security controls and policy requirements, among other things. Many, but not all, of these changes are summarized below.

Among other things, the amended regulations clarify the responsibilities of a covered entity's Chief Information Security Officer (CISO), require specific data protection measures, expand the annual certification requirements and modify exemptions from Part 500. Various amendments are scheduled to take effect between December 1, 2023, and November 1, 2025.

CLASS A COMPANY REQUIREMENTS

A covered entity is any company operating under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law, or the Financial Services Law. All covered entities must comply with the cyber regulations unless they are subject to an exemption.

A Class A Company is a covered entity with at least $20 million in gross annual revenue in each of the last two fiscal years from all of its business operations and the business operations of its affiliates located in New York State. In addition, the entity must either have (1) more than 2,000 employees, including those of affiliates, averaging over the last two fiscal years or (2) over $1 billion in gross annual revenue, including revenue earned by affiliates.

In addition to requirements applicable to covered entities, heightened requirements for Class A Companies include, but are not limited to, designing and conducting independent audits of its cybersecurity program, monitoring privileged access activity, automatically blocking commonly used passwords and implementing endpoint detection.

RESPONSIBILITIES AND OVERSIGHT OF THE CHIEF INFORMATION SECURITY OFFICER

The amendments clarify if a covered entity employs a third-party CISO, the covered entity remains responsible for compliance with the cyber regulations, and that the CISO is subject to additional oversight requirements. In connection with the CISO's implementation and enforcement of the cybersecurity program and policy, the CISO now has to not only report at least annually on the entity's cybersecurity program, but also timely report "material cybersecurity issues" to the "senior governing body," such as the board of directors. If a Class A Company does not implement automatic blocking of common passwords, endpoint detection and response solution, or centralized logging and security event alerting, the CISO is tasked with approving in writing the use of reasonably equivalent or more secure controls.


Anna Mercado Clark


Adelyn Burns

RESPONSIBILITIES OF THE SENIOR GOVERNING BODY

The amendments require the senior governing body to oversee the covered entity's cybersecurity risk management. This includes understanding cybersecurity-related matters, maintaining cybersecurity programs, regularly reviewing cybersecurity reports and confirming that the entity has allocated sufficient resources to cybersecurity programs.

Specific data protection measures

The amendments to Part 500 clarify or heighten the requirements for a covered entity's cybersecurity programs. That is, under the current cyber regulations, a covered entity's cyber-

security program must include, among other things:

- Documented asset inventory of the entity's information systems
- Written incident response and business continuity and disaster recovery plans to respond and recover from cybersecurity incidents
- Risk-based controls designed to protect against malicious code
- Annual cybersecurity awareness training
- A written policy requiring encryption to protect nonpublic information
- Multi-factor authentication for remote access and all privileged accounts

DFS NOTIFICATION REQUIREMENTS

Annual certification

Covered entities still have to provide a compliance certification to the superintendent. But, the amendments now require that such certification be based on certain supporting materials, as well as a written acknowledgement of material non-compliance and remediation. These statements are due annually by April 15.

Security event notification

Now, in addition to having to provide notice of cybersecurity incidents that occur at a covered entity, the amendments explicitly require notice of incidents that occur at a third-party service provider or affiliate. The timing remains the same, and notice has to be given to the superintendent as "promptly as possible," but not later than 72 hours after determining that the event occurred.

Covered entities are now required to provide notice of extortion payments in connection with a cybersecurity incident within 24 hours of the payment or notice of the payment. Then, within 30 days of such payment, a description of alternatives considered and the due diligence used to identify such alternatives must be provided.

MODIFIED EXEMPTIONS

The amendments modify the criteria that covered entities must satisfy in order to qualify for a limited or full exemption to the cyber regulations. The amendments allow for more businesses to be exempt from certain requirements of the cyber regulations.

Small business exemption

The amendments expand the exemption criteria for small businesses, resulting in additional financial services companies that may be exempt from sections of the cyber regulations. Small businesses are defined as covered entities with (1) fewer than 20 employees and independent contractors of the covered entity and affiliates; (2) less than $7,500,000 in gross annual revenue in each of the last three fiscal years from all business operations of the covered entity and business operations of its affiliates within New York State; or (3) less than $15,000,000 in year-end total assets, including assets of all affiliates. The requirements that small businesses are exempt from include designating a CISO to report to the senior governing body and establishing written incident response plans, among other things. However, small businesses must still comply with all other sections of the cyber regulations.

Full exemptions

Apart from limited exemptions for small businesses, an otherwise covered entity may qualify for a full exemption from the cyber regulations if:

- The covered entity is an employee, agent, wholly owned subsidiary, representative or designee of another DFS-regulated business
- The other business's cybersecurity program fully covers the covered entity

This section exempts entities that are subject to the cyber regulations of a separate DFS-regulated business. While this exemption existed previously, the amendments add wholly owned subsidiaries to the categories of entities included in this section.

Additionally, the amendments create new exemptions for:

- Inactive individual insurance brokers
- Individual insurance agents who are placed in inactive status under Insurance Law section 2103
- Individual licensees placed in inactive status under Banking Law section 599-i

If a covered entity qualifies for a full exemption from Part 500, it must submit a Notice of Exemption through the DFS Portal within 30 days of the determination that the covered entity is exempt.

It is important that financial services companies review their compliance programs and seek assistance from experienced professionals in light of the amendments to the DFS cyber regulations.

Anna Mercado Clark, CIPP/E, CIPP/US, CIPM, FIP is a partner and Chief Information Security Officer at Phillips Lytle LLP as well as leader of the firm's Data Privacy and Cybersecurity Industry Team. She can be reached at aclark@phillipslytle.com or (716) 847-8400 ext. 6466.

Adelyn G. Burns is an attorney at Phillips Lytle LLP and member of the firm's Data Privacy and Cybersecurity Industry Team. She can be reached at aburns@phillipslytle.com or (716) 847-5425.