SPONSOR CONTENT

New Cybersecurity Requirements for Financial Services Companies

By Anna Mercado Clark and Adelyn G. Burns
Phillips Lytle LLP

As of November 1, 2023, the New York State Department of Financial Services (DFS) amended 23 NYCRR 500 (Part 500) to create new cybersecurity requirements for financial services companies. Among other things, the amended regulations clarify the responsibilities of Chief Information Security Officers (CISOs), require specific data protection measures, expand annual certification requirements and create new requirements for entities' cybersecurity programs. The amendments are scheduled to take effect from December 1, 2023 through November 1, 2025. This article highlights some, but not all, of the key changes made to Part 500.

Covered Entities

Part 500 applies to 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. Part 500 includes subcategories of covered entities such as Class A Companies and small businesses.

Class A Companies are covered entities that have at least $20 million in gross annual revenue and (1) more than 2,000 employees, including those of affiliates, averaged over the last two fiscal years or (2) over $1 billion in gross annual revenue, including that of its affiliates. N.Y. Comp. Codes R. & Regs. tit. 23, § 500.1(d) (2023). Class A Companies are subject to additional requirements under Part 500, including, but not limited to, conducting independent audits of their cybersecurity programs, monitoring privileged access activity and automatically blocking commonly used passwords.

Small businesses are now classified as covered entities with (1) fewer than 20 employees and independent contractors, (2) less than $7,500,000 in gross annual revenue, or (3) less than $15,000,000 in year-end total assets. Small businesses are subject to several exemptions from Part 500. Among other things, small businesses are exempt from designating a CISO to report to the senior governing body and establishing written incident response plans.

CISO and Senior Governing Body

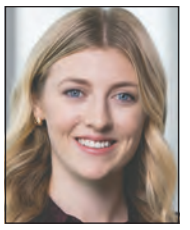
The CISO of a covered entity now, among other things, has to report at least annually on the entity's cybersecurity program, report material cybersecurity issues to the senior governing body and manage the entity's privileged accounts. Part 500 also now requires senior governing bodies, such as a board of directors, to understand cybersecurity-related matters and maintain, review and fund the entities' cybersecurity programs.

Cybersecurity Program

The amendments to Part 500 create new requirements that must be included in covered entities' cybersecurity programs. Among other things, the cybersecurity programs must now include:

- Documented asset inventory of the entity's information systems
- Written incident response plans and business continuity disaster recovery plans
- A written policy requiring encryption of nonpublic information
- Multi-factor authentication for remote access

Anna Mercado Clark
Partner



Adelyn G. Burns
Attorney

Annual Certification

Covered entities still have to provide a compliance certification to the DFS superintendent, however, the amendments require that the 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

Covered entities now have to provide notice of cybersecurity incidents that occur at third-party service providers or affiliates, in addition to incidents that occur at the covered entity. The timeframe remains the same, granting covered entities 72 hours from determining that the incident occurred to provide notice to the DFS superintendent.

In addition to the cybersecurity incident notification, 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, a detailed report of the payment is due within 30 days of the payment.

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.