New York Cybersecurity Amendments Raise Regulatory Bar

By **Elizabeth Roper, Cyrus Vance and Cynthia Cole** (November 29, 2023)

Elizabeth Roper

Cyrus Vance

Cynthia Cole

Effective Nov. 1, the New York State Department of Financial Services has strengthened cybersecurity requirements for financial services companies. All companies should take account of these amendments, as these NYDFS regulations are increasingly referenced as key benchmarks for cybersecurity compliance programs.

New York's Department of Financial Services finalized significant amendments to the cybersecurity requirements for financial services companies in Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York. This follows two rounds of proposed amendments and public comment periods. Covered entities should take steps to address the amendments to the regulations.

Part 500 was initially introduced in March 2017. It was a first-of-its-kind regulation that aimed to improve cybersecurity preparedness, response and governance in New York's financial services sector.

The original Part 500 included several provisions related to an entity's cybersecurity program, like the requirement that it be overseen by a chief information security officer or the equivalent, and incorporate risk-based measures for information security standards, like encryption, penetration testing and access management. It also required that covered entities report cybersecurity events to the NYDFS within 72 hours.

In the years since Part 500 became effective, the NYDFS has demonstrated a willingness to enforce its provisions aggressively when entities failed to comply.

In March 2021, the NYDFS ordered mortgage lender Residential Mortgage Services Inc. to pay a $1.5 million penalty for its failure to disclose or conduct an investigation into a 2019 phishing attack. The attack allowed hackers to access the email account of an employee who handled a substantial amount of customer financial information. According to the NYDFS, the comparatively modest penalty reflected the company's cooperation during the NYDFS review of the incident.

In October 2022, the NYDFS imposed a $4.5 million penalty on health insurance company EyeMed Vision Care LLC in relation to a July 2020 event that allowed an attacker to access and infiltrate an account that contained six years' worth of customer information. The NYDFS review of the incident found that the company had relied on cybersecurity assessments that did not meet Part 500's standards, filed noncompliant certifications with the NYDFS, did not implement access controls, and had not fully implemented multifactor authentication.

Part 500, as amended, reinforces what was already one of the most robust cybersecurity regulations in the country, and requires covered entities — that is, anyone operating under, or required to operate under, an authorization under New York banking, insurance or

financial services law — to implement specific governance controls, technical safeguards, and incident preparedness and response protocols.

The amendments took effect immediately upon being finalized Nov. 1. However, covered entities will have 180 days from the effective date of the amendments to achieve compliance with most of the new requirements.

Certain requirements for multifactor authentication will take effect two years after the finalized amendments were adopted. Other requirements for incident response planning and cybersecurity governance will take effect one year following adoption of the amendments.

Notable Features of the Amendment

The amendment creates Class A companies, which will be subject to stricter requirements, outlined below. Class A companies are defined as covered entities

> with at least $20,000,000 in gross annual revenue in each of the last two fiscal years from business operations of the covered entity and the business operations in [New York state] of the covered entity's affiliates and:
>
> > (1) Over 2,000 employees averaged over the last two fiscal years, including employees of both the covered entity and all of its affiliates no matter where located; or
> >
> > (2) 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.

The amendment also introduces enhanced requirements for Class A companies, including independent audits completed at least annually, as well as certain technical safeguards like endpoint monitoring, privileged access management, and vulnerability scans.

Additionally, it introduces a requirement that all covered entities update their cybersecurity risk assessments annually.

Also included is a new term, "cybersecurity incident," which 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 also includes new required technical safeguards for privileged accounts, including password management and the use of multifactor authentication, or MFA. MFA had previously been required for any individual accessing a covered entity's internal networks from an external network, but the amendments extend the MFA requirement to the

accessing of the covered entity's information systems from any location.

There are additionally new requirements for cyber risk governance, including that the chief information security officer make timely reports to the board of directors regarding cybersecurity issues. The amendment also creates new requirements for a covered entity to, at a minimum, annually test its incident response, business continuity and disaster recovery plans, and its ability to restore critical data from backups.

It also newly requires companies to report making a ransom payment within 24 hours. Within 30 days, they must provide a statement describing why the payment was necessary, the alternative means considered, and the steps taken to ensure compliance with relevant laws.

In the final amendments, the NYDFS clarified that a covered entity shall notify the superintendent "as promptly as possible but in no event later than 72 hours after determining that a cybersecurity incident has occurred."

Focus on Governance and Board Oversight

Importantly, the NYDFS maintains a requirement that the board exercise oversight of cybersecurity risk in certain specific ways. The final Part 500 requires that the board, or equivalent senior governing body,

> exercise oversight of the covered entity's cybersecurity risk management, including by:
>
> > (1) having sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors;
> >
> > (2) requiring the covered entity's executive management or its designees to develop, implement and maintain the covered entity's cybersecurity program;
> >
> > (3) regularly receiving and reviewing management reports about cybersecurity matters; and
> >
> > (4) confirming that the covered entity's management has allocated sufficient resources to implement and maintain an effective cybersecurity program.

While stopping short of requiring boards to include cybersecurity experts among their members, the NYDFS is clearly signaling an expectation that boards make oversight of cybersecurity risks a priority, if it is not already.

Next Steps

Covered entities should take steps to integrate the new requirements now, so they will be ready to comply by the newly established effective dates. Some key steps companies can take include the following.

- Organizations should consider the application of Part 500 to their business and take steps to operationalize compliance as necessary. Organizations should take note that even firms that aren't directly governed by Part 500 as covered entities should

assess the potential applicability of the amended regulation to affiliates and subsidiaries and should review the effects on enterprise-wide cybersecurity policies.

- Conduct gap assessments by reviewing existing cybersecurity governance programs, identifying where gaps exist, and ensuring these gaps are remediated by the effective dates.

- Class A companies should engage independent third-party auditors as required by the revised amendments.

- Covered entities should review and update their incident response plans, and test those plans by conducting tabletop exercises with key stakeholders. This includes tabletop exercises with senior leadership or board members. Covered entities should also note that certain requirements, such as a 72-hour reporting deadline, may differ from other applicable requirements, and these distinctions should be accounted for in their incident response plans.

- In light of the reporting requirement for ransom payments, covered entities may want to consider creating a specific playbook for ransom events that includes a framework for assessing whether and when such a payment may be made.

Elizabeth Roper is a partner at Baker McKenzie.

Cyrus Vance Jr. is a partner and the global chair of the cybersecurity practice at the firm.

Cynthia Cole is a partner at the firm.

Baker McKenzie associate Manisha Reddy contributed to this article.