ALERT

New York Department of Financial Services' New Enhanced Cybersecurity Requirements Effective November 1, 2024

Financial institutions subject to New York's already comprehensive cybersecurity regulation must prepare for new, enhanced requirements.

By Mark L. Krotoski, Brian H. Montgomery

TAKEAWAYS

- The next phase of the recent amendments to New York's comprehensive cybersecurity regulations become effective November 1, 2024.
- Under this phase, the amendments remove exemptions and require enhanced governance, business continuity and encryption standards.
- Entities covered by the regulation should prepare for continued scrutiny of their cybersecurity programs.

10.30.24

On November 1, 2024, the next phase of several significant amendments to the New York Department of Financial Services' (NYDFS) cybersecurity regulation take effect. These specific amendments, enacted in 2023, impact the scope of entities covered by the regulation and require covered entities to implement enhanced governance, business continuity and encryption standards.

NYDFS regulates more than 3,000 financial institutions with assets totaling more than $9.7 trillion, including banks, money services businesses, non-bank lenders, virtual currency companies, insurance companies, and many others. The NYDFS cybersecurity regulation, which was first issued in 2017, was

© 2025 Pillsbury Winthrop Shaw Pittman LLP. Attorney Advertising. pillsburylaw.com

already the most comprehensive of any U.S. financial regulator. NYDFS' recent amendments to the regulation will require covered entities to adapt to even more detailed and prescriptive requirements.

Limited Exemptions

The NYDFS cybersecurity regulation applies across the board to the many types of entities NYDFS supervises, from global systemically important financial institutions to small businesses. However, the regulation does include three limited exemptions from certain of its provisions from the smallest businesses NYDFS supervises. The amendments that become effective on November 1, 2024, change the threshold of these exemptions, and as a result will likely subject entities that could formerly claim a limited exemption to the full scope of the regulation.

- The regulation originally provided a limited exemption for entities with fewer than 10 employees and independent contractors of the entity and its affiliated who were either located in New York or responsible for the entity's business. Although the amended version of the regulation increases this figure to 20 employees and independent contractors, it removes the limitation that such personnel be located in in New York or responsible for the entity's business.
- The regulation originally provided a limited exemption for entities with less than $5 million in gross annual revenue in each of the last three years from New York operations. Although the amended version of the regulation increases this figure to $7.5 million, it removes the limitation to revenue from New York operations and will now apply to all of the entity's revenue (whether derived from New York or elsewhere).
- The regulation originally provided a limited exemption for entities with less than $10 million in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates. The amendment increases this figure to $15 million.

Entities that qualify for a limited exemption are exempt from the regulation's governance (Section 500.4), vulnerability management (Section 500.5), audit (Section 500.6), application security (Section 500.8), personnel and intelligence (Section 500.10), certain training (Sections 500.14(a)(1), (a)(2), and (b)), encryption (Section 500.15), and incident response and business continuity management (Section 500.16) requirements.

Notably, the regulation originally provided a limited exemption from the regulation's multifactor authentication requirements. The amendments that become effective November 1, 2024, remove this exemption, meaning that all entities supervised by NYDFS must comply with the regulation's multifactor authentication requirements.

Enhanced Governance

The phased-in amendments effective November 1, 2024, place increased importance on oversight of cybersecurity-related matters by the entity's senior governing body (e.g., the board of directors) and build on existing requirements.

© 2025 Pillsbury Winthrop Shaw Pittman LLP. Attorney Advertising. pillsburylaw.com

The NYDFS cybersecurity regulation originally required covered entities to designate a qualified chief information security officer (CISO) to manage the entity's cybersecurity program. The CISO is also required to provide an annual written report on the condition of the entity's cybersecurity program to the entity's senior governing body.

The amendments effective November 1, 2024, required enhanced oversight and governance measures. First, a covered entity's senior governing body must have sufficient understanding of cybersecurity-related matters to exercise effective oversight of cybersecurity-related matters. The senior governing body is also tasked with overseeing management's implementation of an effective cybersecurity program and ensuring that management has allocated sufficient resources to the entity's cybersecurity program. In addition, the entity's CISO will now be specifically required to make timely reports of material cybersecurity issues to the senior governing body, which should in turn use such information in its oversight of cybersecurity-related matters. The annual CISO report to the senior governing body will need to address "plans for remediating material inadequacies."

Incident Response

The NYDFS cybersecurity regulation originally required covered entities to establish and implement an incident response plan. The amendments effective November 1, 2024, require covered entities to implement new, proactive incident response measures, as well as business continuity and disaster recovery plans.

A covered entity's business continuity and disaster recovery plans must be reasonably designed to ensure the availability and functionality of the covered entity's systems and services, and protect the entity's personnel, assets and nonpublic information in the event of a cybersecurity-related disruption. The amended regulation prescribes a series of items that entities must include in business continuity and disaster recovery plans, including identification of documents needed for the entity's continued operations, key personnel responsible for implementing the plans, and procedures for backup and recovery. Covered entities must also implement enhanced incident response, business continuity, and disaster recovery training and testing.

New incident response plan requirements include addressing recovery from backups, providing training "to all employees responsible for implementing the plans regarding their roles and responsibilities," an annual test of the incident response and business continuity and disaster recovery plans, and the "ability to restore its critical data and information systems from backups."

Encryption

The amendments that become effective November 1, 2024, also include enhanced encryption requirements. Covered entities will now be required to implement an industry standard encryption policy to protect nonpublic information both in transit and at rest. Under the original regulation, covered entities had

© 2025 Pillsbury Winthrop Shaw Pittman LLP. Attorney Advertising. pillsburylaw.com

flexibility to implement compensating controls as an alternative to encryption. That flexibility is significantly limited in the amended regulation, and the entity's CISO must approve any alternative controls in writing and review such controls at least annually.

Conclusion

NYDFS has instituted a series of enforcement actions involving millions of dollars in fines assessed against covered entities for alleged violations of the NYDFS cybersecurity regulation. Many of the amendments that become effective on November 1, 2024, are based on issues identified through prior NYDFS examinations and enforcement actions. Entities subject to NYDFS supervision should be prepared to be examined on these new requirements during their next examination cycle and should implement these new requirements effectively to successfully navigate the examination process. Additionally, covered entities must comply with the annual Certification of Material Compliance or Acknowledgement of Noncompliance on April 15 of each year and will need to confirm compliance with the new requirements.

These and any accompanying materials are not legal advice, are not a complete summary of the subject matter, and are subject to the terms of use found at: https://www.pillsburylaw.com/en/terms-of-use.html. We recommend that you obtain separate legal advice.