NOVEMBER 2023

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

New York adds more stringent cybersecurity requirements

The New York Department of Financial Services (NYDFS) released the final amendments to its cybersecurity rules for financial, banking and insurance companies. The changes add obligations for accountability, incident reporting, and compliance certification—among others—to an already highly prescriptive framework. Companies need to have measures in place for the compliance and incident-reporting changes by December 1, 2023 (the other changes will be phased in over the next two years).

Key Takeaways

- **NYDFS gets (even more) prescriptive.** The new obligations get more granular and eschew the "reasonableness" frameworks advanced in other laws.
- **CEOs and CISOs will be more involved.** The obligation for a CEO/CISO to personally certify compliance raises the stakes for them and increases the likelihood that they will be more hands-on in the compliance process.
- **Other regulators will likely follow suit.** These prescriptive rules will influence industry norms and other legislators/regulators are likely to incorporate the ideas into new frameworks.

Notable New Requirements

The most notable additions are:

- **Compliance Certifications** [500.17(b)]. Submit certifications from the CISO and highest executive attesting to material compliance or submit a written acknowledgment discussing the lack of such compliance.

SUBSCRIBE

ARCHIVE

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Josh Hansen
Associate
303.285.5306
jahansen@shb.com

- **Incident Reporting** [500.17(c)]. Notify NYDFS of cyber-extortion payments within 24 hours and explain within 30 days why the payment was necessary.
- **Multifactor Authentication** [500.12(a-b)]. Use multifactor authentication for access to information system, unless the CISO approves in writing an equivalent control.
- **Policy Review** [500.12(a-b)]. Obtain approval for policies each year from senior officer or senior governing body (board of directors or equivalent).
- **Vulnerability Management** [500.5(a)]. Conduct automated scans (and manually review systems not covered by the scans) to discover vulnerabilities.
- **Asset Inventories** [500.13(a)]. Create and maintain a complete, accurate asset inventory.
- **Oversight** [500.4(d)]. Ensure the governing body (board of directors or equivalent) has appropriate cybersecurity expertise or receives advice from those with such expertise.
- **IR/Continuity Plan Testing** [500.16(a, d)]. Develop a business continuity and disaster recovery plan and annually test it and the IR plan.
- **Backups** [500.16(e)]. Maintain backups necessary to restore material operations.
- **Training** [500.14(a)]. Conduct annual (or more frequent) cybersecurity training that includes social engineering for all personnel.
- **Access Controls** [500.7(a)]. Deploy more robust access controls, including limiting the number of privileged accounts and reviewing privileges at least annually.
- **CISO Duties** [500.4(b-c)]. Require that the CISO report material cybersecurity issues (e.g., significant changes or cybersecurity events) and provide annual plan for remediating material inadequacies.
- **Risk Assessments** [500.9(a)]. Update the risk assessment at least annually and whenever there is a material change to the cyber risk.

The amendments impose even more onerous obligations on large companies ($20 million in gross revenue + other criteria)—which NYDFS calls "Class A Companies." Those companies must, for example: deploy an Endpoint Detection and Response solution, implement a solution for centralized logging and security alerts, and conduct independent audits at a frequency determined by their risk assessment.

NYDFS also made some tweaks on the enforcement front; they provided a non-exhaustive list of factors the department will consider when assessing penalties and clarified that a company violates the rule if they fail to materially comply with any part for a 24-hour period.

The obligations come into effect over the next two years:

December 1, 2023	• **Compliance Certifications.** Ensure the CEO/CISO certify compliance

	• **Incident Reporting.** Notify NYDFS of extortion payments
April 29, 2024	• **Risk Assessments.** Update risk assessments at least annually • **Audit.** Conduct independent audits (Class A Companies only) • **Policy Review.** Obtain annual approval for cybersecurity policies
November 1, 2024	• **Access Controls.** Add more robust access/privilege controls • **Backups.** Maintain material backups • **CISO Duties.** Ensure the CISO reports material developments • **IR/Continuity Plan Testing.** Create and test IR/continuity plan • **Oversight.** Ensure governing body has appropriate expertise
May 1, 2025	• **Vulnerability Management.** Deploy automated scanning • **Training.** Conduct training addressing social engineering • **Endpoint Detection.** Deploy EDR (Class A Companies only) • **Logging.** Centralize logging and alerts (Class A Companies only)
November 1, 2025	• **Asset Inventories.** Create and maintain asset inventory • **Multifactor Authentication.** Deploy multifactor authentication

Changes From Prior Drafts

When compared to NYDFS's last draft, the final version has some notable (and useful) changes/clarifications:

- **CISO Definition** [500.1(c); 500.4(d)]. Removes requirement that the CISO have the power to ensure risks are appropriately managed and direct resources to implement/maintain the cybersecurity program. [Management is now responsible for ensuring adequate resources are allocated, and the senior governing body must confirm that occurred.]
- **Audits** [500.2(c)]. Eliminates Class A companies' obligation to conduct annual audits and replaced it with a requirement to conduct such audits in accordance with the risk assessment.
- **CISO Reporting** [500.4(c)]. Permits the CISO to report material cybersecurity issues to senior officers or the senior governing body. [Previously, the CISO had to report those issues to the senior governing body.]

- **IR/Continuity Plan Testing** [500.16(d)]. Removes requirements for senior officers and highest-ranking executive to attend regular testing of the IR and business continuity plans. [Now, only "staff and management critical to the response" are required.]
- **Incident Reporting** [500.1(g)]. Eliminates obligation to report every incident of unauthorized access to a privileged account. [Now, such access only triggers notice if it otherwise qualifies as reportable event.]
- **Incident Updates** [500.17(a)]. Clarifies that covered entities need to supplement their incident notices when there are "material changes or new information previously unavailable." [Previously, there was just a general obligation to "supplement the information provided."]
- **Exemptions** [500.19(a)]. Increases the revenue threshold to qualify for the limited exemption (which allows a company to avoid certain NYDFS obligations) from $5 million in gross revenue to $7.5 million and clarified that the only affiliate revenue included in that calculation is money derived from operations in New York.

NYDFS also now requires reporting of a "cybersecurity incident" (rather than "cybersecurity event"), but this is just a change in terminology—the substantive reporting triggers remain the same.

Action Items

- **Consider attending NYDFS training.** Attend one of NYDFS's webinars covering the new rules on November 15, November 30, and December 7.
- **Revise and test IR plan.** You should add a process for alerting NYDFS of any cybersecurity extortion payment (e.g., ransomware) and ensure you test the full plan on a regular basis with key stakeholders.
- **Update the CEO and CISO on compliance efforts.** Brief the CEO and CISO on new rules and existing compliance measures because they have new exposure under the rules: They must personally certify that the company is compliant.
- **Coordinate now with IT and InfoSec.** Work now with IT/InfoSec to assess what new measures are needed because many provisions could require significant operational changes (and that will eat into the grace period provided by the delayed effective dates).

The choice of a lawyer is an important decision and should not be based solely upon advertisements.