# A Summary of the Final Amendments to the NYDFS Cyber Rules

**November 15, 2023**

On November 1, 2023, the New York Department of Financial Services ("NYDFS" or the "Department") announced the adoption of the second amendment to its Cybersecurity Regulation (the "Second Amendment" or "Final Amendment") that reflects NYDFS's revisions as a result of comments it received on the proposed amendment released in June 2023 (the "June 2023 Proposal"). A redline of the Final Amendment against the version of Part 500 that is currently in effect can be found here.

Throughout the amendment process, the Department was resolute in promulgating a set of standards for larger companies rather than deferring to those companies to make all risk-based decision-making. The Final Amendment reflects that the Department carefully considered public comments, and made revisions to its Cybersecurity Regulation that demonstrate an understanding of the complex nature of cybersecurity governance and oversight.

The Second Amendment's compliance requirements will take effect in phases. For legal and compliance teams, the new requirements on certification, risk assessments, and governance will call for cross-functional participation throughout the coming year as companies assess their compliance with NYDFS's Cybersecurity Regulation. To assist businesses impacted by the Second Amendment with tracking key compliance dates, NYDFS published Cybersecurity Implementation Timelines for small businesses, Class A businesses, and covered entities, and announced that it will host webinars to assist regulated entities with compliance.

Below we provide a high-level timeline for when the new and updated requirements contained within the Final Amendment will become effective:

- December 1, 2023:
  - 500.17: Notification obligations to NYDFS.
- April 15, 2024:

- 500.17(b): Certification requirements.

- April 29, 2024:
  - 500.9: Risk assessments requirements;
  - 500.3: Cybersecurity policy requirements;
  - 500.5(a)(1), (b), and (c): Penetration testing and monitoring requirements;
  - 500.14(a)(3): Training requirements; and
  - 500.2(c): For Class A companies, audit requirements.
- November 1, 2024:
  - 500.4: CISO, management, and board governance requirements;
  - 500.15: Encryption requirements; and
  - 500.16: Incident response and business continuity planning and testing requirements.
- May 1, 2025:
  - 500.5(a)(2): Scanning requirements;
  - 500.7: Access privilege and password requirements;
  - 500.14(a)(2): Requirements for protection against malicious code;
  - 500.7: For Class A companies, requirements relating to privileged access management solutions and blocking of commonly used passwords; and
  - 500.14(a)(2) and (b): For Class A companies, requirements for endpoint detection and response solutions and centralized logging.
- November 1, 2025:
  - 500.12: MFA requirements; and
  - 500.13(a): Asset inventory requirements.

A review of the redline of the June 2023 Proposal against the Final Amendment demonstrates that NYDFS incorporated several important changes in response to the comments it received. The Department also released a helpful 38-page Assessment of Public Comments ("APC") that details why NYDFS accepted or rejected certain comments.

## The Six Key Updates to Part 500

The changes in the Final Amendment can be roughly divided into six categories: New Obligations for Larger ("Class A") Companies, Governance, Technical Requirements, Business Continuity, Breach Notification Obligations, and Enforcement.

### New Obligations for Class A Companies

The Final Amendment creates a category of "Class A" companies that are covered entities with at least $20,000,000 in gross annual revenue in each of the last two years from all business operations of the entity and the business operations in New York State of its affiliates, and either (i) over 2,000 employees or (ii) $1 billion in gross annual revenue for each of the past two fiscal years for the global business operations of the covered entity and its affiliates. Importantly, when calculating the number of employees and the gross annual revenue, the term "affiliates" should include "only those that share information systems, cybersecurity resources, or all or any part of a cybersecurity program with the covered entity."

Class A companies are subject to several additional cybersecurity obligations under the Final Amendment, including:

- **Independent Audits**: Class A companies must design and conduct independent audits of their cybersecurity programs, using internal or external auditors who are free to make decisions not influenced by the covered entity, at a frequency determined by their individual risk assessment. [500.2(c)]

- **Access Privileges and Management**: Class A companies must monitor privileged-access activity, implement a privileged access management solution, and implement an automated method of blocking commonly used passwords. [500.7(c)]

- **Monitoring**: Class A companies must implement an endpoint detection and response solution to monitor anomalous activity, including lateral movement, and a solution that centralizes logging and security event alerting. [500.14(b)]

## New Governance Requirements for CISOs, Management, and the Board

NYDFS views strong governance as a central aspect of good cybersecurity. The original Part 500 required cybersecurity reporting to the board, written policies approved by a senior officer, and the need for a CISO or equivalent. The Final Amendment provides several enhancements, including:

- **Additional Board Reporting**: Under the original Part 500, the CISO is required to report to the board annually on the company's cybersecurity program and material cybersecurity risks. The Final Amendment provides for additional annual reporting to the board (or senior governing body) on plans for remediating material inadequacies, as well as timely reporting to the board on material cybersecurity issues, such as significant cybersecurity events and significant changes to the cybersecurity program. [500.4(b) and (c)]

- **Board Oversight**: Under the Final Amendment, the board or senior governing body of covered entities must exercise oversight of cybersecurity risk management by (1) having sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include advice of advisors; (2) requiring management to maintain the covered entity's cybersecurity program; (3) regularly reviewing management reports about cybersecurity matters; and (4) confirming that management has allocated sufficient resources to maintain an effective cybersecurity program. [500.4(d)]

- **CEO/CISO Annual Certification**: The annual certification of compliance must now be signed by the covered entity's highest-ranking executive (e.g., CEO) and its CISO, rather than by a "senior officer" under the original Part 500. [500.17(b)(2)]

- **Material Compliance for Previous Calendar Year**: The annual certification now requires the CEO and CISO to certify that the covered entity *materially complied with the Part 500 requirements during the prior calendar year*, and must be based on data and documentation that is sufficient to accurately demonstrate such material compliance. These changes appear to require some form of ongoing compliance review during the calendar year, rather than a one-time-snapshot assessment. In practice, this kind of assessment will be challenging for most covered entities to operationalize and document. They will have to consider what risk management tools can be used to track compliance gaps on an ongoing basis, decide what counts as "material noncompliance," and determine how their CISO and CEO will get comfortable making a certification of compliance with dozens of cybersecurity requirements for an entire calendar year. [500.17(b)(1)(i)]

- **Acknowledgement of Noncompliance**: If the highest-ranking executive and/or CISO cannot certify to material compliance, they must: (1) provide an acknowledgement that the covered entity did not materially comply with the requirements of Part 500 for the previous calendar year; (2) identify the sections of Part 500 that the entity has not materially complied with, and describe the nature and extent of such noncompliance; and (3) provide a remediation timeline or confirmation that remediation has been completed. [500.17(b)(1)(ii)]

- **Tabletop Exercises and Other Testing**: Under the Final Amendment, covered entities must test, at least annually, their incident response and business interruption and disaster recovery ("BCDR") plans with all staff and management who are critical to the response. The requirement in the June 2023 proposal that the CEO must participate in such testing was removed in the Final Amendment. Annual testing of the covered entity's ability to restore its systems from backups is also a new requirement. [500.16(d)]

- **Annual Risk Assessments**: The risk assessments will need to be reviewed and updated annually, as well as whenever a change in the business or technology causes a material change to the covered entity's cyber risk. [500.9(a)]. The definition of "risk assessment" is expanded to include "the process of identifying, estimating and prioritizing cybersecurity risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, customers, consumers, other organizations, and critical infrastructure resulting from the operation of an information system. Risk assessments incorporate threat and vulnerability analyses and consider mitigations provided by security controls planned or in place." [500.1(p)]

## New Technical Requirements

In addition to the technical requirements discussed above that apply only to Class A companies, the Final Amendment imposes the following new technical obligations on all covered entities:

- **Multi-Factor Authentication ("MFA")**: With only limited exceptions for very small entities, the Final Amendment otherwise requires MFA "for any individual accessing any information system of a covered entity." The CISO may approve the use of reasonably equivalent or more secure compensating controls. [500.12 (a) and (b)]. In the final round of comments, several organizations expressed concern that this new formulation of MFA would mean that employees who are accessing routine parts of the company's network from inside their office, or from their mobile devices, would be required to use MFA. While NYDFS did not change the revised language in response to these concerns, it did address them in the APC at page 21 as follows:

> *It may be acceptable, in some circumstances, depending on a covered entity's specific cybersecurity risks, to use a device, such as an office workstation, mobile phone, or laptop, as one of the authentication factors required for MFA, especially if, for example, the device contains biometric capabilities or authenticator applications.*

The definition of MFA has also been changed to remove the reference to "text message on a mobile phone." [500.1(j)]. The APC issued with the June 2023 Proposal indicated that NYDFS had eliminated this reference because "[t]ext message MFA, while still acceptable, is widely considered to be a weaker form of MFA, and the Department encourages the adoption of more secure forms of MFA, in particular phishing-resistant forms of MFA." NYDFS indicated that mobile phone authenticator applications satisfy, and might be preferred for, the possession factor. NYDFS also recognized that it "will be too costly and burdensome at this time to require only phishing-resistant MFA for all covered entities[,]" but also noted that "physical security tokens, such as personal identity verification ('PIV') cards and security keys, offer phishing resistance[.]"

- **Monitoring**: Covered entities will be required to implement risk-based controls designed to protect against malicious code, including those that monitor and filter web traffic and email to block malicious content. [500.14(a)(2)]

- **Encryption**: The Final Amendment removes the ability of covered entities to implement effective alternative compensating controls to encryption of nonpublic information in transit over external networks. [500.15]. In the APC, the Department explained that it "is unaware of any effective alternative compensating control currently being used in the financial services sector that is comparable to encryption in transit over external networks."

- **Vulnerability Management**: In addition to annual penetration testing, covered entities will be required to: (1) conduct automated scans of information systems (and a manual review of systems not covered by such scans), for the purpose of discovering, analyzing, and reporting vulnerabilities at a frequency determined by the risk assessment, and promptly after any material system changes; (2) ensure that they are promptly informed of new security vulnerabilities by having a monitoring process in place; and (3) timely remediate vulnerabilities, giving priority to vulnerabilities based on the risk they pose to the covered entity. [500.5]

- **Asset Inventory**: Each covered entity is now required to implement policies and procedures designed to maintain a complete and accurate asset inventory of the covered entity's information system that includes a method to track key information

for each asset (e.g., owner, location, classification or sensitivity, support expiration date, and recovery time objectives), along with the frequency required to update and validate the asset inventory. [500.13(a)]

- **Access Privileges**: The Final Amendment requires covered entities to: (1) limit user access privileges to only those necessary to perform the user's job function; (2) limit the number of privileged accounts; (3) review all user access privileges at least annually and disable accounts that are no longer necessary; (4) disable or securely configure all protocols that permit remote control of devices; and (5) promptly terminate access following departures. [500.7(a)]. The term "privileged account" is newly defined in the Final Amendment as "any authorized user account or service account that can be used to perform security-relevant functions that ordinary users are not authorized to perform, including but not limited to the ability to add, change or remove other accounts, or make configuration changes to information systems." [500.1(n)]

- **Password Management**: To the extent passwords are employed as a method of authentication, the Final Amendment requires covered entities to implement a written password policy that meets industry standards. [500.7(b)]

### Incident Response and Business Continuity Planning

The Final Amendment introduces several new requirements for companies' incident response and BCDR plans, including:

- **Incidence Response Plans**: IRPs now need to address recovery from backups and root cause analysis as to how and why an event occurred, what business impact it had, and what will be done to prevent reoccurrence. [500.16(a)(1)]

- **BCDR Plans**: Covered entities are now required to have a BCDR plan to ensure the availability of the covered entity's information systems and material services. Such plans shall: (1) identify documents, data, facilities, infrastructure, services, personnel and competencies essential to the continued operations of the covered entity's business; (2) include a plan to communicate with essential persons in the event of a cybersecurity-related disruption; (3) include procedures for the timely recovery of critical data and information systems; (4) include procedures for backing up information essential to the operations of the covered entity and storing such information off-site; and (5) identify third parties that are necessary to the continued operations of the covered entity's information systems. [500.16(a)(2)]

## Breach Notification Obligations

The original Part 500 required covered entities to notify NYDFS within 72 hours of determining that a cybersecurity event occurred that (1) had a reasonable likelihood of materially harming normal operations of the entity, or (2) required notification to any other regulatory body. The Final Amendment expands these notification obligations, including by:

- **Ransomware Notification Requirements**: The Final Amendment adds "the deployment of ransomware within a material part of the covered entity's information systems" as an additional notification trigger. [500.17(a) and 500.1(g)]. There is also a new 24-hour notification obligation for any extortion payment connected to a cybersecurity event, as well as a 30-day reporting requirement explaining why payment was necessary, alternatives that were considered, and sanctions diligence that was conducted. [500.17(c)]

- **Information Updates**: The Final Amendment requires covered entities to promptly provide the superintendent with any information requested regarding a reported incident, and provides that entities have a continuing obligation to update the superintendent with material changes or new information previously unavailable. [500.17(a)(2)]

## Enforcement

The Final Amendment adds two significant enforcement provisions to Part 500. First, it provides that the commission of a single act prohibited by Part 500, or the failure to satisfy an obligation, constitutes a violation. Such failures include: (1) the failure to prevent unauthorized access to nonpublic information due to noncompliance; or (2) the material failure to comply for any 24-hour period with any Part 500 obligation. [500.20(b)]

The Final Amendment also provides a list of mitigating factors that NYDFS will consider when assessing penalties, including cooperation, good faith, intentionality, history of prior violations, harm to customers, gravity of violation, number of violations, involvement of senior management, penalties imposed by other regulators, and the financial resources of the covered entity and its affiliates. [500.20(c)]

## Three Takeaways

- **Incident Response Plans**: Given that new reporting requirements are effective on December 1, 2023, entities should update their incident response plans, especially with regard to their ransomware policy.

- **Gap Assessment**: Covered entities should consider conducting a gap analysis between the requirements in the Final Amendment and their cybersecurity program, along with a road map for closing any gaps that is consistent with the timeline for implementation of the new Part 500 requirements. For some companies, it may take significant time and resources to fully implement these new requirements, and so they may want to start early. And even companies that are not subject to Part 500 may consider conducting a gap analysis in anticipation that similar rules are likely to be adopted by other regulators and likely will be considered best practices for cybersecurity governance and compliance programs.

- **Budget**: For many companies, compliance with the new Part 500 requirements will require a significant increase in their cybersecurity compliance budgets and the securing of additional resources for 2024 and beyond. Some companies may want to address this likely needed increase now as 2024 budgets are being considered.

To subscribe to the Data Blog, please click here.

*The Debevoise Data Portal is an online suite of tools that help our clients quickly assess their federal, state, and international breach notification and substantive cybersecurity obligations. Please contact us at dataportal@debevoise.com for more information.*

* * *

Please do not hesitate to contact us with any questions.

Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandra@debevoise.com

Luke Dembosky
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com

**Erez Liebermann**
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

**Caroline N. Swett**
Partner, New York
+1 212 909 6432
cnswett@debevoise.com

**Johanna N. Skrzypczyk**
Counsel, New York
+1 212 909 6291
jnskrzypczyk@debevoise.com

**Michael R. Roberts**
Associate, New York
+1 212 909 6406
mrroberts@debevoise.com

**Stephanie D. Thomas**
Associate, New York
+1 212 909 6535
sdthomas@debevoise.com

**Joshua A. Goland**
Law Clerk, New York
+1 212 909 6420
jagoland@debevoise.com