NYDFS Publishes Revised Amendments to Its Cybersecurity Regulation—What Got Fixed, and What Still Needs Fixing

July 10, 2023

On June 28, 2023, the New York Department of Financial Services ("NYDFS") announced its Revised Proposed Second Amendment to its Cybersecurity Regulation, 23 NYCRR Part 500 (the "Revised Amendment" or "June 2023 Amendment"), which reflects revisions made by the NYDFS as a result of comments it received on its Initial Proposed Second Amendment released in November 2022 (the "Initial Amendment" or "November 2022 Amendment"). The 45-day comment period for the Revised Amendment ends on August 14, 2023.

In this blog post, and during our Webcast that took place on Friday, July 7 at 11:00 AM Eastern, we discuss the changes reflected in the Revised Amendment and what additional changes the NYDFS should consider before issuing its final amendment. Highlights of the Revised Amendment revisions discussed below include:

- narrowing the definition of Class A companies;
- removing some of the external requirements for audits and risk assessments;
- softening the cyber expertise requirement for boards;
- removing the internal reporting requirement for material issues found during penetration testing;
- significantly increasing the MFA requirements;
- narrowing the scope of incident response and business continuity plans;
- adding a materiality threshold for both violations and certifications of compliance;
- responding to requests for clarification; and
- changing the effective dates for certain requirements.

In sum, a review of the changes between the November 2022 Amendment and the June 2023 Revised Amendment shows that NYDFS took the comments on the Initial Amendment very seriously and incorporated many of them into the Revised Amendment. At the same time, there were some comments that NYDFS declined to address that we believe NYDFS should reconsider in the current comment period. We discuss those below as well.

Companies or trade groups considering making comments on the Revised Amendment should carefully review the 92-page Assessment of Public Comments that the NYDFS released explaining why it accepted certain comments and rejected others.

Revised Definition of Class A Companies

In the Initial Amendment, Class A companies (which are subject to several additional cybersecurity obligations under the Rule) were defined as covered entities with:

- at least $20 million in gross annual revenue in each of the last two fiscal years from business operations of the covered entity and its affiliates in this State; and either:
    - over 2,000 employees as an average over the last two fiscal years, including employees of both the covered entity and all of its affiliates no matter where located; or still accounting for the covered entity and affiliates; or
    - over $1 billion in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and its affiliates.

The Revised Amendment narrows the definition of a Class A company by adding that, "when calculating the number of employees and gross annual revenue, affiliates shall include only those that share information systems, cybersecurity resources or all or any part of a cybersecurity program with the covered entity." Part 500.1(d). This creates incentives for some covered entities to separate their information systems and cyber program from overseas affiliates to avoid having those affiliates considered for the purposes of the Class A calculation.

Revisions to Audits and Risk Assessments

The Initial Amendment required that the independent audit be conducted by external auditors. The Revised Amendment allows covered entities to use their internal auditors to conduct independent audits so long as the auditor is free to make decisions not

influenced by the covered entity being audited or by its owners, managers, or employees.

The Revised Amendment also removes the requirement that Class A companies use external experts to conduct their risk assessments at least once every three years. In addition, it removes the following language from the risk assessment requirement:

> *Risk assessments shall take into account the specific circumstances of the covered entity, including but not limited to its size, staffing, governance, businesses, services, products, operations, customers, counterparties, service providers, vendors, other relations and their locations, as well as the geographies and locations of its operations and business relations. Part 500.1(o).*

According to the NYDFS, this change was in response to comments it received that certain terms, such as "counterparties" and "other relations," were unclear, difficult to assess, or overly broad and was aimed at further alignment with the definition of "risk assessment" used in the various special publications from NIST.

Board Expertise

The Initial Amendment required the board (or senior governing body) of a covered entity to "have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge, to exercise effective oversight of cybersecurity risk management." The Revised Amendment lowers this requirement and instead provides that boards must have "sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors." Part 500.4(d)(2). It also limits the board's obligation to provide effective oversight of the covered entity's cybersecurity risk management, removing the language that boards must "provide direction to management" that appeared in the Initial Amendment. Part 500.4(d)(1).

Vulnerability Assessments – Reporting Management and "Independence"

The Revised Amendment removes the requirement that covered entities must document material issues found during vulnerability assessments or penetration testing and report those to senior management and the board. Part 500.4(d). However, according to NYDFS, this change was made because that provision was redundant, as the requirement already exists in 500.4(c), which provides that the CISO must timely report to the board on material cybersecurity issues.

Additionally, the Revised Amendment removes the word "independent" from the penetration testing section, making clear that such tests can be conducted using internal resources.

Changes to Multi-Factor Authentication ("MFA") Requirements

The Revised Amendment significantly increases the MFA requirements by providing that MFA "be utilized for any individual accessing any of the covered entity's information systems." Part 500.12(a). The only exceptions are for (a) small covered entities that meet the 500.19(a) exemption requirements, and for (b) covered entities with a CISO, where the CISO has approved in writing the use of reasonably equivalent or more secure compensating controls, which must be reviewed at least annually.

In its explanation for this change, the NYDFS states that the FTC Safeguards Rule requirement in 16 C.F.R. § 314.4(c)(5) would effectively require MFA in all instances because that provision requires MFA for any individual accessing any information system, unless the qualified individual responsible for overseeing the information security program and enforcing the information security program approves reasonably equivalent or more secure access controls. Similarly, according to the NYDFS, following zero-trust principles would effectively require MFA in all instances on all systems.

It is unclear whether these new MFA requirements would encompass employees who are accessing routine parts of the company network while using a computer at the office. It is possible that such devices would have a token associated with them that would count as a second factor, but this issue is worth clarifying during the comment process.

In addition to expanding the scope of MFA, NYDFS changed the definition of MFA in 500.1(i) in the Initial Amendment "to eliminate the reference to text message on a mobile phone." The Department has clarified that, while text message is still an acceptable form of MFA, it is a weaker form and that the Department encourages stronger forms of MFA that are more resistant to phishing.

Limiting Scope of Incident Response and Business Continuity to Cybersecurity

The Revised Amendment clarifies that incident response plans should be designed to address cybersecurity events rather than all disruptive events. Part 500.16(a). It also adds a requirement that such plans address preparing a root cause analysis that describes how

and why the event occurred, what business impact it had, and what will be done to prevent reoccurrence. Part 500.16(a)(1)(ix).

Similarly, the provisions in the Revised Amendment relating to business continuity have been changed to clarify that these requirements apply to cybersecurity-related disruptions, as opposed to all emergencies, and are limited to addressing the availability and functionality of the covered entity's information systems and material services rather than all services. Part 500.16(a)(2).

The Revised Amendment also clarifies that the backups that covered entities maintain must be able to restore material operations and be protected from unauthorized alterations or destruction. Part 500.16(e).

Notification Obligations

The Revised Amendment makes clear that a cyber incident must be reported to the NYDFS if it meets one of the four definitions of a notifiable event, even if the event occurred at a non-regulated affiliate or a third party. The four notifiable events are those:

- impacting the covered entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body;
- that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity (the words "disrupting or degrading" were removed after "harming");
- where an unauthorized user has gained access to a privileged account; or
- that resulted in the deployment of ransomware within a material part of the covered entity's information system. Part 500.17(a)(1)(i)-(iv).

Although three of these notification criteria require an impact on the covered entity, the trigger for unauthorized access to a privileged account does not, and the NYDFS should add that requirement in the final rule.

Note that the definition of "privileged account" in the Revised Amendment removes accounts that can be used to "affect a material change to the technical or business operations of the covered entity." Part 500.1(m). According to the NYDFS, this change was made to address comments that the definition of "privileged account" was

overbroad, but the NYDFS stressed that accounts that can perform security-relevant functions that ordinary users are not authorized to perform are still considered privileged accounts.

Additionally, the Initial Amendment required that each covered entity provide the NYDFS with any information requested regarding the investigation of the event within 90 days of the notice to the superintendent. This has been changed in the Revised Amendment and now requires covered entities to "promptly" provide any information requested by the NYDFS regarding such event, with a continuing obligation to update and supplement the information provided. Part 500.17(a)(2).

Materiality Threshold for Certification

Perhaps the most significant change in the Revised Amendment is the introduction of a materiality threshold for certification. Covered entities must now certify that they "materially complied with the requirements set forth in [Part 500] during the prior calendar year." Part 500.17(b)(1)(i)(i). The addition of the words "during the prior calendar year" strongly suggests that material compliance as of the date of the certification, or as of the last day of the previous calendar year, will not be viewed as satisfactory compliance for certification purposes if there was material noncompliance in the previous calendar year.

The same materiality threshold was added to the violation provisions in 500.20, which now provide that a violation of Part 500 includes the material failure to comply for any 24-hour period with any section in the regulation. Part 500.20(b)(2).

In the event that a covered entity cannot certify to material compliance, under the Revised Amendment, the written acknowledgment that must be sent to the NYDFS no longer requires the covered entity to identify all areas, systems, and processes that require material improvements, updating, or redesign, although this information must be maintained by the covered entity for examination and inspection by the NYDFS upon request. Part 500.17(b)(ii). The written acknowledgment still requires the covered entity to identify all sections of Part 500 that the covered entity did not materially comply with and describe the nature and extent of such noncompliance, along with a remediation timeline.

NYDFS Responses to Requests for Clarification

Several comments on the Initial Amendment requested clarification on the meaning of "qualified" personnel as it relates to requirements such as penetration testing. The Revised Amendments do not make any changes to the provisions that use the term "qualified," but according to NYDFS, the Revised Amendment does not prescribe any "particular level of education, experience or certification" and "[n]ecessary qualifications will depend upon the size and complexity of an organization's information system and the volume of the information maintained."

Commentators also sought clarification on the elimination of the third-party service provider exemption in 500.11(c), and the NYDFS clarified that the removal of this exemption was non-substantive because the exemption already exists in 500.19(b).

NYDFS also elected not to eliminate the requirement that CISOs "direct sufficient resources to implement and maintain the cyber program" but did note that the CISO is still subject to a covered entity's regular budgetary approval process. At the same time, the NYDFS did warn that "an insufficiently resourced cybersecurity program may result in a covered entity's non-compliance with Part 500 if the covered entity is otherwise unable to meet the other requirements contained in Part 500."

The NYDFS should reconsider this comment. A failure to direct sufficient resources to cybersecurity is often not a CISO issue, so if this obligation remains in the final version of Part 500, it should be placed with senior management.

Changes to Effective Dates

The Revised Amendment includes several changes to effective dates. Notably, the CISO and board cybersecurity governance requirements in 500.4 are now effective one year after the Amendment is adopted. Part 500.22(d)(2). Similarly, requirements for access privileges and management under 500.7 are now effective 18 months after adoption, and MFA requirements have an effective date of two years. Part 500.22(d)(3) and Part 500.22(d)(4).

Unaddressed Comments NYDFS Should Reconsider

There were several comments NYDFS declined to address that NYDFS should reconsider, including:

- *Changing the cadence of certain requirements*. The Revised Amendment retains annual requirements for the independent audit, policy and procedure review, penetration testing, user access privilege review, application security development review, testing of incident response plans and business continuity and disaster recovery plans with senior officers and the CEO, and the ability to restore critical data and information systems from backups. Instead of these prescriptive annual requirements, the NYDFS should allow companies to fulfill these requirements periodically, consistent with risks identified in the annual risk assessment, but at least once every three years.

- *Having the senior governing body, rather than senior management, approve cyber policies*. The NYDFS rejected calls to eliminate the requirement that governing bodies (boards or equivalent) approve their covered entity's cybersecurity policy, stating that boards "must be aware of cybersecurity risks and ensure the company has a written cybersecurity policy in place." While boards certainly need to be aware of cybersecurity risks to exercise oversight, it does not follow that they need to be the ones approving those policies. Instead, management should develop, approve, and implement the cybersecurity policies, and boards should be aware of those policies in order to effectively carry out their oversight obligations.

- *Eliminating the requirement that backups be stored offsite*. The Revised Amendment appears to continue to require that covered entities maintain backups offsite, as Part 500.16(a)(2)(v) requires BCDR plans to include procedures for backing up information offsite, and Part 500.16(e) requires covered entities to maintain backups. The Revised Amendments do limit the backup requirement in 500.16(e) to "backups necessary to restoring material operations," and NYDFS comments note that storage of information offsite is one way to satisfy the backup requirement. But the final rules should be explicit that the offsite requirement in 500.16(a)(2)(v) can be met with equivalent on-premises security.

The authors would like to thank Debevoise Summer Law Clerks Achutha Raman, Adam Shankman, and Michelle Shen for their contribution to this blog post.

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.

NEW YORK

Avi Gesser
agesser@debevoise.com

Erez Liebermann
eliebermann@debevoise.com

Ned Terrace
jkterrace@debevoise.com

Stephanie D. Thomas
sdthomas@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com