GIBSON DUNN

New York Department of Financial Services Proposes Updated Second Amendment to Cybersecurity Regulation

Client Alert | August 3, 2023

On June 28, 2023, the New York Department of Financial Services ("NYDFS") published a Revised Proposed Second Amendment to its Part 500 Cybersecurity Rules ("Revised Proposed Amendment"). This is the third draft NYDFS has put out for this round of amendments, following the initial Draft Proposed Second Amendment (released on July 29, 2022) and the issuance of the Proposed Second Amendment (released on November 9, 2022, and covered in our prior alert), and reflects NYDFS' response to stakeholder comments.

We highlight seven key takeaways of the Revised Proposed Amendment:

- Reduce requirements for audits, risk assessments, and penetration testing;
- Reduce governance requirements;
- Change notification requirements;
- Expand requirements for multi-factor authentication;
- Change requirements for incident response and business continuity and disaster recovery plans;
- Clarify certification requirements; and
- Clarify penalties.

1. **Reduced Requirements for Audits, Risk Assessments, and Penetration Testing**

In the initial Proposed Second Amendment, NYDFS imposed strict requirements that those conducting audits, risk assessments, and penetration testing be independent, including specifically requiring external experts to conduct audits and risk assessments. Public commenters focused on these requirements, noting concerns about potential costs (e.g., from hiring an outside vendor), limits on human capital (e.g., taking staff away from critical operations to ensure the independence of an internal party), and backlogs (e.g., due to the increased demand for external vendors). Appearing to acknowledge these concerns, and the implicit assumption that using external vendors does not guarantee additional value, NYDFS modified the independence requirements in the Revised Proposed Amendment. Specifically, the Revised Proposed Amendment includes three such modifications:

1. The definitions are revised to clarify that while Class A companies[1] need to conduct independent audits, such audits can now be conducted by internal auditors rather than only by external auditors, as long as the auditors are free to make their decisions without influence from the covered entity. This change realigns the Revised Proposed Amendment with the initial Draft Proposed Second

Related People

Vivek Mohan

Stephenie Gosnell Handler

Terry Wong

Ruby B. Lang

Amendment from July 2022, which also specified that audits could be conducted by internal or external auditors.

2. The requirement that Class A companies use external experts to conduct risk assessments at least once every three years is removed. The relevant section no longer mentions experts and only requires risk assessments be reviewed and updated at least annually and whenever a change in the business or technology causes a "material change."[2]
3. The scope of who can conduct penetration testing is expanded to include any "qualified internal or external party," removing the requirement that the party be independent.

2. Reduced Governance Requirements

In the Proposed Second Amendment, NYDFS required that the board of directors have "sufficient expertise and knowledge," or be advised by persons with sufficient expertise and knowledge, to effectively oversee cybersecurity risk management. Noting that the phrase "expertise and knowledge" is vague, NYDFS clarified that it did not intend to suggest that cybersecurity experts are required on the board, but meant that a board should have sufficient understanding of cybersecurity-related matters. NYDFS therefore revised this section to require *effective* oversight of the entity's cybersecurity risk management and "sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors."

NYDFS also removed the requirement that senior governing bodies "provide direction to management" on cybersecurity risk management because of confusion that this implied the board should become involved in the day-to-day management of the covered entity's cybersecurity program. NYDFS clarified that the board's job is to determine the strategic direction of the entity, while the day-to-day management of the cybersecurity program should be handled by management.

3. Changes to Notification Requirements

The Revised Proposed Amendment expands the requirements around notification of cybersecurity events. Specifically, covered entities must notify NYDFS regarding security events that occur not only at the covered entity, but also those that occur at an affiliate or third-party service provider. This is a notable expansion of NYDFS' notification requirement.

In its Assessment of Public Comments, NYDFS provided guidance clarifying that notification is required where cybersecurity events at third-party service providers: (i) require notice to a government body, self-regulating agency, or any other supervisory body; or (ii) have a reasonable likelihood of materially harming any material part of the normal operations of the covered entity. While NYDFS is not explicit about this, the same threshold can likely be applied to affiliates, which are defined in the Cybersecurity Regulation as "any person that controls, is controlled by, or is under common control with another person." In response to public requests to clarify or delete the term "affiliate," NYDFS commented that this term is clearly defined.

The requirement that, following initial notification, entities provide NYDFS with information requested to assist with investigating events within 90 days was met with objections from commenters suggesting it would be difficult or impossible to meet this deadline. In response, NYDFS relaxed this specific timetable requirement and the Revised Proposed Amendment now provides that requested information must be provided "promptly."

4. Expanded Requirements for Multi-Factor Authentication

Requirements related to multi-factor authentication are notably expanded in the Revised Proposed Amendment to require multi-factor authentication for any individual who

accesses a covered entity's information system. There are exceptions to these requirements for small covered entities that meet certain criteria and where "reasonably equivalent or more secure compensation controls" are used, which must be reviewed by the chief information security officer and approved in writing at least annually. These expanded requirements for multi-factor authentication are now more aligned with those outlined in the FTC Safeguards Rule (a federal regulation requiring financial institutions develop, implement, and maintain an information security program to protect customer information). In its past enforcement actions, NYDFS has often alleged violations of the Cybersecurity Regulation's provisions covering multi-factor authentication. Covered entities should therefore be careful to ensure compliance with these new expanded requirements.

5. **Changes to Requirements for Incident Response and Business Continuity and Disaster Recovery Plans**

On incident response plans, the Revised Proposed Amendment makes a number of changes, including narrowing the requirement that incident response plans address ways to specifically mitigate "disruptive" events to just "cybersecurity" events. NYDFS made this change to address concerns that "disruptive event" was undefined and therefore might include events that are not cybersecurity events. Signaling the importance of determining the root cause of a cybersecurity event, NYDFS also added a requirement that, as part of the incident response plan, covered entities prepare 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."

There are also updates to the requirements around business continuity and disaster recovery ("BCDR") plans, including specifying that BCDR plans should include procedures to enable the timely recovery of "critical data and information systems" rather than "data and documentation." The Revised Proposed Amendment additionally specifies that covered entities must maintain "backups necessary to restoring material operations" that are "adequately protected from unauthorized alterations or destruction."

Consistent with the Proposed Second Amendment, both incident response plans and BCDR plans must be tested at least annually.

6. **Clarification of Certification Requirement**

The Revised Proposed Amendment changes the obligation that covered entities submit written confirmation to NYDFS of compliance with the Part 500 requirements by qualifying that only "material" compliance "during the prior calendar year" must be certified. This materiality qualifier was added in direct response to a comment requesting it. Although NYDFS does not provide a specific definition for what constitutes "material" compliance, this update will presumably make it easier for covered entities to achieve certification.

The second change, made in response to concerns that remediation during the year would prevent a covered entity from submitting a certification of compliance, suggests that material compliance at the time of submission, or the last day of the prior calendar year, is not adequate to certify compliance. Where a covered entity does not fully comply with the requirements, they must submit a written acknowledgment identifying the requirements they did not materially comply with, describing such noncompliance, and providing a remediation timeline.

In several recent enforcement actions, NYDFS found violations of the certification requirement where covered entities that have been subject to cybersecurity events, raising concerns that NYDFS is imposing effectively a strict liability regime. Adding a materiality qualifier suggests that a threat actor's success in obtaining unauthorized access to data does not itself evidence a violation of the Cybersecurity Regulation.

7. **Clarification of Penalties**

The Revised Proposed Amendment provides additional clarity on the factors NYDFS should consider in assessing any penalty by adding a new criterion—the extent to which the relevant policies comply with nationally recognized cybersecurity frameworks.

It is also worth noting that the Revised Proposed Amendment changes the transitional periods for several sections, extending most of the effective dates.

Next Steps

This alert is not an exhaustive list of the changes contained in the Revised Proposed Amendment, but provides a high-level overview of the updates from NYDFS' Proposed Second Amendment. The Revised Proposed Amendment will be subject to an additional 45-day comment period, which ends on August 14, 2023. Pending further revisions, the amendment will take effect following the updated transitional periods.

The Revised Proposed Amendment demonstrates NYDFS' continued efforts to weigh comments received while also ensuring covered entities are taking preventative measures to protect customer information and information technology systems from new and evolving threats. This underscores NYDFS' risk-based approach to cybersecurity. Covered entities should review these requirements and ensure they have appropriate measures in place to comply if they are finalized.

---

[1] In the initial Draft Proposed Second Amendment, NYDFS established a group of larger companies it titled "Class A companies" to be subject to heighted compliance requirements. The Revised Proposed Amendment narrows the companies that qualify as "Class A companies" by revising this term's definition to specify that when calculating the number of employees and gross annual revenue, affiliates should only include "those that share information systems, cybersecurity resources or all or any part of a cybersecurity program with the covered entity."

[2] The definition of "risk assessment" is also revised to remove the requirement that such assessments "take into account the specific circumstances of the covered entity," such as size, business, products, and location.

The following Gibson Dunn lawyers assisted in preparing this alert: Alexander Southwell, Vivek Mohan, Stephenie Gosnell Handler, Terry Wong, and Ruby Lang.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity & Data Innovation practice group:

United States S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com) Jane C. Horvath – Co-Chair, PCDI Practice, Washington, D.C. (+1 202-955-8505, jhorvath@gibsondunn.com) Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com) Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com) Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com) David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com) Gustav W. Eyler – Washington, D.C. (+1 202-955-8610, geyler@gibsondunn.com) Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com) Svetlana S. Gans – Washington, D.C. (+1 202-955-8657, sgans@gibsondunn.com) Lauren R. Goldman – New York (+1 212-351-2375, lgoldman@gibsondunn.com) Stephenie Gosnell Handler – Washington, D.C. (+1 202-955-8510, shandler@gibsondunn.com) Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com) Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com) Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com) Vivek Mohan – Palo Alto (+1

650-849-5345, vmohan@gibsondunn.com) Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com) Rosemarie T. Ring – San Francisco (+1 415-393-8247, rring@gibsondunn.com) Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com) Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com) Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com) Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com) Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)

Europe Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com) Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com) Joel Harrison – London (+44(0) 20 7071 4289, jharrison@gibsondunn.com) Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com)

Asia Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com) Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)

Related Capabilities

Privacy, Cybersecurity, and Data Innovation

Artificial Intelligence