Schulte Roth&Zabel

Alert

NYDFS Continues Effort to Amend Cybersecurity Regulation ("Part 500") and Publishes Revised Proposed Amendments

November 23, 2022

On Nov. 9, 2022, the New York Department of Financial Services ("NYDFS") published a proposed amendment ("Proposed Amendment")[1] to its 2017 cybersecurity regulation ("Part 500"), which requires certain NYDFS-regulated financial services companies to, among other things, safeguard consumer data and adopt and implement a cybersecurity program. The Proposed Amendment is subject to a 60-day notice and comment period, which will be open until Jan. 9, 2023. Based on NYDFS' review of any comments received, NYDFS will either propose further revisions to the Proposed Amendment or adopt the final regulation.

The Proposed Amendment is the NYDFS' second rulemaking in its effort to amend Part 500, and follows NYDFS' Pre-Proposed Amendment, which was published on July 29, 2022 (the "Pre-Proposed Amendment").[2] The Proposed Amendment generally maintains most of the material changes reflected in the Pre-Proposed Amendment, as well as imposing certain additional regulatory burdens. Key changes in the Proposed Amendment include: (1) a revised definition of "Class A companies" that is narrower than the definition included in the Pre-Proposed Amendment, so that only entities with large New York operations are subject to the heightened requirements applicable to such companies;[3] (2) requiring increased accountability for cybersecurity governance at the board of directors and C-suite levels; (3) allowing more risk-based controls to prevent initial unauthorized systems access and the spread of a cyberattack than those included in the Pre-Proposed Amendment, such as allowing the Chief Information Security Officer ("CISO") to authorize reasonable alternatives to NYDFS-prescribed multi-factor authentication requirements; (4) putting in place additional requirements to those included in the Pre-Proposed Amendment for incident response, business continuity and disaster recovery testing and training; (5) adding further NYDFS reporting requirements to those included in the Pre-Proposed Amendment; and (6) proposing different implementation periods for certain requirements as compared with the Pre-Proposed Amendment. Each of these key changes is discussed in turn below.

---

[1] *See* Proposed Amendment, available here. Part 500, which originally went into effect on March 1, 2017, establishes cybersecurity requirements for any person or entity "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the [New York] Banking Law, the [New York] Insurance Law or the [New York] Financial Services Law." 23 NYCRR § 500.1(c). Additional information on Part 500 is available on the NYDFS website.

[2] The Pre-Proposed Amendment was subject to a short pre-proposal comment period, which ended Aug. 18, 2022. For additional information regarding the Pre-Proposed Amendment, please see our prior *Alert* "NYDFS Publishes Pre-Proposed Amendment to Cybersecurity Regulations ('Part 500')."

[3] Part 500 does not currently include the term "Class A companies."

1. Class A Companies

- *Definition*. The Proposed Amendment narrows the definition of "Class A companies" so that only larger entities are subject to the heightened requirements applicable to such companies. A "Class A company" is defined in the Proposed Amendment to only include a covered entity with at least $20 million in gross annual revenue in each of the last two fiscal years from the New York operations of the covered entity and its affiliates; and either (1) over 2,000 employees averaged over the last two fiscal years, including both those of the covered entity and all of its affiliates regardless of location; *or* (2) over $1 billion in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and all of its affiliates. The Pre-Proposed Amendment previously defined "Class A companies" to include firms with either (1) over 2,000 employees or (2) over $1 billion in gross annual revenue averaged over the previous three years from all business operations of the covered entity and its affiliates, which would have covered a broader range of entities.
- *Privileged Access and Password Management*. Additionally, whereas the Pre-Proposed Amendment required Class A companies to implement a password vaulting solution for privileged accounts, the Proposed Amendment replaces this solution with requirements that Class A companies implement (1) a privileged access management solution, and (2) an automated method for blocking commonly used passwords for all accounts. If it is not feasible to implement an automated password blocking solution, a Class A company's CISO would be required to approve in writing reasonably equivalent controls on an annual basis.

2. Increased Accountability for Cybersecurity at the Leadership Level

- *CISO*. Currently, each covered entity must designate a CISO pursuant to Part 500. The Pre-Proposed Amendment introduced a requirement that the CISO have "adequate independence and authority" to ensure cybersecurity risks are appropriately managed. The Proposed Amendment, however, removes the term "independent" and adds a requirement that the CISO must be able to direct sufficient resources to implement and maintain a cybersecurity program. Additionally, like the Pre-Proposed Amendment, the Proposed Amendment includes a new requirement that the CISO report in writing on the cybersecurity program to the covered entity's "senior governing body"[4] at least annually. The Proposed Amendment also includes a new requirement and specifies that the report must include plans for remediating material inadequacies in the covered entity's cybersecurity program.
- *Senior Governing Body*. The Proposed Amendment adds a new governance requirement, not previously included in the Pre-Proposed Amendment, mandating that a covered entity's senior governing body must have sufficient cybersecurity expertise or be advised by persons that have such expertise. It also includes a new requirement that covered entities have in place written cybersecurity policies and procedures subject to approval at least annually by the firm's senior governing body.

[4] "Senior governing body" is defined to mean "the covered entity's board of directors (or an appropriate committee thereof) or equivalent governing body or, if neither of those exist, the senior officer of the covered entity responsible for the covered entity's cybersecurity program." Proposed § 500.1(p).

3. Risk-Based Controls to Prevent Unauthorized Systems Access and the Spread of a Cyberattack

- *Multi-Factor Authentication*. Part 500 currently provides for the CISO's ability to approve in writing reasonably equivalent or more secure compensating controls in lieu of NYDFS-prescribed multi-factor authentication requirements subject to the CISO's annual review. The Pre-Proposed Amendment[5] eliminated this ability, but the Proposed Amendment adds it back in.
- *Access Privileges*. The Proposed Amendment adds a new requirement (not included in the Pre-Proposed Amendment) that covered entities review access privileges at least annually and that such entities ensure that unnecessary accounts and access privileges are terminated.
- *Password Policy*. The Proposed Amendment requires covered entities that utilize passwords as a method of authentication to implement a written password policy that meets industry standards — a new requirement not included in the Pre-Proposed Amendment.

4. Enhanced Requirements for Vulnerability Management, Penetration Testing and Incident Response, Business Continuity, and Disaster Recovery Testing and Training

- *Vulnerability Management and Penetration Testing*. Part 500 currently requires covered entities that do not continuously monitor their information systems to conduct annual penetration testing of such systems. The Pre-Proposed Amendment added a requirement that penetration testing be conducted by a qualified independent party. The Proposed Amendment, in turn, specifies that such a qualified independent party could be either internal (e.g., a firm employee) or external (e.g., a third-party provider or outside expert), and that testing specifically address unauthorized access through social engineering, and adds a new requirement, not previously included in the Pre-Proposed Amendment, that covered entities develop and implement written policies and procedures for vulnerability management. Further, the Proposed Amendment requires penetration testing to be conducted at least annually *in addition to* the automated scanning of information systems and a manual review of systems not covered by the scans, whereas the Pre-Proposed Amendment required that covered entities *either* perform penetration testing *or* conduct continuous scans. Additional requirements introduced in the Proposed Amendment include: (1) putting in place monitoring systems to promptly alert the covered entity to cybersecurity vulnerabilities; (2) timely remediating such vulnerabilities; (3) documenting material issues during testing; and (4) reporting the same to the firm's senior management and senior governing body.
- *Incident Response, Business Continuity and Disaster Recovery Testing and Training*. The Proposed Amendment adds new requirements, not previously included in the Pre-Proposed Amendment, that covered entities (1) test their incident response and business continuity and disaster recovery plans, at least annually, with the participation of all applicable staff (including senior management); and (2) provide relevant training to all employees responsible for implementing such plan.

[5] Proposed § 500.12(b).

5. Additional Reporting Requirements[6]

Part 500 currently only requires reporting to NYDFS cybersecurity events that have a material likelihood of harming the covered entity's operations. The Pre-Proposed Amendment added additional requirements for covered entities to notify NYDFS within *72 hours* of any cybersecurity event in which an unauthorized user has gained access to a privileged account or any cybersecurity event in which ransomware was deployed within a material part of such covered entity's systems, as well as within *24 hours* of any extortion payment made in connection with a cybersecurity event. Documentation regarding the covered entity's investigation of a reportable cybersecurity event must be provided to the NYDFS electronically within *90 days* of such covered entity's initial report of the event to the NYDFS. The Proposed Amendment, in turn, preserves these requirements and adds to them a new requirement that covered entities notify NYDFS within *72 hours* of becoming aware of a cybersecurity event at a third-party service provider if it affects the covered entity.

6. Revised Transitional Implementation Periods for Certain Technical Requirements[7]

Although the NYDFS rulemaking would generally become effective 180 days from the date of publication of the Notice of Adoption in the State Register ("Effective Date"), the Proposed Amendment establishes different timelines for compliance with certain requirements proposed therein. For example, covered entities would have (i) *30 days* from the Effective Date to comply with the new NYDFS notice requirements; (ii) *one year* from the Effective Date to comply with the Proposed Amendment's data backup requirements*;* (iii) *18 months* from the Effective Date to comply with the new requirement to conduct automated or manual scans of information systems as set forth in the Proposed Amendment; and (iv) *two years* from the Effective Date to comply with the requirement that covered entities implement written policies and procedures designed to ensure a complete, accurate and documented asset inventory.[8]

Conclusion

If adopted as a final rule, coming into compliance with the Proposed Amendment is likely to require substantial time, effort and resources for covered entities, especially in light of the NYDFS' 180-day implementation period.

Firms that are subject to Part 500 may wish to comment on aspects of the Proposed Amendment that they believe, for example, would be unduly burdensome or do not sufficiently reflect the operational considerations faced by industry members. They should also consider instances where they believe exemptions or exceptions should apply. Firms may also wish to seek clarification on how the Proposed Amendment would impact other areas of compliance. Comments on the Proposed Amendment must be submitted to the NYDFS before Jan. 9, 2023.

[6] *See* Proposed § 500.17.

[7] Proposed § 500.22(d).

[8] *See* Proposed §§ 500.22(d)(4), 500.13(a).

Schulte Roth & Zabel's lawyers are available to assist you in preparing a public comment or addressing any questions you may have regarding these developments. Please contact the Schulte Roth & Zabel lawyer with whom you usually work, or any of the following attorneys:

Donald J. Mosher – New York (+1 212.756.2187, donald.mosher@srz.com)
Alexander M. Kim – New York (+1 212.756.2075, alex.kim@srz.com)
Melissa G.R. Goldstein – Washington, DC (+1 202.729.7471, melissa.goldstein@srz.com)
Kara A. Kuchar – New York (+1 212.756.2734, kara.kuchar@srz.com)
Adam J. Barazani – New York (+1 212.756.2519, adam.barazani@srz.com)
Jessica Romano – New York (+1 212.756.2205, jessica.romano@srz.com)
Jessica Sklute – New York (+1 212.756.2180, jessica.sklute@srz.com)
Noah N. Gillespie – Washington, DC (+1 202.729.7483, noah.gillespie@srz.com)
Hadas A. Jacobi – New York (+1 212.756.2055, hadas.jacobi@srz.com)
Rebecca A. Raskind – New York (+1 212.756.2396, rebecca.raskind@srz.com)
Jesse Weissman – New York (+1 212.756.2460, jesse.weissman@srz.com)

Schulte Roth & Zabel
New York | Washington DC | London
www.srz.com