Schulte Roth&Zabel

Alert

NYDFS Publishes Pre-Proposed Amendment to Cybersecurity Regulations ("Part 500")

August 15, 2022

On July 29, 2022, the New York State Department of Financial Services ("NYDFS") published pre-proposal amendments ("Proposed Amendments")[1] to its cybersecurity regulations ("Part 500").[2] While NYDFS will be accepting comments on the Proposed Amendments through its website until Aug. 18, 2022, there will still be a full 60-day notice and comment period before the amendments are final.

Key provisions of NYDFS's Proposed Amendments include: (1) new notification requirements; (2) new obligations for "Class A" companies; (3) new requirements concerning entity governance; (4) modifications to the compliance certification requirement; and (5) clarifications around penalties.

1. Notification Requirements

The Proposed Amendments would add additional reporting requirements, including the requirement to notify the NYDFS within 72 hours of any unauthorized access to privileged accounts or deployment of ransomware within a material part of an entity's information systems. It should be noted that this requirement is in addition to the already existing requirement to notify NYDFS within 72 hours of any cybersecurity events that require notice to any supervisory body or that have a reasonable likelihood of materially harming a material part of an entity's normal operations. Furthermore, the Proposed Amendments would add a new 24-hour notification obligation for ransomware payments, and a corresponding 30-day reporting requirement within which an entity must provide a written explanation of why payment was necessary, alternatives to payment that were considered and sanctions diligence that was conducted.

2. Obligations for Class A Companies

The Proposed Amendments would impose requirements on a new category of covered entities, "Class A" companies, which are defined as covered entities 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. Under the Proposed Amendments, Class A companies must: (1) conduct independent audits of the cybersecurity program, at least annually; (2) conduct vulnerability assessments (such as systematic scans or reviews) at least weekly; (3) implement mandatory password vaulting solutions for privileged accounts; (4) maintain an endpoint detection and response solution to

[1] *See* Proposed Second Amendment to 23 NYCRR 500, available here.

[2] Compliance with Part 500 is required 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." *See* 23 NYCRR 500.1(c).

monitor anomalous activity, as well as a solution for centralized logging and security event alerting; and (5) utilize external experts to conduct a risk assessment at least once every three years.

3. Enhanced Governance Requirements

The Proposed Amendments would add additional requirements concerning entity governance. More specifically, the Proposed Amendments would require that, among other additional obligations: (1) the Chief Information Security Officer ("CISO") have adequate independence and authority to ensure appropriate management of cybersecurity risks; (2) the CISO provide the board with additional detailed annual reporting on plans for remediating inadequacies, as well as timely reports regarding material cybersecurity issues or events; (3) the entity's cybersecurity policy be approved by the board, rather than senior management; and (4) an entity's board have sufficient knowledge and expertise (or be advised by persons with sufficient knowledge and expertise) to exercise effective oversight of cybersecurity risk.

4. Certification/Acknowledgment of Compliance Modifications

The Proposed Amendments would require that the annual certification of compliance be signed by the CEO and the CISO (or the CEO and senior officer responsible for the cybersecurity program where the entity lacks a CISO). The Proposed Amendments would also allow entities to submit an acknowledgment of less-than-full compliance for the prior calendar year. An entity which submits an acknowledgment of less-than-full compliance must also identify the cybersecurity program's specific deficiencies, describe the nature and extent of noncompliance and identify the systems, areas and processes which require material improvement, updating or redesign. Furthermore, an entity which submits an acknowledgment of less-than-full compliance must be ready to provide NYDFS with documentation detailing the remedial efforts planned and underway, along with a timeline for implementing those efforts.

5. Penalty Clarifications

The Proposed Amendments would provide additional clarity concerning NYDFS's penalty calculation process. For example, the Proposed Amendments note that the commission of a single act prohibited by Part 500, or the failure to satisfy an obligation required by Part 500, constitutes a violation, including an entity's failure to comply for any 24-hour period with any section or subsection of Part 500. In addition, the Proposed Amendments include a list of factors that NYDFS will consider when assessing a penalty (e.g., cooperation, good faith, isolated incident v. systemic violations, etc.).

Moving Forward

While this *Alert* is not an exhaustive list of the modifications contained in the Proposed Amendments, it is intended to highlight key provisions of the Proposed Amendments, should these proposed provisions be finalized and adopted.

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)
Kara A. Kuchar – New York (+1 212.756.2734, kara.kuchar@srz.com)
Melissa G.R. Goldstein – Washington, DC (+1 202.729.7471, melissa.goldstein@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)
Steven T. Cummings – New York (+1 212.756.2251, steven.cummings@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