King & Spalding

Client Alert

Providing Strategic Legal Guidance to the Global Financial Services Industry

FINANCIAL SERVICES

AUGUST 24, 2022

For more information, contact:

Jarno Vanto
+1 212 556 2210
jvanto@kslaw.com

William Johnson
+1 212 556 2125
wjohnson@kslaw.com

William Sadik-Khan
+1 212 790 5323
bsadik-khan@kslaw.com

King & Spalding

New York
1185 Avenue of the Americas
New York, New York 10036-4003
Tel: +1 212 556 2100

New York Department of Financial Services Proposes New Cybersecurity Rules

On July 29, 2022, the New York Department of Financial Services ("NYDFS") released Draft Amendments to its Part 500 Cybersecurity Rules, which propose substantial new obligations for the cybersecurity programs of companies subject to these rules. Companies should closely review the Draft Amendments and consider providing comments. A brief pre-proposal comment period ended on August 18, 2022. As a next step, the NYDFS will publish the official proposed amendments, which will be followed by a 60-day comment period. This article provides a high-level overview of the changes contained in the Draft Amendments.

NEW OBLIGATIONS FOR LARGE COMPANIES

The Part 500 cybersecurity requirements currently apply to all "covered entities," which include any person operating under or required to operate under a license, registration, charter, certificate or similar authorization under the Banking Law, the Insurance Law, or the Financial Services Law. The Draft Amendments propose the creation of a new subcategory of larger covered entities, called "Class A companies," which would be subject to additional security and auditing requirements in addition to the general requirements that apply to all covered entities. Class A companies are defined as covered entities with over 2,000 employees or over $1,000,000,000 in gross annual revenue averaged over the last three fiscal years. If implemented as currently proposed, the Draft Amendments would impose the following new requirements upon Class A companies:

- Conduct an annual independent audit of their cybersecurity programs;
- Use external experts to conduct a risk assessment at least once every three years;
- Conduct systematic scans or reviews of information systems at least weekly, rather than the current bi-annual review requirement;

- Implement an endpoint detection and response solution to monitor anomalous activity, including lateral movement, as well as a solution that centralizes logging and security event alerts; and
- Implement certain password security measures for "privileged accounts."
    - A "privileged account" is a newly defined term in the Draft Amendments that refers to accounts that can be used to: 1) perform security-relevant functions that ordinary users are not authorized to perform, or 2) effect a material change to the technical or business operations of the covered entity.

Although these proposed changes to Part 500 are specific to covered entities that are also Class A companies, the following proposals would apply to all covered entities, including Class A companies, if adopted.

EXPANDED NOTIFICATION REQUIREMENTS

Part 500 currently requires covered entities to notify the NYDFS, within 72 hours, of any cybersecurity event that: 1) has a reasonable likelihood of harming a material part of the normal operation of the covered entity, or 2) impacts the covered entity and notice is required to be provided to any government body, self-regulatory agency, or any other supervisory body. Under the Draft Amendments, the 72-hour notification obligations would be expanded to also require notice of:

- Cybersecurity events where an unauthorized user has gained access to a privileged account; or
- Cybersecurity events that resulted in the deployment of ransomware within a material part of the covered entity's information system.

GOVERNANCE

The Draft Amendments include new minimum requirements for the cybersecurity policies and governing bodies of covered entities. Part 500 already requires that every covered entity designate a chief information security officer (CISO), implement and maintain written cybersecurity policies, and provide its board with an annual report on the entity's cybersecurity program. The Draft Amendments include several additional measures that build on these obligations, including:

- A requirement that the CISO has adequate independence and authority to ensure cybersecurity risks are appropriately managed;
- The CISO must present an annual written report to the covered entity's senior governing body that addresses, at a minimum, five topics described in the regulation and the company's plans for remediating inadequacies identified therein;
    - Currently, Part 500 only requires the CISO to "consider," rather than "address" the five topics, does not require remediation plans, and does not require a written report.
- The board of a covered entity must have sufficient expertise and knowledge, or be advised by persons with sufficient expertise or knowledge, to exercise effective oversight of cyber risk and a committee or subcommittee assigned responsibility for cybersecurity;
- The CISO must timely report to the senior governing body regarding material cybersecurity issues, such as updates to the covered entity's risk assessment or major cyber events;
- Additional detailed requirements for business continuity and disaster recovery plans; and
- Covered entities must periodically test their incident response and disaster recovery plans with all staff critical to the continuity and response efforts, including senior officers.

RISK ASSESSMENTS

The Draft Amendments do not change the substantive requirements of risk assessments, but would require covered entities to:

- Conduct an impact assessment whenever a change in the business or technology causes a material change to the covered entity's cyber risk;
- Update their risk assessment at least annually;
- Use external experts to conduct a risk assessment at least once every three years; and
- When performing a risk assessment, take into account their own "specific circumstances," such as size, staffing, products, customers, services providers, counterparties, and the geographies of its operations.

DATA SECURITY AND RETENTION

Part 500 currently requires that covered entities have policies and procedures for the secure disposal of nonpublic information on a periodic basis and limit user access privileges to information systems that provide access to nonpublic information. The Draft Amendments would also obligate covered entities to:

- Implement written policies and procedures design to ensure a complete, accurate, and documented asset inventory that tracks key information for each asset;
    - Under the Draft Amendments, this "key information" includes, as applicable, the following: owner, location, classification or sensitivity, support expiration date, and recovery time requirements.
- Limit user access privileges to nonpublic information to those necessary to perform the user's job;
- Limit the use of privileged accounts to instances when performing functions requires the use of such access;
- Periodically review all user access privileges and remove accounts and access that are no longer necessary;
- Disable or securely configure all protocols that permit remote control of devices;
- Ensure strong, unique passwords are used, to the extent passwords are employed as a method of authentication; and
- Implement multifactor authentication for all privileged accounts, except for service accounts.

ENFORCEMENT

Finally, the Draft Amendments provide clarification on the conduct sufficient to constitute a violation under Part 500 and the factors the NYDFS will consider when assessing penalties:

- The failure to comply with any section or subsection of Part 500 for a 24-hour period is a violation of that section or subsection;
- The commission of a single act prohibited by Part 500 constitutes a violation;
- In assessing penalties, the NYDFS may consider the covered entity's: cooperation, good faith, intent, history of prior violations, harm to customers, the gravity of the violations, the participation of senior management, etc.

NEXT STEPS

Companies subject to the New York cybersecurity regulation should begin to evaluate the extent to which their cyber programs are compliant with these new requirements. Covered entities may need to invest significant time and resources to implement the final Part 500 amendments and, if adopted, most of these changes would take effect only 180 days following their adoption. However, the new notification obligations would become effective 30 days after the adoption of the Draft Amendments and many of the data security-related changes would take effect one year after adoption. Companies subject to Part 500 should consider whether they want to comment on the proposed regulations and how significantly their cyber programs would need to change in response to the Draft Amendments.