Cullen | Dykman

New York State Cybersecurity Regulation Expanded to Include New Requirements

December 4, 2023

The New York Department of Financial Services ("NYDFS") announced the adoption of the second amendment to its Cybersecurity Regulation[1] (the "Second Amendment"), expanding a number of requirements imposed under the existing regulation.

The Second Amendment took effect on November 1, 2023; however, there are some transitional periods defining the dates by which covered entities[2] will need to demonstrate compliance with the new provisions.

I. Summary of Key Changes

Compliance Obligations for Newly-Defined "Class A Companies"

The Second Amendment introduces new requirements for larger entities referred to as "Class A Companies." The Cybersecurity Regulation did not previously have separate requirements for large companies. A "Class A Company" is a covered entity with (1) at least $20 million in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and the business operations in New York State of the covered entity's affiliates and (2) either (i) more than 2,000 employees averaged over the last two fiscal years, including employees of both the covered entity and all of its affiliates no matter where located; or (ii) 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 no matter where located. For purposes of calculating revenue and employee thresholds, covered entities should include all affiliates with which they share information systems, cybersecurity resources, or any part of its cybersecurity program.

While most of the changes in the Second Amendment will apply uniformly to all covered entities, a Class A Company is subject to stricter compliance obligations, including requirements to (1) design and conduct independent audits of its cybersecurity program; (2) monitor user privileged access activity, including by implementing a privileged access management system and an automated method of blocking commonly used passwords for all accounts; and (3) implement endpoint detection and response solutions to monitor anomalous activity and a centralized logging and security event alerting solution, unless the covered entity's Chief Information Security Officer ("CISO") approves, in writing, a reasonable equivalent or more secure compensating controls.

Additional Reporting Requirements

The Second Amendment expands and clarifies the scope of Section 500.17 which sets forth the requirement that covered entities notify NYDFS of certain cybersecurity incidents. These updated notification requirements are effective beginning on December 1, 2023.

In addition to the 72-hour notification requirement for certain cybersecurity incidents, the Second Amendment creates additional notification obligations for covered entities in the event the covered entity makes an extortion payment in connection with a cybersecurity event. Specifically, a covered entity must notify the superintendent of the payment within 24 hours via the NYDFS website and, within 30 days of payment, provide a written description of the reasons payment was necessary, a description of alternatives to payment considered, all diligence performed to find alternatives to payment and all diligence performed to ensure compliance with applicable rules and regulations including those of the Office of Foreign Assets Control.

New Governance Requirements

Section 500.4 now requires that a "senior governing body"—a new term in the Cybersecurity Regulation—oversee a covered entity's cybersecurity risk management. A senior governing body is defined as the board of directors (or an appropriate committee thereof) or equivalent governing body or, if neither of those exist, the senior officer or officers of a covered entity responsible for the covered entity's cybersecurity program. As part of its oversight responsibilities, the senior governing body must have "sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors," require management to "develop, implement and maintain the covered entity's cybersecurity program," receive and review regular "management reports about cybersecurity matters," and confirm that management has "allocated sufficient resources to implement and maintain an effective cybersecurity program."

Additionally, the covered entity's CISO must timely report any material cybersecurity issues, including significant updates to the covered entity's cybersecurity program or significant cybersecurity events, to the covered entity's senior governing body. While a covered entity's CISO has been required under the Cybersecurity Regulation to provide annual written reports to a covered entity's board, the Second Amendment requires this annual report be provided to the senior governing body, and to include "plans for remediating material inadequacies" that may be identified in the covered entity's security program.

Requirements for Written Plans, Policies and Procedures

Section 500.16's existing requirement to establish a written incident response plan has been expanded in the Second Amendment. The incident response plan is now required to provide for recovery from backups and for the preparation of 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."

Section 500.16 also includes a new requirement that a covered entity maintain a business continuity and disaster recovery ("BCDR") plan reasonably designed to ensure the availability and functionality of a covered entity's services and protect the covered entity's personnel, assets, and nonpublic information in the event of a cybersecurity-related disruption. The BCDR plan must, at minimum:

1. Identify documents, data, facilities, infrastructure, services, personnel and competencies essential to the continued operations of the covered entity's business;
2. Identify the supervisory personnel responsible for implementing each aspect of the BCDR plan;
3. Include a plan to communicate with essential persons in the event of a cybersecurity-related disruption to the operations of the covered entity, including employees, counterparties, regulatory authorities, third-party service providers, disaster recovery specialists, the senior governing body and any other persons essential to the recovery of documentation and data and the resumption of operations;
4. Include procedures for the timely recovery of critical data and information systems and to resume operations as soon as reasonably possible following a cybersecurity-related disruption to normal business activities;
5. Include procedures for backing up or copying, with sufficient frequency, information essential to the operations of the covered entity and storing such information offsite; and
6. Identify third parties that are necessary to the continued operations of the covered entity's information systems.

Note that copies of both a covered entity's incident response plan and its BCDR plan must be distributed to or accessible by all employees necessary to implement them. Under the Second Amendment, a covered entity must provide relevant training on both its incident response plan and BCDR plan to all employees who are necessary to implement such plans, test both plans at least annually "with all staff and management critical to the response," and "revise the plan as necessary."

In addition, under Section 500.3, the required contents of a covered entity's written cybersecurity policies must be approved at least annually by the senior governing body or a senior officer. Section 500.3 requires covered entities to develop, document, and implement procedures in accordance with those policies. Specifically, a covered entity's policies must now address data retention, asset and device end of life management, remote access controls, security awareness and training, systems and application security, incident notification, and vulnerability management.

Further, Section 500.13 requires each covered entity to implement written policies and procedures designed to produce and maintain a "complete, accurate and documented asset inventory" of the covered entity's information systems. Those policies and procedures must include a method to track each asset's owner, location, classification or sensitivity, support expiration date, and recovery time objectives, along with establishing the frequency required for updating and validating the asset inventory.

Lastly, Section 500.5 expands the Cybersecurity Regulation's requirements with respect to vulnerability management. Specifically, it requires covered entities to develop and implement written cybersecurity policies and procedures specifically for vulnerability management. The Second Amendment requires that those policies and procedures ensure that the covered entity (1) conduct annual penetration testing of information systems "from both inside and outside the systems' boundaries by a qualified internal or external party," and (2) conduct automated scans of information systems, and a manual review of other systems at a frequency determined by its risk assessment, as well as after any material system changes.

Access Controls for Privileged Accounts

Section 500.7 has new and expanded requirements regarding access controls. The Second Amendment requires covered entities to limit the number of privileged accounts, and limit access functions and use of privileged accounts to only those persons for which access is necessary, periodically review access privileges (at least annually) to remove unnecessary access credentials or accounts, disable or securely configure protocols that permit remote control of devices, and promptly terminate access following departures.

Multi-factor Authentication ("MFA")

Section 500.12 has been amended to require a covered entity to use MFA for any individual accessing a covered entity's information systems. A covered entity's CISO may, however, approve in writing the use of reasonably equivalent or more secure compensating controls for purposes of accessing the covered entity's internal network from an external network. In such instances, the CISO must review the alternative controls at least annually.

Compliance Certification

Covered entities continue to be subject to a requirement that they certify their compliance with the Cybersecurity Regulation annually to NYDFS. That certification must (1) certify "material compliance" based upon data and documentation to demonstrate that material compliance, and (2) be signed by both the CISO and the highest ranking executive of the covered entity.

In a new requirement under the Second Amendment, in the event a covered entity cannot make the required certification, the entity must submit a written acknowledgment of noncompliance describing the provisions with which it is not in compliance and providing a timeline for coming into compliance.

Enforcement

The Second Amendment clarifies that the commission of a single act prohibited by the Cybersecurity Regulation or any failure to act to satisfy obligations imposed by the Cybersecurity Regulation constitutes a violation subject to agency enforcement. Such acts or failures include any failure to secure or prevent authorized access to nonpublic information due to noncompliance with the Cybersecurity Regulation or any failure to comply with the Cybersecurity Regulation for any 24-hour period with any provision thereunder. In assessing penalties, the superintendent may consider a variety of factors, such as:

1. The extent to which the covered entity has cooperated with the superintendent in the investigation of such acts;
2. The good faith of the entity;
3. Whether the violations resulted from conduct that was unintentional or inadvertent, reckless or intentional and deliberate;
4. Whether the violation was a result of failure to remedy previous examination matters requiring attention, or failing to adhere to any disciplinary letter, letter of instructions or similar;
5. Any history of prior violations;
6. Whether the violation involved an isolated incident, repeat violations, systemic violations or a pattern of violations;
7. Whether the covered entity provided false or misleading information;

8. The extent of harm to consumers;
9. Whether required, accurate and timely disclosures were made to affected consumers;
10. The gravity of the violations;
11. The number of violations and the length of time over which they occurred;
12. The extent, if any, to which the senior governing body participated therein;
13. Any penalty or sanction imposed by any other regulatory agency;
14. The financial resources, net worth and annual business volume of the covered entity and its affiliates;
15. The extent to which the relevant policies and procedures of the company are consistent with nationally recognized cybersecurity frameworks, such as NIST; and
16. Such other matters as justice and the public interest require.

II. Key Compliance Dates

The Second Amendment's compliance requirements will take effect in phases. Unless otherwise specified, covered entities have 180 days from date of adoption to come into compliance, or until April 29, 2024. Changes to reporting requirements take effect one month after publication of the Second Amendment on December 1, 2023. For certain other requirements, the Cybersecurity Regulation provides for a period of up to one year, 18 months, or two years to come into compliance.

The hyperlinks below link to outlines of the requirements and key compliances dates for each of the categories of businesses impacted by the Second Amendment:

- Implementation Timeline for Small Businesses
- Implementation Timeline for Class A Businesses
- Implementation Timeline for Covered Entities

III. Conclusion

Covered entities should assess the impact of the Second Amendment and evaluate what measures must be implemented to ensure compliance with the new and updated requirements.

This advisory is a general overview of the Second Amendment and is not intended as legal advice. The Second Amendment is very detailed and should be reviewed in its totality. If you have any questions about the Second Amendment, please feel free to contact Joseph D. Simon at (516) 357-3710 or via email at **jsimon@cullenllp.com**, Kevin Patterson at (516) 296-9196 or via email at **kpatterson@cullenllp.com**, Elizabeth A. Murphy at (516) 296-9154, or via email at **emurphy@cullenllp.com**, or Gabriela Morales at (516) 357-3850 or via email at **gmorales@cullenllp.com**.

Footnotes

[1] 23 NYCRR Part 500

[2] Covered entity means any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the

Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies. 23 NYCRR 500.1(e).

Practices

- Banking and Financial Services

Attorneys

- Joseph D. Simon
- Kevin Patterson
- Elizabeth A. Murphy
- Gabriela Morales