CARTER LEDYARD

our resources

New York DFS Finalizes Amendment to its Cybersecurity Regulations

December 20, 2023

On November 1, 2023, the New York State Department of Financial Services (the "DFS") finalized and adopted its long-awaited Second Amendment (the "Amendment")[1] to its Cybersecurity Regulations, 23 NYCRR Part 500. As summarized in our advisories dated September 22, 2022, and November 29, 2022, the Amendment first announced on July 29, 2022, and subsequently revised, includes additional audit and reporting requirements, enhanced technology requirements, and specific oversight and management obligations for Chief Information Security Officers ("CISOs"), senior management, and governing bodies.

The following are a few of the key changes in the Amendment:

Senior Governing Body

- The Amendment introduces a new term, "Senior Governing Body." [2] The Senior Governing Body is responsible for the Covered Entity's[3] cybersecurity program. This governing body may be an entity's board of directors or equivalent governing body, or, if neither of those exist, the senior officers of a Covered Entity. The Senior Governing Body's responsibilities include understanding cybersecurity matters, overseeing the development and maintenance of the entity's cybersecurity program by executive management or its designees, reviewing management reports, approving cybersecurity policies annually, and ensuring adequate resources are allocated for cybersecurity, considering the entity's risks.

Class A Companies

- It introduces a new category of "Class A" company that is subject to more stringent compliance requirements. A Class A company is a Covered Entity that meets the following criteria:
    - Has at least $20 million in gross annual revenue in each of the last two fiscal years from all of its business operations and that either (a) has employed over 2,000 employees averaged over the last two fiscal years or (b) has over $1 billion in gross annual revenue in each of the last two fiscal years from all of its business operations.[4]
- A Class A company must comply with the following additional requirements:
    - Design and conduct independent audits of its cybersecurity program based on its risk assessment;[5]
    - Monitor privileged access activity by implementing certain access controls, such as a privileged access management solution and imposing password complexity requirements;[6] and
    - Implement an endpoint detection and response solution to monitor anomalous activity and use a centralized solution for system logging and security event alerts.[7]

Additional Reporting Requirements

- CISOs must timely report to the Senior Governing Body or senior officer(s) on material cybersecurity issues, such as significant cybersecurity events and significant changes to the Covered Entity's cybersecurity program.[8]

- The CISO, together with the top executive of the Covered Entity, must annually certify that the entity has substantially adhered to the Cybersecurity Requirements over the past year. If not, they must acknowledge in writing that the entity did not substantially comply and provide an explanation of the non-compliance.[9]

- In connection with covered entities reporting cybersecurity events, they must now report whether ransomware was used and whether an extortion payment was made, as well as additional information.

Takeaways

The Amendment became effective on November 1, 2023, and covered entities have varying timeframes to come into compliance with the new requirements. Covered Entities should understand all aspects of the Amendment, assess their level of compliance, and implement administrative, physical, and technical safeguards to ensure compliance. Covered Entities are encouraged to consult legal counsel to assist in interpreting the DFS Cybersecurity Regulations and the Amendment, evaluating compliance obligations, and instituting measures to ensure compliance.

---

[1] *See* DFS, Second Amendment to 23 NYCRR 500, available at https://dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf.

[2] *Id.* § 500.1(q).

[3] A "Covered Entity" is defined under Section 500.1(e) of the Amended Cybersecurity Requirements as "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."

[4] *See* 23 NYCRR § 500.1(d).

[5] *Id.* § 500.2(c).

[6] *Id.* § 500.7(c).

[7] *Id.* § 500.14(b)

[8] *Id.* § 500.4(c).

[9] *Id.* § 500.17(b)(2).

related professionals

Matthew D. Dunn / Partner
D 212-238-8706
mdunn@clm.com

Jodutt Marwan Basrawi / Associate
D (212) 238-8767
basrawi@clm.com

Claudia Carbone / Associate
D 212.238.8688
carbone@clm.com