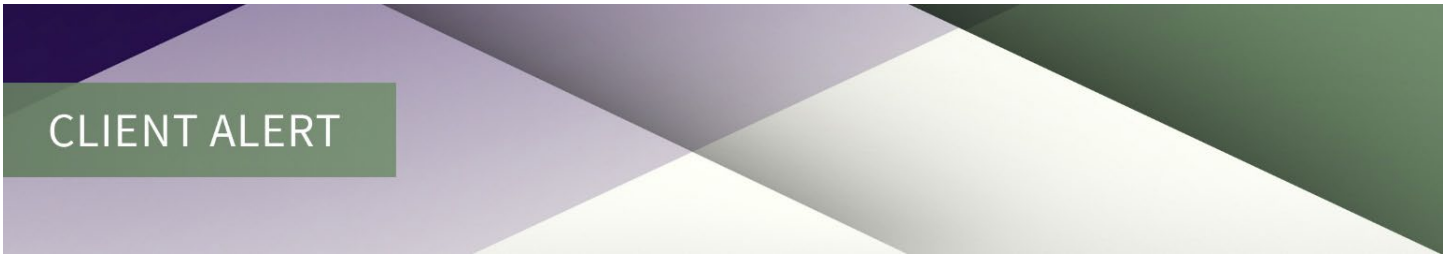
WILLKIE FARR & GALLAGHER LLP



NYDFS Finalizes Amendments to the Cybersecurity Regulation

November 7, 2023

AUTHORS

Daniel K. Alvarez | Kara Baysinger | Leah Campbell | Stephanie Duchene
Matthew J. Gaul | Laura E. Jehl | Allison J. Tam | Eun Jung Bae (Michelle)
Kari Prochaska

On November 1, 2023, the New York Department of Financial Services ("NYDFS") announced the adoption of amendments to its Cybersecurity Regulation 23 NYCRR Part 500 (the "Amended Cybersecurity Regulation").[1] Prior to the final adoption of the Amended Cybersecurity Regulation, NYDFS had released a series of proposed amendments from July 29, 2022 to June 28, 2023, which are summarized and analyzed in previous client alerts located here, here, and here.

Summary of Key Changes for Covered Entities

The Amended Cybersecurity Regulation includes several significant changes, including an explicit mandate that covered entities' boards of directors and/or senior officers have "sufficient understanding of cybersecurity-related matters" to exercise appropriate oversight, and new options related to annual certification, including an "acknowledgement" of non-compliance when a company cannot certify material compliance for the previous year.

The Amended Cybersecurity Regulation also creates a new type of a covered entity, a "Class A company," which is subject to heightened requirements. With respect to a "cybersecurity incident" that is notifiable to NYDFS within 72 hours after determining that such an incident has occurred, the Amended Cybersecurity Regulation creates a new notification

[1] New York State Department of Financial Services Final Adoption of the Second Amendment to 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies, located here: https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf ("Amended Cybersecurity Regulation").

requirement involving an incident that "results in the deployment of ransomware within a material part of the covered entity's information systems." The Amended Cybersecurity Regulation's new requirements have different transitional periods, as detailed below.

Requirement	Description of Requirements and Compliance Deadline
Senior Governing Body Oversight Sections 500.3 and 500.4(d)	• "Senior governing body," which means the board of directors (or an appropriate committee thereof) or the board-equivalent governing body (if neither of those exist, the senior officer responsible for the cybersecurity program) must exercise oversight of the covered entity's cybersecurity risk assessment. Although a newly defined term, the concept of the senior governing body already existed in the Cybersecurity Regulation. However, the Amended Cybersecurity Regulation specifies the senior governing body's oversight duties, which include: (i) having sufficient understanding of cybersecurity-related matters (which may include the use of advisors), (ii) regularly receiving and reviewing management reports about cybersecurity matters, (iii) requiring the executive management or its designees to develop, implement, and maintain the covered entity's cybersecurity program, and (iv) confirming that the covered entity's management has allocated sufficient resources to implement and maintain an effective cybersecurity program. Compliance deadline: 1 year from November 1, 2023 • Additionally, the Amended Cybersecurity Regulation requires that a covered entity's written policies must be approved at least annually by a senior officer or the covered entity's senior governing body for the protection of its information systems and nonpublic information. Compliance deadline: 180 days from November 1, 2023
CISO Reporting Section 500.4(c)	• The Chief Information Security Officer ("CISO") must timely report to the senior governing body or senior officer(s) regarding material security issues (e.g., significant cybersecurity events or significant changes to the covered entity's cybersecurity program). Compliance deadline: 1 year from November 1, 2023
"Class A Company"	• The Amended Cybersecurity Regulation creates a new category of covered entity, a "Class A company," which is an entity with at least $20 million in gross annual

Requirement	Description of Requirements and Compliance Deadline
Sections 500.2(c), 500.7(c), and 500.14(b)	revenue from all business operations of the covered entity and the New York business operations of its affiliates, and has either (a) over 2,000 employees; or (b) more than $1 billion in gross annual revenue in each of the last two fiscal years. • A Class A company will be subject to additional requirements, including conducting an independent audit of its cybersecurity program based on its risk assessment and implementing additional security controls, such as heightened access privileges, and an endpoint detection and response solution. Compliance deadline: 180 days from November 1, 2023, with an exception for the requirement regarding privileged access controls in Section 500.7(c) which becomes mandatory 18 months from November 1, 2023
Annual Certification to NYDFS Section 500.17(b)	• Covered entities have two options for certifying their annual compliance to NYDFS: (a) a written certification that certifies that the covered entity materially complied with the requirements during the prior calendar year; or (b) a written acknowledgement that the covered entity did not materially comply with all the requirements of the Cybersecurity Regulation, including a description of the nature of any such noncompliance. • The annual certification must be signed by the covered entity's highest-ranking executive and the CISO.[2] Compliance deadline: 30 days from November 1, 2023
Notice of a Cybersecurity Incident Section 500.17(a)	• The Amended Cybersecurity Regulation expands the types of cybersecurity events that require notification to NYDFS within 72 hours after determining that such an event has occurred. In addition to the existing requirements, covered entities must now report a cybersecurity event that results in the deployment of ransomware within a material part of the covered entity's information systems.

[2] NYDFS explained in its assessment of public comments that "both the CISO, who is the person in charge of overseeing the cybersecurity program at the covered entity, and the CEO or other highest-ranking executive, who is the person in charge of the business, have active involvement with cybersecurity compliance and sign off on the certifications and acknowledgements."

Requirement	Description of Requirements and Compliance Deadline
	• The Amended Cybersecurity Regulation also clarifies that covered entities must provide an update notice to NYDFS regarding a cybersecurity incident if there are material changes or new information that was previously unavailable. Compliance deadline: 30 days from November 1, 2023
Notice of an Extortion Payment Section 500.17(c)	• If a covered entity makes an extortion payment in connection with a cybersecurity event involving a covered entity, the covered entity must notify NYDFS of the payment within 24 hours. Within 30 days of the payment, covered entities must provide a written description of the extortion payment, including the reasons for payment. Compliance deadline: 30 days from November 1, 2023
Vulnerability and Risk Assessments Sections 500.5(a)(1), 500.5(a)(2), and 500.9(a)	• At least annually, penetration testing of information systems from both inside and outside the information systems' boundaries must be conducted by a qualified internal or external party. Compliance deadline: 180 days from November 1, 2023 • Automated scans of information systems (and a manual review of systems not covered by automated scans) must be conducted at a frequency determined by the risk assessment. Compliance deadline: 18 months from November 1, 2023 • A risk assessment must be periodically conducted over the covered entity's information systems, and reviewed and updated, at a minimum annually, and whenever a change in business or technology causes a material change to the covered entity's cyber risk. Compliance deadline: 180 days from November 1, 2023
Policies, Procedures, and Plans Sections 500.3 and 500.16	• The Amended Cybersecurity Regulation adds a number of new requirements regarding a covered entity's written policies and procedures, such as those related

Requirement	Description of Requirements and Compliance Deadline
	to remote access, vulnerability management, end-of-life management, data retention, and access privileges. Compliance deadline: 180 days from November 1, 2023 • It also adds prescriptive requirements regarding Business Continuity and Disaster Recovery ("BCDR") plans. A covered entity must test their BCDR plan at least annually including all staff and management critical to the response, and must provide relevant training to all employees responsible for implementing the BCDR plans. Compliance deadline: 1 year from November 1, 2023

Explanation of Changes from the June 28, 2023 Draft of the Revised Second Amendment

For covered entities that have been actively tracking the first and second draft amendments proposed by NYDFS, certain sections were revised from the June 28, 2023 draft of the proposed amendments,[3] including a summary of NYDFS' responses to public comments:[4]

- The defined term "Chief Information Security Officer" was revised to delete language referring to the CISO's "adequate authority to ensure cybersecurity risks are appropriately managed including the ability to direct sufficient resources to implement and maintain an effective cybersecurity program."[5] NYDFS stated that it had deleted this language in response to comments that CISOs do not typically make enterprise-wide resource allocation decisions, which are typically the responsibility of CEOs or other senior management.[6]

- The new defined term "cybersecurity incident" was added to clarify the "cybersecurity events" that require notification to NYDFS (although "cybersecurity event" still remains as a defined term).[7] NYDFS explained that

[3] New York State Department of Financial Services Revised Proposed Second Amendment to 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies, located here: https://www.dfs.ny.gov/system/files/documents/2023/06/rev_rp_23a2_text_20230628.pdf ("Revised Second Amendment").

[4] Assessment of Public Comments on the Revised Proposed Second Amendment to 23 NYCRR Part 500, located here: https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_apc_20231101.pdf ("Assessment of Public Comments").

[5] Revised Second Amendment, Section 500.1(c).

[6] Assessment of Public Comments, at 3.

[7] Revised Second Amendment, Section 500.1(c).

"cybersecurity incident" was added in response to comments and to conform with other regulations and industry usage.[8]

- The blanket requirement that Class A companies conduct an annual audit was removed, and instead was revised to note that an independent audit of an entity's cybersecurity program should be conducted based on the entity's risk assessment.[9] In response to comments, NYDFS explained that the updated language was based on requests from commenters that the annual requirement is burdensome, time-consuming, and unrealistic given the complexities in various companies' cybersecurity programs.[10]

- In assessing the limited exemption for compliance with the Cybersecurity Regulation, NYDFS increased the threshold for the gross annual revenue for covered entities from $5,000,000 up to $7,500,000 for the last three fiscal years for all business operations for the covered entity and its affiliates.[11] NYDFS indicated that it took comments into consideration regarding inflationary and cost pressures when raising the limited exemption threshold.[12]

Next Steps and Considerations for Covered Entities

Covered entities should assess the impact of the Amended Cybersecurity Regulation and evaluate if any measures must be implemented to ensure compliance with the new and updated requirements with respect to the covered entity's cybersecurity program and the relevant policies and procedures. The Amended Cybersecurity Regulation demonstrates that regulatory focus on cybersecurity continues, in particular with regard to timely reporting cybersecurity incidents and engaging the board of directors and/or senior management regarding appropriate oversight. For example, a covered entity that is an SEC registrant should take into consideration the requirements of the SEC's new cybersecurity rules for public companies (see our previous client alert here) in assessing its cybersecurity program and compliance posture.

8 Assessment of Public Comments, at 6.
9 Revised Second Amendment, Section 500.2(c).
10 Assessment of Public Comments, at 10.
11 Revised Second Amendment, Section 500.19(b).
12 Assessment of Public Comments, at 35.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Kara Baysinger
415 858 7425
kbaysinger@willkie.com

Leah Campbell
212 728 8217
lcampbell@willkie.com

Stephanie Duchene
310 855 3066
sduchene@willkie.com

Matthew J. Gaul
212 728 8261
mgaul@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Allison J. Tam
212 728 8282
atam@willkie.com

Eun Jung Bae (Michelle)
202 303 1166
ebae@willkie.com

Kari Prochaska
312 728 9080
kprochaska@willkie.com

Copyright © 2023 Willkie Farr & Gallagher LLP.

This alert is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This alert may be considered advertising under applicable state laws.

Willkie Farr & Gallagher LLP is an international law firm with offices in Brussels, Chicago, Frankfurt, Houston, London, Los Angeles, Milan, New York, Palo Alto, Paris, Rome, San Francisco and Washington. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.