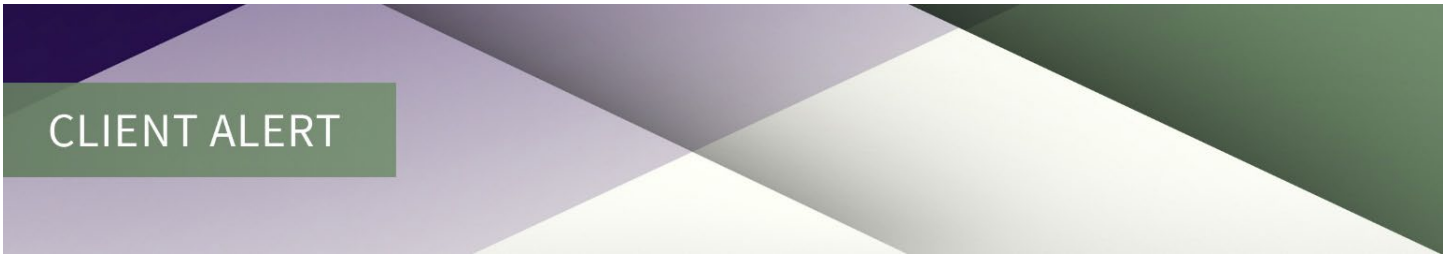
WILLKIE FARR & GALLAGHER LLP



NYDFS Publishes Second Round of Proposed Amendments to the Cybersecurity Regulation

November 15, 2022

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Kara Baysinger | Matt J. Gaul
Allison J. Tam | Kari Prochaska

On November 9, 2022, the New York Department of Financial Services ("NYDFS") released a second round of amendments to 23 NYCRR Part 500 (the "Cybersecurity Regulation"), which supplement the first round of proposed amendments (the "Proposed Amendments").[1] The public comment period for these Revised Proposed Amendments expires on January 9, 2023.[2] According to its press release accompanying the Proposed Amendments, NYDFS will review all received comments and either propose additional revisions or adopt the final regulation.[3]

As summarized and analyzed in our earlier alert, the original set of Proposed Amendments would add additional and significant compliance requirements for covered entities. The Revised Proposed Amendments further refines certain amended language proposed in July and would create even more new requirements for covered entities. Specifically:

1 New York State Department of Financial Services Proposed Second Amendment to 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies, located here: https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_text_20221109_0.pdf ("Revised Proposed Amendments").

2 New York Department of Financial Services, https://www.dfs.ny.gov/industry_guidance/regulations/proposed_fsl

3 Press Release, "DFS Superintendent Adrienne A. Harris Announces Updated Cybersecurity Regulation" November 9, 2022, located at https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20221109221

- Notification of Cybersecurity Events Affecting Third Party Service Providers. The Revised Proposed Amendments would expressly provide that where a covered entity is affected by and aware of a cybersecurity event on the systems of a third party service provider, notification to NYDFS will be required within 72 hours.[4]

- Notification of Investigations Regarding Cybersecurity Events. The revisions to the Proposed Amendments require covered entities to provide requested information regarding the status of their investigations into any cybersecurity event within 90 days of the notification of the cybersecurity event. While the proposed language now includes a specific time period by which covered entities affected by a cybersecurity event must provide an update, the Revised Proposed Amendments affirm that covered entities "have a continuing obligation to update and supplement the information provided."[5]

- Board Oversight. As proposed in the latest set of revisions, board responsibilities would be increased to include duties of oversight and direction to management regarding the covered entity's cybersecurity risk management program, and would require the board of directors to have sufficient expertise or knowledge – or to be advised by those with sufficient expertise and knowledge – regarding cybersecurity risk management.[6]

- Remediation Plans. Under the Revised Proposed Amendments, covered entities would be required to provide remediation plans and a timeline for implementation of those plans as part of their acknowledgement of any areas of non-compliance with the Cybersecurity Regulation, together with their annual certification of compliance.[7] Similarly, the CISO of each covered entity would be required to include remediation plans for material inadequacies in their reporting to the covered entity's "senior governing body."[8] Finally, under the Revised Proposed Amendments, certifications of compliance would require the signature of the covered entity's highest-ranking executive, rather than the signature of the covered entity's CEO, as was proposed under the initial Proposed Amendments.[9]

- Multi-Factor Authentication Requirements. The Revised Proposed Amendments would expand requirements to deploy Multi-Factor Authentication ("MFA") to remote access to a covered entity's systems, to remote access to third-party applications, and to all privileged accounts (including service accounts). The Revised Proposed

4 Section 500.17(a)(3).
5 Section 500.17(a)(2).
6 Section 500.4(d).
7 Section 500.17(b)(ii)(d).
8 Section 500.4(b)(6).
9 Section 500.17(b)(2).

Amendments would also require the CISO to periodically - at least annually, and more frequently as determined by the risk assessment - review any approvals for compensating controls for MFA.[10]

- Vulnerability Management. Covered entities would be required to implement policies and procedures related to vulnerability management that cover (i) penetration testing from both inside and outside a covered entity's information systems' boundaries by a qualified independent party; and (ii) automated scans of information systems, and a manual review of systems not covered by such scans, for the purpose of discovering, analyzing, and reporting vulnerabilities determined by (a) the risk assessment and (b) major system changes. [11]

- Written Password Policy. Under the Revised Proposed Amendments, covered entities would be required to implement a written password policy that meets industry standards. In addition, Class A companies (see revised definition below) would be required to implement a privileged access management solution and an automated method of blocking commonly used passwords for all accounts. However, if it is determined by the covered entity that blocking commonly used passwords is infeasible, the CISO may instead utilize reasonably equivalent or more secure compensating controls.[12]

- Monitoring and Training. The Revised Proposed Amendments also added monitoring requirements related to controls that protect against malicious code, including those that monitor web traffic and email to block malicious content. The revised training requirement would mandate that covered entities provide annual cybersecurity awareness training that includes social engineering exercises.[13]

- Annual Testing. Under the Revised Proposed Amendments, the incident response plan and business continuity and disaster recovery plans would be required to be tested at least annually; the testing would be required to include the covered entity's highest-ranking executive.[14]

- Additional CISO Resources. In the revised language, the CISO's governance duties would be supplemented to include the ability of the CISO to direct sufficient resources to implement and maintain a cybersecurity program.[15]

- Class A Company Threshold. The revisions to the Proposed Amendments refine thresholds for the definition of a Class A company and look back over the last two fiscal years. The amended language would now require a covered entity and its affiliates to have at least $20M in gross annual revenue over the last two fiscal years in New

[10] Section 500.12(b)(c).
[11] Section 500.5(a)(1)(2).
[12] Section 500.7(b).
[13] Section 500.14(a).
[14] Section 500.16(d).
[15] Section 500.4(a). This was likely added due to concerns from CISOs that compliance obligations may not be supported with adequate budgetary authority and the revised language likely makes it difficult for the board to reduce requests from the CISO related to budget.

> York, and either (as addressed in the first set of Proposed Amendments): (i) over $1B in gross annual revenue from all business operations *over the last two fiscal years*; or (ii) over 2,000 employees, averaged *over the last two fiscal years*, and regardless of the location of those employees.[16]

The Revised Proposed Amendments include updated compliance deadlines that provide a brief window for certain covered entities to prioritize necessary improvements and come into compliance with the requirements. These include updated compliance deadlines for requirements regarding: (i) backups that are adequately protected from unauthorized alteration (one year from the effective date of the Proposed Amendments); (ii) automated scanning, written password policies, endpoint detection solutions and security event logging, and implementation of controls that block malicious content (18 months from the effective date of the Proposed Amendments); and (iii) asset management and data retention (two years from the effective date of the Proposed Amendments). Given the potentially significant lift that some of these changes will require, meeting these deadlines will likely be a challenge for many. Covered entities subject to the Cybersecurity Regulation and their CISOs may want to consider taking initial efforts now to understand how their current practices, contracts, and other activities map to the Revised Proposed Amendments.

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

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

Kara Baysinger
415 858 7425
kbaysinger@willkie.com

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

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

Kari Prochaska
312 728 9080
kprochaska@willkie.com

[16] Section 500.1(c)(1)(2).