November 14, 2022

New York State Department of Financial Services Proposes Significant Amendments to Cybersecurity Regulations

Agency Proposes Comprehensive Updates to Cybersecurity Protections Covered Entities Are Required to Implement

SUMMARY

On November 9, 2022, the New York State Department of Financial Services ("DFS") announced proposed amendments ("Amendments") to DFS's Cybersecurity Requirements for Financial Services Companies ("Cybersecurity Regulation"),[1] representing a comprehensive update of the existing cybersecurity requirements to which Covered Entities are subject.[2] The Amendments are similar to the pre-proposed amendments DFS issued on July 29, 2022 ("Pre-Proposed Amendments"), but include several significant changes and additional proposed requirements that are highlighted in this memorandum.

The 60-day notice-and-comment period for the Amendments began on November 9, 2022 and runs until 5:00 P.M. E.S.T. on Monday, January 9, 2023.[3] If the Amendments are promulgated, Covered Entities will have 180 days from the publication of the Notice of Adoption in the State Register to bring their cybersecurity programs into compliance with the amended Cybersecurity Regulation, subject to certain exceptions.

BACKGROUND

The cybersecurity regulatory landscape has grown significantly more complex since the initial 2017 iteration of the Cybersecurity Regulation. Financial institutions now face a complex system of overlapping cybersecurity requirements from different government bodies, many of which were issued within the last year alone. In the wake of these developments, on July 29, 2022, DFS published the Pre-Proposed Amendments, accepting initial "outreach" comments to those Pre-Proposed Amendments for approximately

three weeks thereafter. DFS has now issued the official, proposed Amendments and published them in the State Register for formal notice-and-comment. If adopted, the Amendments will represent the most significant revisions to the Cybersecurity Regulation since it became effective on March 1, 2017.[4]

Among other things, the Amendments would (i) require Covered Entities to notify the DFS Superintendent within 24 hours of making an "extortion payment" as a result of a cybersecurity event, and within 30 days provide the Superintendent with written information concerning the decision to make such payment, (ii) require Covered Entities to implement a business continuity and data recovery plan in addition to incident response plans, and (iii) establish additional auditing, reviewing, and monitoring requirements for a new classification of "Class A" companies based on the number of employees and revenue—Covered Entities that, together with their affiliates, have both: (i) $20 million in gross annual revenue from business operations in New York in each of the preceding two fiscal years, and (ii) over 2,000 employees averaged over the preceding two fiscal years or over $1 billion in gross annual revenue in each of the preceding two fiscal years.

OVERVIEW OF THE CHANGES TO THE PROPOSED AMENDMENTS

The Amendments retain many of the updates from the Pre-Proposed Amendments, with certain material differences, described below.

A. PROPOSED REQUIREMENTS FOR CYBERSECURITY GOVERNANCE

Boards of Directors. The new Amendments clarify that a Covered Entity's "board of directors or equivalent" or an "appropriate committee thereof" not only must exercise oversight of cybersecurity risk management, but shall "provide direction to management on . . . cybersecurity risk management,"[5] adding an explicit new responsibility for a Covered Entity's directors.

Chief Information Security Officers ("CISO"). While the Pre-Proposed Amendments stated that a Covered Entity's CISO must have "adequate independence and authority" to ensure appropriate management of cybersecurity risks, the Amendments remove the reference to a CISO's "independence" and add that a CISO must have the "ability to direct sufficient resources to implement and maintain a cybersecurity program."[6] The Amendments also add a proposed requirement that the annual written report provided by the CISO to the Covered Entity's senior governing body include "plans for remediating material inadequacies."[7]

B. CLASS A COMPANIES

The Amendments revise the proposed criteria for a Covered Entity to be treated as a "Class A" company subject to enhanced cybersecurity requirements, adding a requirement that a Class A Covered Entity must have "at least $20,000,000 in gross annual revenue in each of the last two fiscal years from business operations of the [C]overed [E]ntity and its affiliates" in New York.[8] The Amendments also adjust the

remaining proposed Class A criteria, such that a Class A company must have: (i) "over 2,000 employees averaged over the last two fiscal years"; or (ii) "over $1,000,000,000 in gross annual revenue in each of the last two fiscal years"—as opposed to in each of the last three—"from all business operations of the Covered Entity and all of its affiliates."[9]

C. PROPOSED REQUIREMENTS FOR WRITTEN POLICIES AND PROCEDURES

Specific Required Provisions. DFS proposes new minimum requirements for the written cybersecurity policies that must be approved by a Covered Entity's senior governing body, including that such policies address "security awareness and training," data retention, and incident notification,[10] that they provide for scanning of information systems to identify vulnerabilities,[11] and that they cover password use to the extent a Covered Entity uses passwords for authentication.[12]

Specific Required Training. Covered Entities are already required to provide personnel with regular cybersecurity training, but the amended Cybersecurity Regulation would require that all personnel receive training annually, including through "social engineering exercises."[13]

Incident Response Plan and Business Continuity Disaster Recovery ("BCDR") Plan. A Covered Entity would be required to provide relevant training on its incident response plan and BCDR plan to all employees necessary to implement such plans, and test both plans at least annually.[14] DFS also removed the proposed requirement that copies of the incident response and BCDR plans be maintained at one or more accessible offsite locations, and clarified that its incident response plan and BCDR plan must be both distributed to and accessible by all employees necessary to implement them.[15] The amended Section 500.16 would also require Covered Entities to maintain backups adequately protected from unauthorized alterations or destruction (instead of "isolated from network connections," as the Pre-Proposed Amendments had provided).[16]

D. ENHANCED CYBERSECURITY TESTING REQUIREMENTS

Under the current Cybersecurity Regulation, a Covered Entity that does not continuously monitor vulnerabilities in its information systems must conduct annual penetration testing by attempting to penetrate the Covered Entity's databases or controls from outside or inside its information systems.[17] The Pre-Proposed Amendments added a requirement that penetration testing be conducted by a qualified independent party, and the proposed Amendments that were just published clarify that a qualified independent party may be either internal or external to the Covered Entity.[18] The Amendments also supplement vulnerability management requirements such that a Covered Entity would need to conduct automated scans of information systems and manually review systems not covered by the scans, put in place monitoring systems to promptly flag new security vulnerabilities, timely remediate vulnerabilities, and document material issues during testing.[19] Covered Entities would be required to block malicious content

by implementing controls that would protect against malicious code, including controls that "monitor and filter web traffic and electronic mail."[20]

The Amendments require existing risk assessments to be "reviewed and updated" whenever changes to a Covered Entity's business or technology materially change its cybersecurity risk, instead of requiring an "impact assessment" each time that occurs.[21]

Additionally, the proposed amended definition of an "independent audit" would require that an audit be conducted by an external auditor to be considered independent.[22] The Pre-Proposed Amendments would have permitted an independent audit to be conducted by an internal auditor so long as the auditor was sufficiently independent.

E. PRIVILEGED ACCOUNT AND PASSWORD MANAGEMENT REQUIREMENTS

The Amendments include a number of new prescriptive enhancements of existing required cybersecurity controls concerning the use of privileged accounts and password security.

Privileged Account Limitations. The Amendments propose new requirements related to the management of privileged accounts and passwords. Covered Entities would be required to review access privileges at least annually to remove or disable unnecessary access or accounts, and promptly terminate access following departures.[23] To the extent a Covered Entity uses passwords for authentication, the Covered Entity would be required to implement an industry-standard written password policy.[24]

The Amendments also include a new proposal that Class A companies be required to implement a "privileged access management solution" and an "automated method for blocking commonly used passwords for all accounts."[25] To the extent such blocking is infeasible, the CISO would need to annually approve in writing reasonably equivalent controls.[26] DFS removed the proposal that a Class A Covered Entity be required to implement a password vaulting solution for privileged accounts.

Multi-factor authentication ("MFA"). DFS's revised Amendments require MFA for all privileged accounts, eliminating certain exceptions that were permitted in the Pre-Proposed Amendments, and require the CISO to periodically review and to approve the use of any compensation controls in place of MFA.[27]

F. NOTIFICATION TO DFS OF A THIRD-PARTY CYBERSECURITY INCIDENT

The Amendments add a new scenario to the existing list of incidents about which a Covered Entity must notify DFS. Under the Amendments, a Covered Entity would need to notify the Superintendent within 72 hours of learning of a cybersecurity event at a third-party service provider affecting the Covered Entity.[28]

G. COMPLIANCE WITH AN AMENDED CYBERSECURITY REGULATION

The Amendments also set out new timelines for compliance with certain Amendments in the event they are implemented. For example, a Covered Entity would have one year to ensure maintenance of backups

adequately protected from unauthorized alterations or destruction,[29] and two years to implement written policies and procedures concerning its asset inventory.[30] Additionally, Class A companies would have 18 months to implement endpoint detection and response solutions for monitoring anomalous activity, controls protecting against malicious code, and a solution for centralizing logging and security event alerting.[31]

IMPLICATIONS

The additional proposed requirements in the Amendments add to a growing variety of cybersecurity obligations that financial institutions must meet, and come at a time of increased enforcement efforts in cybersecurity. The heightened enforcement risk in this area is reinforced by the new proposed provision in the Amendments pursuant to which even a single act prohibited by the amended Cybersecurity Regulation would constitute a violation.

DFS has noted that it remains open to feedback on the proposed Amendments, and its press release announcing the Amendments observed certain adjustments that were made "based on feedback from the industry and . . . the realities of operating a small business."[32]

* * *

ENDNOTES

1 23 NYCRR Pt. 500.

2 A "Covered Entity" means any individual or non-governmental entity "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." 23 NYCRR at §§ 500.1(c), (i).

3 Cybersecurity Resource Center: Proposed Second Amendment to 23 NYCRR Part 500, DFS, https://dfs.ny.gov/industry_guidance/cybersecurity.

4 Cybersecurity Regulation at § 500.0.

5 Amendments at § 500.4(d)(1).

6 *See id.* at §§ 500.4(a), (c).

7 *See id.* at § 500.4(b)(6).

8 *See id.* at § 500.1(c).

9 *See id.*

10 *See id.* at § 500.3.

11 *See id.* at § 500.5(a)(2).

12 *See id.* at § 500.7(b).

13 *See id.* at § 500.14(a)(3).

14 *See id.* at §§ 500.16(b)-(d).

15 *See id.* at § 500.16(b).

16 *See id.* at §§ 500.16(a)(1)(vii), (d)(3), (e).

17 Cybersecurity Regulation at §§ 500.1(h), 500.5(a).

18 Amendments at § 500.5(a)(1).

19 *See id.* at §§ 500.5(a)-(d).

20 *See id.* at § 500.14(a)(2).

21 *See id.* at § 500.9(c).

22 *See id.* at § 500.1(f).

23 *See id.* at §§ 500.7(a)(4), (6).

24 *See id.* at § 500.7(b).

25 *See id.* at § 500.7(b).

26 *See id.* at § 500.7(b)(2).

27 *See id.* at §§ 500.12(b)-(c).

28 *See id.* at § 500.17(a)(3).

29 *See id.* at §§ 500.22(d)(2), 500.16(e).

30 *See id.* at §§ 500.22(d)(4), 500.13(a).

31 *See id.* at §§ 500.22(d)(3), 500.14(a)(2), 500.14(b).

ENDNOTES (CONTINUED)

[32] Press Release, DFS Superintendent Adrienne A. Harris Announces Updated Cybersecurity Regulation (Nov. 9, 2022), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20221109221.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 900 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.