SULLIVAN & CROMWELL LLP

S&C memo

November 10, 2023

New York DFS Adopts Significant Amendment to Its Cybersecurity Regulation

Covered Entities Will Be Subject to Enhanced Requirements Concerning Cybersecurity Governance, Notifications, Controls, Policies and Other Matters

SUMMARY

On November 1, 2023, the New York State Department of Financial Services ("DFS") adopted the Second Amendment (the "Amendment") to its Cybersecurity Requirements for Financial Services Companies ("Cybersecurity Regulation"),[1] expanding a number of requirements imposed under its existing cybersecurity regime. The Amendment tracks the proposed amendments to the Cybersecurity Regulation DFS issued on November 9, 2022 (the "Proposed Amendments"),[2] with certain changes described in this Memorandum, and represents the most significant expansion of the Cybersecurity Regulation since the regulation became effective on March 1, 2017.

Covered Entities[3] subject to the Cybersecurity Regulation generally have 180 days from the date of adoption, *i.e.*, until April 29, 2024, to come into compliance with the Amendment, although the Amendment sets forth separate, generally longer time frames for compliance with certain provisions.[4]

Notably, however, the Amendment's enhanced requirements to report certain cybersecurity incidents to DFS will take effect on December 1, 2023.[5]

OVERVIEW OF THE AMENDMENT

A. REQUIRED NOTIFICATIONS TO DFS REGARDING CERTAIN CYBERSECURITY INCIDENTS

The Amendment expands and clarifies the scope of Section 500.17 of the Cybersecurity Regulation, which sets forth the requirement that Covered Entities notify DFS of certain cybersecurity incidents. These updated notification requirements go into effect on December 1, 2023.

Cybersecurity Incident. Under the existing Cybersecurity Regulation, Covered Entities have been required to notify DFS within 72 hours from a determination that a cybersecurity event has occurred that either (1) impacts the Covered Entity and gives rise to an obligation to notify any government body, self-regulatory agency or other supervisory body, or (2) has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity. The Amendment retains this requirement, renaming such notification events "Cybersecurity incidents," and expands upon it in three ways:

- Covered Entities will be required to report the deployment of ransomware within a material part of the Covered Entity's information systems.[6]
- Covered Entities will be required to notify DFS within 24 hours of making any "extortion payment" in connection with a cybersecurity event.[7] Within 30 days of making such an extortion payment, the Covered Entity must also provide DFS with 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."[8]
- Covered Entities will be required to "promptly provide" to DFS "any information requested regarding the incident" and will also be under a "continuing obligation to update [DFS] with material changes or new information previously unavailable."[9]

The Amendment also clarifies that otherwise reportable cybersecurity incidents include those that occur not only at the Covered Entity but also at "its affiliates[] or a third party service provider."[10] To address concerns raised in comments on the Proposed Amendments that Covered Entities may not learn of such incidents until after 72 hours has elapsed, DFS clarified in the adopting release and language of the Amendment that the 72-hour time frame for notification begins when the Covered Entity itself learns of the incident.

B. CYBERSECURITY GOVERNANCE REQUIREMENTS

Oversight by a "Senior Governing Body." The Amendment requires that a "senior governing body"—a new term in the Cybersecurity Regulation—oversee a Covered Entity's cybersecurity risk management.[11] A senior governing body is defined as a Covered Entity's board of directors, board committee or "equivalent governing body," or, if no such body exists, "the senior officer or officers of a [C]overed [E]ntity responsible for the [C]overed [E]ntity's cybersecurity program."[12]

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 [C]overed [E]ntity'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."[13]

Reporting to the senior governing body by the Chief Information Security Officer ("CISO"). 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 Amendment requires this annual report be provided to the senior governing body, and to include "plans for remediating material inadequacies" in the Covered Entity's

cybersecurity program.[14] Further, the Amendment requires that the CISO "timely report" to the senior governing body or senior officers on "material cybersecurity issues, such as significant cybersecurity events and significant changes to the [C]overed [E]ntity's cybersecurity program."[15] This language differs slightly from the Proposed Amendments, which would have required the CISO to timely report on updates to the [C]overed [E]ntity's risk assessment or major cybersecurity events.[16] Notably, in response to comments expressing concern that a company's overall resource allocation is not typically for the CISO to determine, DFS did not adopt a proposed requirement that the CISO be able to direct sufficient resources to implement and maintain a cybersecurity program,[17] replacing it with the requirement, noted above, that the senior governing body confirm that management has allocated sufficient resources to the cybersecurity program.[18]

C. CLASS A COMPANIES

The Amendment creates a new category of Covered Entities, designated as "Class A companies," subject to specific, enhanced requirements. A Covered Entity is considered Class A if it has "at least $20,000,000 in gross annual revenue in each of the last two fiscal years from all business operations of the [C]overed [E]ntity and the business operations in [New York] of the Covered Entity's affiliates," and either:

1. "over 2,000 employees averaged over the last two fiscal years";[19] or
2. "over $1,000,000,000 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."[20]

In addition to the requirements set forth in the Amendment applicable to all Covered Entities, the following enhanced requirements apply to Class A companies:

- Section 500.2(c) mandates that a Class A company "design and conduct independent audits of its cybersecurity program based on its risk assessment." The Amendment defines "independent audit" as "an audit conducted by internal or external auditors free to make decisions not influenced by the covered entity being audited or by its owners, managers, or employees." [21]
- Section 500.7(c) requires that a Class A company monitor privileged access by implementing both "a privileged action management solution" and "an automated method of blocking commonly used passwords" for "all accounts" on company systems and "all other accounts wherever feasible." To the extent blocking commonly used passwords is infeasible, the CISO must "approve in writing at least annually the infeasibility and the use of reasonably equivalent or more secure compensating controls."[22]
- Section 500.14(b) requires that a Class A company implement "an endpoint detection and response solution to monitor anomalous activity," including but not limited to lateral movement, as well as a "solution that centralizes logging and security event alerting." If a Class A company does not implement these controls, the CISO must "approve in writing the use of reasonably equivalent or more secure compensating controls."[23]

D. REQUIREMENTS FOR WRITTEN PLANS, POLICIES AND PROCEDURES

Incident Response Plan and Business Continuity and Disaster Recovery Plan. Section 500.16's existing requirement to establish a written incident response plan has been expanded in the Amendment, which requires the incident response plan both to provide for recovery from backups, and to require the

preparation of a "root cause analysis that describes how and why [an] event occurred, what business impact it had, and what will be done to prevent reoccurrence."[24]

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.[25] 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;
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 Covered Entity's operations and offsite information storage; and
6. Identify third parties necessary to the continued operations of the Covered Entity's information systems.[26]

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.[27] Under the Amendment, a Covered Entity must provide relevant training on both its incident response plan and BCDR plan to all employees 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."[28]

Written Policies and Procedures. Section 500.3 supplements the required contents of a Covered Entity's written cybersecurity policies, which now must be approved at least annually by the senior governing body or a senior officer, and requires Covered Entities to develop, document, and implement procedures in accordance with those policies. Specifically, with respect to content, a Covered Entity's policies must now address data retention, asset and device "end of life management,"[29] remote access controls, "security awareness and training," systems and application security, incident notification, and "vulnerability management."[30]

Vulnerability Management. Under the Amendment, Section 500.5 restyles and 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.[31] The 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 vulnerability

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.[32] Those policies and procedures must also be designed to ensure the Covered Entity is "promptly informed of new security vulnerabilities by having a monitoring process in place" and to "timely remediate vulnerabilities, giving priority to vulnerabilities based on the risk they pose to the" Covered Entity.[33] The Amendment did not adopt the requirement from the Proposed Amendments that a Covered Entity's policies and procedures document material issues found during testing and report them to its senior governing body and senior management.[34]

Written Password Policy. To the extent a Covered Entity uses passwords for authentication, Section 500.7(b) requires the Covered Entity to implement a written password policy that meets industry standards.

E. PERIODIC ASSESSMENTS, REVIEWS, AND TRAINING

The Amendment requires certain additional periodic assessments and reviews. Specifically, the Amendment requires that existing risk assessments be "reviewed and updated" at least annually and whenever changes to a Covered Entity's business or technology materially change its cybersecurity risk.[35] The Amendment also requires the CISO's review of the Covered Entity's application security procedures, guidelines, and standards at least annually.[36]

More generally, the Amendment requires that cybersecurity awareness training occur at minimum annually, and include "social engineering" exercises.[37]

F. OTHER ENHANCED REQUIREMENTS AND SECURITY MEASURES

Access Controls for Privileged Account. Section 500.7 imposes new, expanded requirements regarding access controls. The Amendment requires Covered Entities to limit the number of privileged accounts, and limit access functions and use of privileged accounts to only those that are necessary, periodically review access privileges (at least annually) to remove unnecessary access or accounts, disable or securely configure protocols that permit remote control of devices, and promptly terminate access following departures.[38]

Multi-factor Authentication ("MFA"). Section 500.12 affirmatively requires a Covered Entity to use MFA for any individual accessing a Covered Entity's information systems.[39] Even when a Covered Entity qualifies for a limited exemption under Section 500.19 due to its size or revenue, MFA will still be required for remote access to the Covered Entity's information systems, for access to third-party applications, and for all privileged accounts "other than service accounts that prohibit interactive login."[40] 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.[41] In such instances, the CISO must review the alternative controls at least annually.[42]

Asset Management and Data Retention. 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 the frequency required to update and validate the asset inventory.[43]

Monitoring. In addition to existing requirements to implement risk-based policies, procedures, and controls to monitor users, Section 500.14 now requires Covered Entities to implement "risk-based controls designed to protect against malicious code," including monitoring and filtering web traffic and electronic mail to block malicious content.

Encryption of Nonpublic Information. Section 500.15 continues to require Covered Entities to implement a written policy regarding encryption that meets industry standards as to information "held or transmitted by the covered entity both in transit over external networks and at rest." As amended, however, the CISO is no longer permitted to approve compensating controls instead of encryption to secure data *in transit* over external networks, but remains permitted to approve compensating controls as an alternative to encryption of data *at rest* when such encryption is not feasible, so long as the CISO reviews and approves them in writing at least annually.[44]

G. COMPLIANCE CERTIFICATION BY COVERED ENTITY'S MOST SENIOR EXECUTIVE

Covered Entities continue to be subject to a requirement that they certify their compliance with the Cybersecurity Regulation annually to DFS, though pursuant to the Amendment, that certification (1) must certify "material compliance" (as opposed to simply "compliance," which has been the standard under the Cybersecurity Regulation and could have been interpreted to mean full compliance), based upon data and documentation to demonstrate that material compliance, and (2) must be signed by both the CISO and the highest ranking executive of the Covered Entity.[45] In the event a Covered Entity cannot make that certification, it 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.[46]

H. ENFORCEMENT

The Amendment provides that violations of the Cybersecurity Regulation include (1) failure to secure, or prevent unauthorized access to a person's or entity's nonpublic information due to noncompliance with the Cybersecurity Regulation, or (2) material failure to comply with "any section" of the Cybersecurity Regulation for a 24-hour period.[47] The Amendment further sets forth a non-exhaustive list of sixteen factors that the superintendent of DFS shall take into account when assessing a penalty, including the Covered Entity's cooperation and good faith, whether the conduct was intentional, the Covered Entity's history of prior or repeated violations, the extent of harm, whether customers were timely and accurately notified, the gravity and number of violations, any participation by the senior governing body, penalties or sanctions imposed by other regulatory agencies, the financial resources of the Covered Entity, and the extent to which the Covered Entity's policies and procedures are consistent with nationally recognized cybersecurity frameworks (like NIST, the National Institute of Standards and Technology).[48]

IMPLICATIONS

The Cybersecurity Regulation was the country's first regulation to impose prescriptive, baseline cybersecurity standards in the financial services industry. It has proved a model for other regulators including, most recently, the FTC, which last month again expanded its Safeguards Rule in ways that emulate and harmonize with the Cybersecurity Regulation. In light of the Cybersecurity Regulation's widespread impact, the enhanced requirements of the Amendment are likely to influence the way in which other regulators evaluate and implement cybersecurity regulation, and private sector entities design and implement cybersecurity programs, over time.

The Amendment's requirement to report and justify, in writing, the need for any cyber extortion payment reflects a less sympathetic view expressed by regulators in recent years toward companies that are victimized in ransomware attacks. In 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control published an advisory stating that, in evaluating an enforcement response with respect to a company that inadvertently violates a sanctions regulation in making a cyber extortion payment, it will be a "significant mitigating factor" if the company had taken meaningful steps in advance to reduce the risk of cyber extortion.[49]

The Amendment underscores the importance of cybersecurity oversight by boards of directors of Covered Entities, and does so at a time when companies' cybersecurity practices are being more closely scrutinized by regulators and private litigants. The Amendment's requirement that a Covered Entity's "highest ranking executive" sign the company's annual certification of compliance is likewise a reflection of a view regulators have expressed increasingly in recent years that cybersecurity is a "whole of business" risk, and not merely an information technology risk. Given the Amendment's requirement that the Covered Entity's senior governing body have a "sufficient understanding of cybersecurity-related matters to exercise [cybersecurity] oversight, which may include the use of advisors," Covered Entities should consider whether their board of directors and/or appropriate board or management committees would benefit from additional and periodic training on topics related to cybersecurity risk.

The Amendment's focus on cybersecurity governance echoes that of the new cybersecurity disclosure rules adopted by the U.S. Securities and Exchange Commission ("SEC") on July 26, 2023. The SEC's new rules underscore the role of senior management and boards in cybersecurity oversight by requiring companies to disclose in their annual reports how senior management and the board oversee cybersecurity.

The Amendment was also released just days after the SEC charged SolarWinds and its CISO with securities fraud and failures under the internal accounting controls, reporting, and disclosure controls provisions of the Exchange Act stemming from various alleged cybersecurity failures. Like the SEC, DFS has made active use of its enforcement authority in cybersecurity-related matters in recent years, and can be expected to continue to do so based on the expanded requirements of the Amendment.

* * *

[1] 23 NYCRR Pt. 500.

[2] Sullivan & Cromwell LLP, *New York State Department of Financial Services Proposes Significant Amendments to Cybersecurity Regulations* (Nov. 14, 2022), *available at* https://www.sullcrom.com/SullivanCromwell/_Assets/PDFs/Memos/sc-publication-new-york-department-financial-services-amendments-cybersecurity-regulations.pdf.

[3] A "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." *See* Cybersecurity Regulation at § 500.1(e).

[4] *See* DFS, *Cybersecurity Resource Center: Amended Cybersecurity Regulation; Key Compliance Dates* https://dfs.ny.gov/industry_guidance/cybersecurity.

[5] *See id.*

[6] *See* Cybersecurity Regulation at § 500.1(g)(3).

[7] *See id.* at § 500.17(c)(1).

[8] *See id.* at § 500.17(c)(2).

[9] *See id.* at § 500.17(a)(2).

[10] *See id.* at § 500.17(a).

[11] *See id.* at § 500.4(d).

[12] *See id.* at § 500.1(q).

[13] *See id.* at §§ 500.4(d)(1)-(4).

[14] *See id.* at § 500.4(b).

[15] *See id.* at § 500.4(c).

[16] *See* Proposed Amendments at § 500.4(c).

[17] *See id.* at § 500.4(a).

[18] *See id.* at § 500.4(d)(4); DFS, *Assessment of Public Comments on the Revised Proposed Second Amendment to 23 NYCRR Part 500* ("Public Comments"), 3-4, https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_apc_20231101.pdf.

[19] *See* Cybersecurity Regulation at § 500.1(d)(1).

[20] *See id.* at § 500.1(d)(2).

[21] *See id.* at § 500.1(h).

[22] *See id.* at § 500.7(c)(2).

[23] *See id.* at § 500.14(b).

[24] *See id.* at §§ 500.16(a)(1)(vii)-(viii).

[25] *See id.* at § 500.16(a)(2).

[26] *See id.* at §§ 500.16(a)(2)(i)-(vi).

[27] *See id.* at § 500.16(b).

[28] *See id.* at §§ 500.16(c)-(d).

[29] In general, the term "end of life management" refers to managing the use of a product or system after its original manufacturer or provider has stopped producing, supporting or providing upgrades for it.

[30] *See* Cybersecurity Regulation at §§ 500.3(b), (c), (d), (g), (h), (i), (n), (o).

[31] *See id.* at § 500.5.

[32] *See id.* at §§ 500.5(a)(1)-(2).

[33] *See id.* at §§ 500.5(b)-(c).

[34] *See* Proposed Amendments at § 500.5(d).

[35] *See* Cybersecurity Regulation at § 500.9(a).

[36] *See id.* at § 500.8(b).

[37] *See id.* at § 500.14(a)(3).

[38] *See id.* at §§ 500.7(a)(1)-(6).

[39] *See id.* at § 500.12(a).

[40] *See id.* at §§ 500.12(a)(1)-(3).

[41] *See id.* at § 500.12(b).

[42] *See id.*

[43] *See id.*

[44] *See id.* at § 500.15(b).

[45] *See id*. at §§ 500.17(b)(1)(i), (b)(2).

[46] *See id.* at § 500.17(b)(1)(ii).

[47] *See id.* at § 500.20(b).

[48] *See id.* at § 500.20(c).

[49] U.S. Department of the Treasury, Office of Foreign Assets Control, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Sept. 21, 2021), https://ofac.treasury.gov/media/912981/download?inline.

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.