Cyber Spotlight:
NYDFS Cybersecurity Regulation

WHAT DO THE PROPOSED CHANGES AND INCREASING ENFORCEMENT MEAN FOR COVERED ENTITIES?

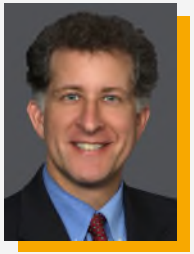
October 11, 2022

CYBERSECURITY AWARENESS MONTH 2022

MAYER | BROWN

Today's Presenters

Dominique Shelton Leipzig
Partner, Los Angeles



Jeff Taft
Partner,
Washington DC

Today's Agenda

- Proposed Changes to NYDFS Cybersecurity Requirements
- Recent Enforcement Actions
- What the Board Should Consider

Proposed NYDFS Regulations

WHAT YOU NEED TO KNOW

The 2022 Proposal

- NYDFS's cybersecurity requirements have become a model for other regulators since they were promulgated in 2017 in part because they are detailed and utilize a risk-focused approach.
- On July 29, 2022, the New York Department of Financial Services issued a "pre-proposal outreach" containing the text of revisions to its cybersecurity requirements for financial institutions ("2022 Proposal"). The 2022 Proposal is extensive and would significantly expand the requirements for covered entities.

We highlight some of these proposed requirements.

Financial institutions need to stay abreast of evolving regulatory expectations.

Section 500.1 – Definitions

The 2022 Proposal would:

- Stratify covered entities by creating "Class A Companies": institutions that have more than 2,000 employees (including employees of affiliates) or more than $1 billion in average gross annual revenue over the last three years (including revenue of affiliates). The measurements would not be limited to activities in New York or the United States.
- Expand the definition of "Risk Assessment" to specify that a risk assessment is a process of identifying cybersecurity risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, customers, consumers, other organizations, and critical infrastructure resulting from the operation of an information system. A risk assessment would need to take into account the specific circumstances of an institution.
- Create new definitions for an "Independent Audit," "Privileged Account," and "Senior Governing Body," which are discussed further in Sections 500.2, 500.7, and 500.3, respectively.

Section 500.2 – Cybersecurity Program

The 2022 Proposal would:

- Require Class A Companies to conduct an Independent Audit of their cybersecurity programs at least annually. An Independent Audit would be defined as an audit conducted by auditors free to make their decisions, not influenced by the institution being audited or by its owners, managers, and employees, and may include an audit by an internal auditor.
- Require all covered entities to make available to NYDFS the relevant and applicable provisions of a cybersecurity program that has been adopted by the institution but is maintained by an affiliate. NYDFS published guidance in 2021 with respect to the adoption of an affiliate's cybersecurity program.

Section 500.5 – Penetration Testing and Vulnerability Assessments

The 2022 Proposal would:

- Expand the penetration testing and vulnerability assessment requirements by specifying that penetration testing must be conducted at least annually by a qualified independent party and vulnerability assessments must be conducted regularly (instead of at least biannually).
- Class A Companies would need to conduct systematic scans or reviews for vulnerabilities at least weekly.
- All institutions would need to ensure that material gaps identified through testing are documented and reported to the Senior Governing Body and senior management.

Section 500.7 – Access Privileges

The 2022 Proposal would:

- Expand the access privilege requirements to more fully implement the principle of least privilege and restrict protocols that permit remote control of devices.
- Privileged Accounts, defined as those that perform security-relevant functions that ordinary users are not authorized to perform or can affect a material change to technical or business operations, would be subject to additional requirements.
- Institutions also would need to implement secure password rules, and Class A Companies would need to implement additional controls over Privileged Accounts.

Section 500.8 – Application Security; Section 500.9 – Risk Assessment

The 2022 Proposal would:

- Specify that the CISO must review application security materials at least annually, instead of periodically.
- With respect to risk assessments, the 2022 Proposal would require all institutions to update them at least annually and conduct an impact assessment whenever a change in the business or technology causes a material change to cyber risk.
- Class A Companies would be required to use external experts to conduct a risk assessment at least once every three years.

Section 500.11 – Third Party Service Provider Security Policy; Section 500.12 – Multi-Factor Authentication; Section 500.13 – Limitations on Data Retention

The 2022 Proposal would:

- Remove the exception that an agent, employee, representative or designee of an institution that is itself regulated by NYDFS need not develop its own third-party information security policy if it follows the policy of the principal institution.
- Require the use of multi-factor authentication for remote access to any network and enterprise and third-party applications from which nonpublic information is accessible. Further, multi-factor authentication would be required for most Privileged Accounts, except for those that prohibit interactive login or where the CISO has approved reasonably equivalent compensating controls. In addition, it would remove language indicating that a possession factor for multi-factor authentication may include a text message to a mobile phone.
- Expand the section on limitations on data retention to include a requirement that an institution maintain an asset inventory of all hardware, software, and outsourced technology resources.
- It would specify the information that must be collected and maintained for each asset, and require that the information be updated and validated as determined by the institution.

Section 500.14 – Training and Monitoring

The 2022 Proposal would:

- Expand the monitoring requirements to require an institution to monitor and filter emails to block malicious content from reaching authorized users.
- Institutions also would need to provide training, exercises, and simulations on cybersecurity and phishing.
- A Class A Company would be required to implement endpoint detection, anomalous activity monitoring, centralized logging, and security event alerting, unless the CISO has determined in writing that it would use a reasonably equivalent or more secure control.

Section 500.15 – Encryption of Nonpublic Information; Section 500.16 – Incident Response Plan

The 2022 Proposal would:

- Require institutions to maintain written encryption policies that meet industry standards and document approval of compensating controls for the non-use of encryption in writing.
- Expand the incident response plan requirement to include business continuity and disaster recovery ("BCDR") planning. Incident and BCDR plans would need to be distributed to all relevant employees, subject to training, and periodically tested.
- Institutions also would be required to periodically test their ability to restore systems from backups and maintain backups that are isolated from network connections.

Section 500.17 – Notices to Superintendent

The 2022 Proposal would:

- Expand the cybersecurity event notification requirement to add notification requirements to NYDFS for cybersecurity events where an unauthorized user has gained access to a privileged account or cybersecurity events that resulted in the deployment of ransomware within a material part of the institution's information system.
- Add a new notification requirement for extortion payments. An institution would be required to notify NYDFS of an extortion payment made in connection with a ransomware cybersecurity event within 24 hours of making the payment. The institution then would be required to provide notice to NYDFS within 30 days 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.
- Expand the annual compliance certification for non-compliance with the requirements by requiring written disclosure of requirements that the institution has not fully complied with and identification of all areas, systems, and processes that require material improvement, updating, or redesign. The compliance certification would need to be signed by the institution's Chief Executive Officer and CISO (or other person responsible for cybersecurity).

Section 500.19 – Exemptions; Section 500.20 – Enforcement

The 2022 Proposal would:

- Modestly expand the exemptions from the cybersecurity requirements by raising the personnel threshold, from 10 to 20, and the total assets threshold from $10 million to $15 million. It also would specify that gross annual revenue should be measured with respect to New York activities, and that reciprocal jurisdiction reinsurers, inactive individual insurance agents, and inactive individual mortgage loan originators are exempt from the cybersecurity requirements.
- Expand the enforcement provision by specifying that a single act or failure to act constitutes a violation of the cybersecurity requirements, including the failure to comply for any 24-hour period with any requirement. It also would list factors that NYDFS will take into account when assessing a penalty for a violation, such as an institution's history of prior violations.

Recent Enforcement Actions

Residential Mortgage Service – March 3, 2021

- Residential Mortgage Services, Inc. (“RMS”), a licensed mortgage banker, paid a $1.5 million penalty to for violations of the Cybersecurity Regulation.
- RMS collected private data in the course of its day-to-day operations, closing thousands of mortgage loans annually. A July 2020 examination uncovered evidence that RMS had been the subject of a cyber breach in 2019 which had not been reported to DFS.
- The breach involved unauthorized access to the email account of an RMS employee with access to a significant amount of sensitive personal data of mortgage loan applicants.
- Until prompted to do so by DFS in 2020, RMS failed to conduct an investigation and identify the consumer data exposed.
- The findings of the exam concluded RMS violated the DFS Cybersecurity Regulation in failing to timely report the breach, and that RMS failed to have a comprehensive Cybersecurity Risk Assessment, another requirement of the Cybersecurity Regulation.

Consent Order

National Securities Corporation – April 14, 2021

- National Securities Corporation ("National Securities"), a licensed insurance company, paid a $3 million penalty for violations of DFS's Cybersecurity Regulation that caused the exposure of a substantial amount of sensitive, non-public, personal data belonging to its customers, including thousands of New York consumers.
- National Securities collects private data in the course of its day-to-day operations, selling life insurance, accident and health insurance, and variable life/variable annuities insurance. The Department's investigation uncovered evidence that National Securities had been the subject of four cyber breaches between 2018 and 2020, two of which had not been reported to the Department as mandated by the Cybersecurity Regulation.
- These cyber breaches involved the unauthorized access of the email accounts of National Securities employees and independent contractors, who have access to a significant amount of sensitive personal data of National Securities' customers. The investigation uncovered, among other things, that National Securities violated the DFS Cybersecurity Regulation in failing to implement Multi-Factor Authentication ("MFA"), and without implementing reasonably equivalent or more secure access controls approved in writing by the Company's Chief Information Security Officer. Further, National Securities falsely certified compliance with the Cybersecurity Regulation for the calendar year 2018, due to the fact that MFA was not fully implemented.

Consent Order

Robinhood Crypto – August 1, 2022

Robinhood Crypto, LLC ("RHC") paid a $30 million penalty for failing to fully meet its legal obligations in two broad areas: (a) to maintain an effective BSA/AML program, including an adequate transaction monitoring system, commensurate with its growth; and (b) to fully comply with the Cybersecurity Regulations. The violations included:

- Enterprise-wide procedures and standards did not promote adequate accountability for RHC's cybersecurity program, including requirements for the CISO to report in writing at least annually to RHC's Board, as required in part by Section 500.04(b). There were also insufficient procedures in place for RHC's Board (or an equivalent governing body) to approve the written cybersecurity policy at least annually.
- Insufficient cybersecurity personnel to manage its cybersecurity risks and to perform the core cybersecurity functions specified in the Cybersecurity Regulation.
- Incident Response Plan did not include a process for notifying regulators and law enforcement in the event of a cybersecurity incident at the time of Examination.
- Notwithstanding these gaps in RHC's compliance with the Cybersecurity Regulation, on May 31, 2020, RHC filed a Certification of Compliance, attesting to compliance with the Cybersecurity Regulation for the calendar year 2019.

Consent Order

Board Issues

WHAT YOU NEED TO DO

Section 500.3 – Cybersecurity Policy

The 2022 Proposal would:

- Clarify that an institution's cybersecurity policy must be approved by the Senior Governing Body at least annually. A Senior Governing Body could be an institution's board of directors (or committee thereof), or the institution's senior officer if no board exists.
- Clarify that an institution should have procedures to implement its cybersecurity policy, and would add end of life management, remote access, and vulnerability and patch management to the laundry list of items that must be addressed in cybersecurity policies and procedures.

Financial institutions need to understand the new proposed board responsibilities.

Section 500.4 – Chief Information Security Officer

The 2022 Proposal would:

- Expand the section on chief information security officer ("CISO") requirements to more broadly address cybersecurity governance. It would specify that a CISO must have adequate independence and authority to ensure cybersecurity risks are appropriately managed.
- Require the CISO to report material cybersecurity issues, including updates to risk assessments and major cyber events, in a timely manner.
- Direct, if an institution has a board of directors, the board or a committee thereof to require management to develop, implement, and maintain a cybersecurity program. The board (or a committee) also would need to have sufficient expertise and knowledge to exercise effective oversight of cyber risk or be advised by persons with sufficient expertise and knowledge.

Section 500.10 – Cybersecurity Personnel and Intelligence

The 2022 Proposal would:

- Explicitly require a CISO and an institution's Senior Governing Body to maintain appropriate oversight to an affiliate or third-party service provider that performs cybersecurity compliance activities on behalf of the institution.

Board Requirements under the 2022 Proposal

- NYDFS' proposed rule would require board approval of cybersecurity policies that cover (at a minimum): "(a) information **security**; (b) **data governance** and classification; and [] customer **privacy**."
- "The board or an appropriate committee of **the board shall have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge,** to exercise effective oversight of cyber risk and a committee or subcommittee assigned responsibility for cybersecurity**.**"

Regulators Recommend Third-Party Advisors to Protect the Board of Directors

Questions?

THANK YOU

Dominique Shelton Leipzig
dsheltonleipzig@mayerbrown.com
+1 213 229 5152

Jeff Taft
jtaft@mayerbrown.com
+1 202 263 3293

Americas | Asia | Europe | Middle East

mayerbrown.com

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively the "Mayer Brown Practices") and non-legal service providers, which provide consultancy services (the "Mayer Brown Consultancies"). The Mayer Brown Practices and Mayer Brown Consultancies are established in various jurisdictions and may be a legal person or a partnership. Details of the individual Mayer Brown Practices and Mayer Brown Consultancies can be found in the Legal Notices section of our website. "Mayer Brown" and the Mayer Brown logo are the trademarks of Mayer Brown. © Mayer Brown. All rights reserved.