

The Newly Revised NYDFS Cyber Requirements for Financial Services Companies

WHAT YOU NEED TO KNOW ABOUT THE PROPOSAL

JULY 12, 2023

Today's Presenters



Raj De
Partner
Washington DC



Justin Herring
Partner
New York



Jeffrey Taft
Partner
Washington DC



Stephen Lilley
Partner
Washington DC



Raj De

Partner, Washington DC
+1 202 263 3366
rde@mayerbrown.com

Raj leads the firm's global Cybersecurity & Data Privacy practice and is a member of the firm's global Management Committee. Raj focuses his practice on cutting-edge legal and policy issues at the nexus of technology, national security, law enforcement and privacy. As the former General Counsel of the National Security Agency (NSA), Raj served as the agency's chief legal officer and senior advisor to the NSA Director. He also previously served in the White House as Staff Secretary and Deputy Assistant to the President of the United States and as Principal Deputy Assistant Attorney General in the Office of Legal Policy at the Department of Justice. Raj was also a Member of President Biden's Department of Justice Transition Team.



Justin Herring

Partner, New York
+1 212 506 2878
jherring@mayerbrown.com

Justin provides comprehensive representation and counseling on sophisticated cybersecurity matters, including global incident response, enforcement actions and related litigation, cyber monitorships and regulatory compliance. Prior to joining the firm, he was Executive Deputy Superintendent of the Cybersecurity Division at the NYDFS, where he served as the first leader of the agency's Cybersecurity Division, itself a first-of-its-kind unit at a financial services regulator. NYDFS issued the nation's first cybersecurity regulation for financial services, which has since become a model for other regulators such as the FTC, the SEC, and dozens of state banking and insurance regulators.



Jeffrey Taft

Partner, Washington DC
+1 202 263 3293
jtaft@mayerbrown.com

Jeff focuses primarily on cybersecurity and privacy issues for financial services entities, as well as bank regulation, payments and consumer financial services. He has extensive experience counseling financial institutions, merchants, technology companies and other entities on various federal and state banking and consumer credit issues, including the development and implementation of privacy, cybersecurity and information security programs under the Gramm-Leach Bliley Act, the NYDFS cybersecurity regulation and industry standards, such as PCI DSS and NIST. He has also advised banks, merchants, technology companies and financial services companies on issues relating to credit cards, debit cards, virtual currency, wire transfers and ACH transactions and other mobile payment products.



Stephen Lilley

Partner, Washington DC
+1 202 263 3865
slilley@mayerbrown.com

Stephen focuses his practice on helping clients navigate cutting-edge and interrelated litigation, regulatory, and policy challenges. He has significant experience working with clients to identify, evaluate, and manage cybersecurity and data privacy risks; responding to cyber incidents and vulnerability disclosures; and defending businesses in related litigation. He is regularly called upon to advise senior executives and board members on their most challenging cybersecurity risks, to help companies develop governance programs to mitigate those risks, and to lead training exercises to implement and refine those programs. Widely recognized for his cybersecurity law and policy experience, Stephen previously served as Chief Counsel to the Senate Judiciary Committee's Subcommittee on Crime and Terrorism.

Today's Discussion

- The DFS Regulation and Proposed Amendment
- Governance and Policy
- Expanded Program Requirements
- Incident Response
- Requirements for Large Companies
- Enforcement

Questions?

Please use the Q&A box (and be sure to include your email address) or email sclark@mayerbrown.com



The DFS Regulation & Proposed Amendment





The NYDFS Cyber Regulation

- NYDFS's cybersecurity regulation was first promulgated in 2017 and applies to financial services companies licensed in New York
- The existing regulation is **detailed and utilizes a risk-focused approach**. It incorporates principles from NIST cybersecurity standards, and requires a risk-based cybersecurity program
- Includes significant governance requirements, such as documented policies and procedures
- Applies broadly to all NYDFS-regulated companies, including companies with DFS-regulated subsidiaries
- Has been explicitly adopted as a model by other regulators, including for the NAIC model cybersecurity law, the CSBS non-bank model cybersecurity rule, and the FTC Safeguards rule



The Proposed Amendment

- **July 29, 2022:** NYDFS first published pre-proposal language for an amendment and accepts comments on the language
- **November 9, 2022:** A revised amendment was published for a 60-day notice and comment period
- **June 28, 2023:** A revised amendment was published for a 45-day notice and comment period
- **August 14, 2023:** Comment period closes
- **November 9, 2023:** Possible target date for finalization for publication of the final amendment



Governance and Policy





New Governance Requirements

Emphasis on governance requirements

- **Boards:** Responsible for approving cybersecurity policies and overseeing cyber risk management. Must have “sufficient understanding of cybersecurity-related matters” to exercise oversight.
- **CISO:** Defined as a qualified individual with adequate authority to implement an effective program. The CISO must also timely report to the Board on material cybersecurity issues.
- **Annual Compliance Certification:** Compliance must be certified by the CISO and CEO.



New Policy Requirements

The Proposed Rule Would Establish New Policy Requirements Relating to:

- Data retention
- End of life management
- Remote access
- Security awareness and training
- Systems and application security, and
- Vulnerability management



Incident Response

IMPLICATIONS FOR PLANNING AND RESPONSE



New Incident Response Requirements

New Requirements for the Incident Response Plan

- Recovering from backups
- Post-incident updates to the incident response plan
- Root cause analysis: how an event occurred and what will be done to prevent recurrence

New Requirements for Incident Notification

- Notification for incidents that resulted in the deployment of ransomware
- Notification for incidents where an unauthorized user gains access to a privileged account
- Requirement to provide any information requested to NYDFS and to provide updates
- Notification requirement for third-party incidents

New Requirement for Notification of Extortion Payment

Business Continuity and Disaster Recovery Planning

Business Continuity and Disaster Recovery (BCDR) Plan must be reasonably designed to ensure availability and functionality of the company's information systems and material services, and protect personnel, assets, and non-public information

Key Requirements:

- Identify all assets and personnel essential to the continued operations of the covered entity's business, including documents, data, facilities, infrastructure, services, etc.
- Identify supervisory personnel for each aspect of the plan
- Include a communications plan



New Requirements for Incident Response Planning & BCDR

- Make sure the plans are accessible during an incident (*i.e.* make hardcopies)
- Provide relevant training to all employees responsible for implementing the plan
- Testing of the plans with senior officers and the CEO at least annually
- Must maintain backups necessary to restore critical operations, and those backups must be adequately protected from alteration or destruction
- The ability to recover from backups must be tested at least annually



Expanded Program Requirements





Access Controls

Multi-Factor Authentication for All User Access

- Exceptions can still be made in writing by CISO
- Such exceptions must be periodically reviewed by CISO

Access Controls

- Several new requirements codify the principles of least access privilege, and require granting each user only the access necessary to perform the user's job, periodically reviewing all user access and privileges, disabling or securing remote control protocols, and promptly terminating access following employee departures
- To the extent passwords are used, the company must have a written password policy that meets industry standards



Other Requirements

- **Asset inventory:** Requires implementing a written policy and procedures to maintain a complete inventory of technology assets, including attributes such as owner, sensitivity, end-of-life date, and recovery time objectives.
- **Cybersecurity training** for all users must be at least annual and must include training in avoiding social engineering attacks.
- **Vulnerability management:** Requires automated vulnerability scanning of information systems at a regular frequency or whenever there are material changes to a system. Also now has an express requirement that vulnerabilities be timely remediated based on the risk they pose.
- **Penetration testing:** Requires annual penetration testing from inside and outside the company's network.



Large Companies

NEW REQUIREMENTS FOR "CLASS A COMPANIES"



Class A Companies

Definition

At least \$20 million in New York revenue, and either:

1. \$1 billion in total revenue, or
2. 2,000+ employees.

Affiliates

- All affiliates count, not just those licensed by NYDFS
- Limited exception: Do not need to count affiliates that do not share information systems, cybersecurity resources, or cybersecurity programs with the NYDFS-licensed entity



Class A Companies

Additional Requirements for Large Companies

- Independent Audit Requirement
- Endpoint Detection & Response
- SIEM (centralized logging and alerting)
- Privilege Access Management & Blocking Common Passwords



Enforcement





New Enforcement Section

Defines a Violation

- The material failure to comply with any section of the regulation for 24 hours; or
- The failure to secure or protect any individual's or entity's non-public information due to non-compliance with the regulation

Adds Mitigation and Aggravating Factors for the Department to Consider

- Mostly tracks similar factors in the New York Banking Law
- Includes cooperation, history of prior violations, extent of harm to consumers, timeliness of disclosures, willfulness of violation, size of business, etc.
- Also includes the extent to which the company's policies and procedures are consistent with nationally recognized cybersecurity frameworks, such as NIST



Thank You

Questions?

Please email
sclark@mayerbrown.com

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 Tauli & 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.