GIBSON DUNN

November 15, 2022

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES REVISES CYBERSECURITY REGULATION TO INCLUDE NEW REQUIREMENTS

To Our Clients and Friends:

On November 9, 2022, the New York Department of Financial Services ("DFS") announced proposed amendments ("Proposed Amendments") to DFS' Part 500 Cybersecurity Rules (the "Cybersecurity Rules"). The Proposed Amendments reflect a revised set of amendments based on the draft Part 500 amendments released on July 29, 2022 ("Draft Amendments"). The initial Draft Amendments were covered in our prior alert. The Proposed Amendments continue to reinforce DFS' forward-leaning, "catalytic" role in strengthening cybersecurity practices, but reflect that DFS did consider the comments received in response to the Draft Amendments as they clarify certain security requirements, strengthen some requirements to protect consumers and covered entities, and soften others to make them more closely aligned with industry standards and better account for public concerns.

We highlight seven key takeaways of the Proposed Amendments:

- Continue the Draft Amendments' stringent 72-hour and 24-hour notification requirements—and add new provisions that would require covered entities to (i) notify DFS within 72 hours if affected by a third-party service provider cybersecurity event, and (ii) respond within 90 days to any requests by DFS in connection with DFS' investigation of the cybersecurity event;
- Modify the definition of Class A companies, likely reducing the scope of those subject to heightened requirements;
- Soften some of the increased requirements on boards and senior management;
- Ease the heightened requirements for incident preparedness and operational resilience;
- Adjust certain technical requirements and their implementation timelines to be less aggressive;
- Expand requirements for risk assessments; and
- Reinforce new enforcement considerations.

We discuss each in turn below.

1. **Even More Stringent Notification Obligations**

The Draft Amendments previously proposed new, more stringent, cybersecurity event notification obligations, including:

- Requiring notification to DFS within 72 hours of unauthorized access to privileged accounts or the deployment of ransomware within a material part of a covered entity's information systems; and

- Imposing a new 24-hour notification obligation in the event a ransom payment is made and a 30-day requirement to provide a written description of why the payment was necessary, alternatives considered, and sanctions diligence conducted.

The Proposed Amendments maintain these tight timetables, as well as add other obligations for incident notification, which reinforces DFS' desire to be promptly kept informed about cybersecurity events at covered entities. These additional obligations include:

- Requiring covered entities to provide DFS with any information requested regarding the investigation of the notified cybersecurity event within 90 days; and

- Requiring covered entities affected by a cybersecurity event at a third-party service provider to notify DFS within 72 hours from the time the covered entity becomes aware of the event.

2. **Revised Definition of "Class A" Companies with Heightened Requirements**

The Draft Amendments increased cybersecurity obligations for a newly defined group of larger DFS covered entities, termed "Class A companies." Although some requirements were removed or altered under the Proposed Amendments, the heightened requirements on this class of covered entities under the Draft Amendments included to:

- Conduct weekly systematic scans or reviews reasonably designed to identify publicly known cybersecurity vulnerabilities and document and report any material gaps in testing to the board and senior management;

- Implement an endpoint detection and response solution to monitor anomalous activity and a solution that centralizes logging and security event alerting;

- Monitor privileged access activity and implement a password vaulting solution for privileged accounts and an automated method of blocking commonly used passwords;

- Conduct an annual, independent audit of their cybersecurity programs; and

- Use external experts to conduct a risk assessment at least once every three years.

After considering public comments, DFS modified its proposed scope for the new category of "Class A companies," likely reducing the number of covered entities that would fall within this definition. The new definition for Class A companies under the Proposed Amendments include covered entities with:

- In-state gross annual revenue of $20 million in each of the last two fiscal years from business operations of the covered entity and its affiliates, and that have:
    - *averaged* over 2,000 employees over the last two fiscal years; or
    - over $1 billion in gross annual revenue in each of the last two fiscal years.

While this is a broad definition that will still cover a large number of entities, it is a material narrowing of the Draft Amendments, which would have covered any entity with over 2,000 employees or companies with a three-year average of over $1 billion in gross annual revenue. Notably, the changes in the Proposed Amendments may result in excluding from the Class A definition certain covered entities that have a small presence in New York, and also shifts the Draft Amendments' focus on gross annual revenues averaged over three years.

Under the Draft Amendments, Class A companies were required to conduct weekly systematic scans or reviews with respect to vulnerability assessments. The Proposed Amendments remove this requirement, instead requiring covered entities more broadly to have a monitoring process that ensures prompt notification of any new security vulnerabilities. The Proposed Amendments also revise certain technical and audit requirements included in the Draft Amendments for Class A companies, requiring:

- A privileged access management solution along with an automated method of blocking commonly used passwords, or a reasonable equivalent of such blocking if approved annually by the CISO and if there is a reasonably equivalent or more secure compensating control; and
- Independent audits to be conducted by external auditors, modifying the initial proposal that an internal auditor would suffice, and thereby reducing flexibility on how such audits should be conducted.

3. **Softened Increased Obligations on Company Governing Bodies**

Under the Proposed Amendments, DFS re-commits to its focus on the accountability of boards and senior management, but softens and removes some of the previously proposed obligations. These revised obligations:

- Continue to require that the CISO has adequate authority and now also the "ability to direct sufficient resources to implement and maintain a cybersecurity program" (notably, the Proposed Amendments remove the Draft Amendments' requirement for adequate "independence");
- Only require that the CISO's annual board reports *consider* certain factors (i.e., the confidentiality of nonpublic information and the integrity and security of the covered entity's information systems, the covered entity's cybersecurity policies and procedures, plans for

remediating material inadequacies, etc.) in the report, but no longer require those factors be expressly addressed;

- Remove the obligation included in the Draft Amendments that the CISO review the feasibility of encryption of nonpublic information at rest and the effectiveness of compensating controls annually;

- Change the obligation that both the CEO and CISO sign an annual certification or acknowledgement of noncompliance to a requirement that the "highest-ranking executive" and the CISO sign—the Proposed Amendments now also require that such certification or acknowledgement include remediation plans and a timeline for their implementation; and

- Clarify that the role of the board (or its equivalent or the appropriate committee) shall also include exercising oversight of and providing direction to management on cybersecurity risk management.

These changes in the Proposed Amendments help clarify some ambiguities. For example, changing the obligation for signing certifications or acknowledgements of noncompliance to the CISO and the "highest-ranking executive" clarifies that all companies, even those without a CEO, are required to have and sign annual certifications or acknowledgements of noncompliance.

4. **Eased Expanded Requirements for Incident Response and Operational Resilience**

The Draft Amendments expanded measures requiring covered entities to have written plans for business continuity and disaster recovery ("BCDR"), including requiring certain measures to mitigate disruptive events. DFS also increased its requirements for incident response plans ("IRPs") in the Draft Amendments, requiring certain additional content requirements for IRPs, such as clearly defined roles. These requirements for BCDR and IRPs have remained largely the same in the Proposed Amendments, with a few practical changes. Specifically, the Proposed Amendments:

- Remove the Draft Amendments' requirement that covered entities provide relevant personnel with copies of the IRPs and BCDR plans and maintain these plans "offsite," instead requiring only that these plans be distributed to or otherwise accessible to relevant personnel; and

- Replace the requirement that backups be "isolated from network connections" with a requirement that backups be "adequately protected from unauthorized alterations or destruction."

Practically implemented, there may not be a significant difference concerning the changes to distribution of the IRPs and BCDR plans, as the Proposed Amendments require that the plans be accessible during a cybersecurity event, but the revised requirement will afford more flexibility for covered entities to develop an approach most effective for them. Further, in the Proposed Amendments, training is still required for personnel involved in implementing the plans, as are incident response and BCDR exercises, which are required at least annually. However, the changes to the requirement concerning backups is a significant technical change that will reduce the burden of compliance for many covered entities who do not have backups fully isolated from network connections.

5. **Modified Enhanced Technology and Policy Requirements**

The Proposed Amendments make significant changes to the strengthened technical and written policy requirements proposed by the Draft Amendments. Changes to technical requirements—focused on penetration testing, vulnerability management, and access controls—include:

- Requiring user access privileges for privileged accounts be reviewed at least annually and terminated upon employee departures, supplementing the Draft Amendments' requirements (i.e., that privileged accounts have multi-factor authentication and be limited to only users who need it to perform their job and when performing functions requiring such access);

- Clarifying that penetration testing should be conducted both inside and outside the covered entity's information systems' boundaries and can be conducted by a qualified internal or external independent party;

- Replacing the Draft Amendments' exception to multi-factor authentication for service accounts with an exception where the CISO approves a reasonably equivalent or more secure control, and otherwise requiring multi-factor authentication for: (i) remote access to the covered entity's information systems, (ii) remote access to third-party applications from which nonpublic information is accessible, and (iii) all privileged accounts; and

- Replacing the Draft Amendments' requirement for "strong, unique passwords" with a requirement to implement a "written password policy that meets industry standards."

Many of these revisions, such as allowing the CISO to approve reasonably equivalent controls to replace multi-factor authentication, provide covered entities with more flexibility in achieving compliance with these regulations.

Amendments focused on covered entities' written policies include:

- Replacing the Draft Amendments' requirement for "strong, unique passwords" with a requirement to implement a "written password policy that meets industry standards";

- Removing the requirement that covered entities' written policies and procedures include all information systems and their components, such as such as hardware, operating systems, applications, infrastructure devices, APIs, and cloud services;

- Requiring that the covered entity's cybersecurity policies, based on its risk assessment, additionally cover data *retention*, systems and network *monitoring*, *security awareness and training*, *systems and application security*, and incident *notification*;

- Requiring that incident responses plans include measures to *investigate*, in addition to mitigate, disruptive events;

- Requiring that cybersecurity awareness training be conducted annually, at a minimum, and cover social engineering exercises rather than just "phishing training"; and

- Requiring that the senior officers and the "highest-ranking executive," rather than the CEO, of the covered entity revise the incident response plan as necessary.

These measures provide important clarification for covered entities. Certain measures, such as allowing for a written password policy that meets industry standards, also demonstrate DFS' consideration of industry best practices in revising these regulations.

6. **Additional Requirements for Risk Assessments**

The Draft Amendments expanded the requirements for and definition of "risk assessments." These changes have been maintained in the Proposed Amendments. The Draft Amendments required that covered entities review and update risk assessments annually and conduct impact assessments whenever a change in the business or technology causes a material change to the covered entity's cyber risk. The requirement for impact assessments has since been removed, so covered entities now only have to review and update risk assessments annually and whenever such a change in business or technology occurs.

The Proposed Amendments also add a requirement that covered entities' written policies and procedures for vulnerability management mandate automated scans of information systems and a manual review of systems not covered by such scans to identify vulnerabilities. The frequency of these scans and reviews is to be determined by the risk assessment and where there are any major system changes.

7. **Reinforced New Enforcement Considerations**

The Draft Amendments contained two significant provisions regarding the enforcement of the Cybersecurity Rules, specifically that:

- Violations occur when a covered entity commits any act prohibited by the regulations or fails to satisfy a required obligation, which includes failing to: (i) comply for more than 24 hours with any part of the regulations, or (ii) prevent unauthorized access to nonpublic information due to noncompliance with the regulations; and

- DFS may consider certain aggravating and mitigating factors when assessing the severity of penalties, for example: cooperation, prior violations, provision of false or misleading information, harm to customers, etc.

The Proposed Amendments do not materially change these requirements.

Next Steps

The Proposed Amendments illustrate DFS' stated commitment to ensuring the Cybersecurity Rules continue to "keep[] pace with new threats and technology purpose-built to steal data or inflict harm," as Superintendent Adrienne Harris stated in announcing the Proposed Amendments. The publication of

the Proposed Amendments triggered a 60-day comment period that will end on January 9, 2023. Covered entities who have views on the proposed changes to the DFS Cybersecurity Rules should consider submitting comments. The Proposed Amendments demonstrate that DFS took into account prior comments as part of their "data-driven approach to amending the regulation to ensure that regulated entities address new and increasing cybersecurity threats with the most effective controls and best practices to protect consumers and businesses." Following this comment period, DFS will review submitted comments and decide whether to re-propose revised amendments or adopt the Proposed Amendments as final regulations.

Covered entities should assess their cybersecurity practices to ensure they have adequate controls in place to comply with these anticipated regulatory changes. We are available to assist in those efforts and will continue to monitor and report on developments during and after the comment period.

This alert was prepared by Alexander Southwell, Stephenie Gosnell Handler, Vivek Mohan, Amanda Aycock, Snezhana Stadnik Tapia, Terry Wong, and Ruby Lang.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity & Data Innovation practice group:

United States

Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)
David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com)
Gustav W. Eyler – Washington, D.C. (+1 202-955-8610, geyler@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)
Svetlana S. Gans – Washington, D.C. (+1 202-955-8657, sgans@gibsondunn.com)
Lauren R. Goldman– New York (+1 212-351-2375, lgoldman@gibsondunn.com)
Stephenie Gosnell Handler – Washington, D.C. (+1 202-955-8510, shandler@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Robert K. Hur – Washington, D.C. (+1 202-887-3674, rhur@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Vivek Mohan – Palo Alto (+1 650-849-5345, vmohan@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Rosemarie T. Ring – San Francisco (+1 415-393-8247, rring@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)

Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)

Europe
Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com)
Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Bernard Grinspan – Paris (+33 (0) 1 56 43 13 00, bgrinspan@gibsondunn.com)
Joel Harrison – London (+44(0) 20 7071 4289, jharrison@gibsondunn.com)
Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com)
Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)

Asia
Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)