PAUL HASTINGS

Stay Current

October 2022

Follow @Paul_Hastings

The New York Department of Financial Services Cybersecurity Rules — What Companies Need to Know

By Aaron Charfoos, Jacqueline W. Cooney & John J. Michels

On March 1, 2017, New York's Department of Financial Services ("NYDFS") implemented a comprehensive cybersecurity regulation aimed at financial institutions (the "Cybersecurity Regulation"). NYDFS has already brought a number of enforcement actions under the regulation resulting in multi-million dollar consent orders, and with the proposed amendments to the regulation that were introduced on July 29, 2022, the prevalence of these types of actions will likely continue.

At bottom, the Cybersecurity Regulation requires any company that is licensed under NYDFS—such as money transmitters and recipients of bit-licenses—to implement and maintain a comprehensive written cybersecurity program that is designed to protect the company's information systems and any non-public personal information stored on those systems. Among its many requirements, the Cybersecurity Regulation mandates that companies carry out and document a periodic risk assessment of their cybersecurity program, and establish policies and procedures governing information security, data governance, asset inventory, access controls, disaster recovery, incident response, and third party service provider management. In addition, the Cybersecurity Regulation requires companies to appoint an individual responsible for oversight of the cybersecurity program, appropriately staff and train its cybersecurity roles, implement encryption or other controls, and perform annual penetration tests on its environment.

To date, NYDFS has demonstrated a commitment to aggressively enforce the Cybersecurity Regulation, including a recent $30M settlement with a crypto company, a $5M settlement with an international cruise line, and a $3M settlement with a life insurance company. With proposed amendments to the Regulation recently announced, high dollar enforcement actions will likely only increase.

In July of 2022, the NYDFS's Superintendent announced that NYDFS was considering several amendments to the Cybersecurity Regulation. NYDFS posted the amendment during a public comment

period that ran from July 29 to August 18, 2022. If adopted as presently drafted, the amendment would implement a number of key changes, including those summarized below.

Topic Area	Key Aspects of Change
Heightened requirements for "large" companies.	The proposed amendment introduces "Class A Companies," which are NYDFS-regulated businesses that either (a) have over 2,000 employees, or (b) have over $1Bn in gross annual revenue, in each case including the company's affiliates. Class A Companies would be subject to heightened requirements, such as independent audits, endpoint detection requirements, and weekly vulnerability assessments.
New policy requirements	New policy requirements, including end-of-life management, remote access, and vulnerability and patch management, would be required under the amendments. These (and the remaining policies mandated by the Cybersecurity Regulation) must be approved annually by a senior governing body.
CISO Independence and Reporting	The covered entity's CISO must have "adequate independence" and authority to "ensure cybersecurity risks are appropriately managed." In the annual report mandated by the existing Cybersecurity Regulation, the proposed amendments require that the CISO additionally discuss plans for remediation of identified deficiencies related to the Company's cybersecurity program.
Limitations and oversight of privileged accounts	The proposed amendments additionally introduce a number of new technical safeguards that covered entities would be required to implement, including limitations on the number and use of privileged accounts, a "password vaulting solution" for privileged accounts, and the use of multi-factor authentication for privileged accounts.
Risk assessment cadence	The proposed amendments would require covered entities to perform a risk assessment annually, instead of "periodically."
Additional requirements for business continuity and disaster recovery plans	The proposed amendments introduce a number of new requirements related to business continuity and disaster recovery plans, including the identification of essential data, facilities, infrastructure, and personnel; a communications plan; and procedures for maintenance of back-up facilities. The amendments also require that covered entities maintain backups that are isolated from network connections.
Breach notification threshold	The proposed amendments require that a covered entity notify NYDFS within 24 hours of any "extortion payment," and, thirty days thereafter, provide a written description of the reasons that the payment was necessary, the alternatives that were considered, and the diligence that was performed with respect to the incident to ensure compliance with applicable law.

Key Takeaway – Companies operating in the financial sector that are subject to NYDFS jurisdiction should begin preparing for these changes now. Although the proposed amendment may be modified to

some extent prior to becoming final, the thrust of these new requirements will likely remain the same, and NYDFS has demonstrated that it is ready and willing to bring enforcement actions against perceived violators. To prepare for these changes, companies subject to NYDFS oversight should review their cybersecurity policies, procedures, and practices with counsel and begin prioritizing compliance efforts.

Our Data Privacy and Cybersecurity practice regularly advises companies on how to meet the requirements of new laws like these. If you have any questions concerning these U.S. state privacy laws or any other data privacy or cybersecurity laws, please do not hesitate to contact any member of our team.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

John J. Michels
1.312.499.6017
johnmichels@paulhastings.com

Washington, D.C.

Jacqueline W. Cooney
1.202.551.1236
jacquelinecooney@paulhastings.com

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com