JENNER & BLOCK

Fintech Focus: New York Issues Significant Amendments to its Forward-Leaning Cyber Regulations

Publications

November 7, 2023
By: Shoba Pillay, Laurel Loomis Rimon, Benjamin C. Seelig

In 2017, the New York Department of Financial Services ("NYDFS") enacted a landmark regulation requiring financial services institutions such as banks and insurance companies in the state to meet substantial cybersecurity preparedness requirements and certify such compliance on an annual basis. On November 1, 2023, Governor Kathy Hochul announced a significant overhaul of that regulation, with the goal of further improving the state's ability to protect sensitive consumer data held by financial institutions.

Key Changes to NYDFS Part 500

NYDFS's updated Part 500 Cybersecurity Regulation, effective November 1, 2023, aims to address the evolving and expanding cybersecurity threat landscape for holders of sensitive data.[1] The revisions both clarify existing requirements and add new obligations for entities under NYDFS's regulatory umbrella. Some of the key provisions in the amendment include:

- Creating a new category of "Class A" companies for covered entities with at least $20 million in gross annual revenue in each of the last two fiscal years from business operations and with either (a) over 2,000 employees, or (b) over $1 billion in gross annual revenue.[2] "Class A" companies will be required to conduct annual independent audits and implement programs to monitor privileged access activity along with endpoint detection and logging as part of their cybersecurity programs.[3]

- Creating a new definition for "senior governing body" as the board of directors or the senior officer or officers of the covered entity responsible for the covered entity's cybersecurity program, who will be required to exercise effective oversight over the covered entity's cybersecurity risk management.[4]

- Requiring cybersecurity policies and procedures focused on end-of-life management, remote access, asset inventory, and vulnerability and patch management, which, in addition to the other

policies required under Part 500.3, must be reviewed and approved by the entity's senior officers at least annually.[5]

- Unique to the Part 500 framework, the covered entity's senior governing body will now have a *scienter* requirement to have "sufficient understanding of cybersecurity-related matters." In addition to receiving regular cybersecurity updates, the governing body must also "confirm[] that the covered entity's management has allocated sufficient resources" to the cybersecurity program.[6]

- Covered entities will now have to annually conduct penetration testing, annual (rather than the previously detailed "periodic") cadence of risk assessments, and automated scans of information systems to identify, analyze, report, and remediate vulnerabilities.[7]

- Covered entities will now be required to employ a written password policy when passwords are used for authentication, a more robust policy on privileged access accounts, and use of multi-factor authentication "for any individual accessing any information systems of a covered entity" except for limited circumstances.[8]

- Covered entities will now be required to implement robust policies and procedures for information system asset management.[9]

- Covered entities will now need to establish, implement, and train employees on, and annually test, incident response, business continuity, and disaster recovery plans.[10]

- Covered entities are still required to certify Part 500 compliance by April 15 of each year but will now also have the option to file an "acknowledgment" when the company is unable to certify to full compliance.[11]

- Starting **December 1, 2023**, covered entities will now be required to report cyber incidents to the NYDFS Superintendent via an electronic form on the department's website within 72 hours of determining a cyber incident occurred at the entity itself, its affiliates, or at a third-party service provider.[12] Covered entities will also now be required to notify NYDFS of a Ransomware "extortion payment" within 24 hours of the payment, with a written description of the reason payment was necessary within 30 days thereafter.[13]

For most of the new regulatory requirements, regulated entities are required to come into compliance by **April 29, 2024**. More onerous sections of the new regulations (such as implementing data mapping, an incident response plan and business continuity plan, and getting executive boards up to speed) have longer transitional periods spanning one year, 18 months, and two years from November 1, 2023.[14] For more information, NYDFS will be hosting a series of

webinars on November 15, 2023, November 30, 2023, and December 7, 2023, to train regulated entities on these new requirements. Registration is available on the Department's website.

Conclusion

NYDFS regulated financial institutions should be keenly aware of how these changes to Part 500 impact their cybersecurity program. This is especially true given the looming April certification (or "acknowledgment") date incorporating some of these new requirements, and the fact that NYDFS is authorized to bring enforcement actions and impose penalties for a **single** violation of the new regulations.[15] Jenner & Block stands ready to assist covered entities with enhancing their cybersecurity program to bring it into compliance with the amended Part 500 regulations.

Footnotes

[1] New York State Department of Financial Services Second Amendment to 23 NYCRR 500, https://www.dfs.ny.gov/industry_guidance/regulations/final_adoptions_fs/rf_fs_2amend23nycrr500_text_20231101 ("Cybersecurity Requirements for Financial Services Companies").

[2] Cybersecurity Requirements for Financial Services Companies at 500.1(d).

[3] Cybersecurity Requirements for Financial Services Companies at 500.2(c) and 500.14(b).

[4] Cybersecurity Requirements for Financial Services Companies at 500.2(q) and 500.4(d).

[5] Cybersecurity Requirements for Financial Services Companies at 500.3.

[6] Cybersecurity Requirements for Financial Services Companies at 500.4(c-d).

[7] Cybersecurity Requirements for Financial Services Companies at 500.5(a-c) and 500.9.

[8] Cybersecurity Requirements for Financial Services Companies at 500.7 and 500.12(a).

[9] Cybersecurity Requirements for Financial Services Companies at 500.13.

[10] Cybersecurity Requirements for Financial Services Companies at 500.16.

[11] Cybersecurity Requirements for Financial Services Companies at 500.17(b).

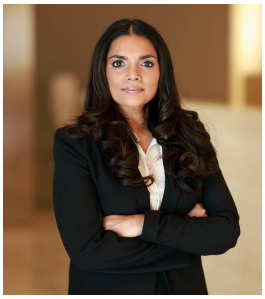
[12] Cybersecurity Requirements for Financial Services Companies at 500.17(a).

[13] Cybersecurity Requirements for Financial Services Companies at 500.17(c).

[14] Cybersecurity Requirements for Financial Services Companies at 500.21.

[15] Cybersecurity Requirements for Financial Services Companies at 500.20.

Related Attorneys



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605

Laurel Loomis Rimon
Partner
lrimon@jenner.com
+1 202 639 6868

Benjamin C. Seelig
Associate
bseelig@jenner.com
+1 312 840 7230

Related Capabilities

Data Privacy and Cybersecurity

Fintech and Crypto Assets

Stay Informed →