August 23, 2022

Via Electronic Mail

New York State Department of Financial Services
One State Street, 20th Floor
New York, NY 10004

Re: Proposed Second Amendment to 23 NYCRR 500 – Cybersecurity Requirements for Financial Services Companies

Ladies and Gentlemen:

The Bank Policy Institute welcomes the request to contribute comments to the New York Department of Financial Services ("NYDFS") pre-proposed outreach on amendments to the cybersecurity regulations contained within 23 NYCRR 500. As with previous iterations of the Part 500 cybersecurity regulations, we look forward to a productive and collaborative engagement with the NYDFS as the amendments are further developed and finalized.

There are four areas we believe the NYDFS should review and update prior to publishing the formal proposal for 23 NYCRR 500.

I. Harmonization

As cybersecurity incident reporting requirements continue to proliferate, it is critical that regulators coordinate and harmonize the increasing number of incident reporting requirements to minimize the regulatory burden placed on financial institutions addressing significant cybersecurity incidents, as well as to harmonize the proposed reporting timelines with existing definitions and notification standards. Harmonization of reporting requirements is central to achieving an appropriate balance between the benefits of incident reporting and the accompanying risks, harms, and operational burdens, particularly during a crisis when restoring and ensuring the security of services to customers is paramount. For example, the proposed amendments require a notice to NYDFS of a ransomware or extortion payment made within 24-hours of the payment. In parallel, the recently enacted Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") legislation contains a similar provision requiring a separate notice to the Cybersecurity and Infrastructure Security Agency ("CISA") in the event of a ransomware payment made as the result of a ransomware attack. Therefore, we urge the NYDFS to survey the incident notification and reporting landscape to ensure its proposed requirements

reasonably enable firms to balance the need to report with the ability to maintain security and a robust response and recovery capability.

Additionally, we have hailed the creation of the Cyber Incident Reporting Council (CIRC), also pursuant to enactment of CIRCIA. This law vests the newly created CIRC with the authority to "coordinate, deconflict, and harmonize" cyber incident reporting requirements to relieve covered entities of the burden of submitting multiple reports while working to investigate and remediate a significant incident. While the CIRC is aimed at enabling federal agencies to coordinate, deconflict, and harmonize federal incident reporting requirements, we encourage the NYDFS to take note of CIRC meetings and work product, and where appropriate consider ways to reflect the findings of CIRC recommendations in pursuit of streamlined and coordinated incident reporting.

II. Adherence to Risk-Based Approaches

The pre-proposal contains many instances where the NYDFS' proposed requirements are overly prescriptive and do not provide an opportunity for covered entities to apply a risk-based approach. The financial sector has long been a target of malicious cyber actors, and accordingly has invested in robust and ever-evolving measures to prevent, detect, and respond to cyber threats. We are leaders in the private sector in developing, maintaining, and enhancing cyber defenses, but there is no one silver bullet. The industry invests billions of dollars each year in cybersecurity, shares cyber threat intelligence through a pioneering model that has been replicated across industries, and employs thousands of cybersecurity professionals in its efforts to protect its customers' sensitive data and financial assets.

To consistently maintain this high level of threat prevention, detection, and response, firms need the flexibility to implement and comply with new requirements, especially those that increase costs, or require substantial interruption and time to implement. As the NYDFS continues to develop its proposed amendments to Part 500, we hope it will consider revising the language around several of its prescriptive security and risk management requirements, including as a non-exhaustive list, those aimed at data management practices (Section 500.13), access controls (500.7 and 500.12), pen-testing (500.5), encryption (500.15), business continuity requirements (500.16), and multifactor authentication (500.12).

III. Senior Governing Body/Board Governance

In its oversight role, the board of directors - or equivalent senior governing body - should receive sufficient information from applicable management or management committees or other sources to assess whether current approaches to address risks (including cyber), including mitigating steps to address process weaknesses, are appropriate in the board's view. In general, however, it should not be necessary – and, indeed, may be counterproductive – for the board to perform management-like responsibilities (e.g., such as formally "approving," or developing, day-to-day policies and procedures, planning activities, strategies or mitigating steps to address planning process weaknesses, or carrying out other risk-management and planning-related activities undertaken in the ordinary course of business) in order to provide effective oversight

of the planning/ risk-management process.[1] Certain specific observations and recommendations relating to proposed/contemplated requirements are set out below:

- **Proposed requirement: Annual requirement for the senior governing body to approve detailed cyber policy and/or policies (Section 500.3).** Security policies of the type described in the pre-proposal are often detailed, technical and voluminous. In general, it is not the role of the board to approve detailed policies (in contrast to strategic objectives and thresholds intended to constrain risk-taking by banking institution personnel) which could unnecessarily divert board attention from its oversight functions. The Board's role should focus on the oversight of enterprise risk management, including overseeing a system of checks and balances intended to safeguard a robust and secure IT infrastructure for the organization. To the extent an approval requirement is maintained, it should be clarified that the senior governing body can rely on summaries and that a board's review and approval is part of its oversight role. Especially if an annual requirement is maintained, there should be a distinction between significant policies that tend to remain constant and those that are updated on a regular basis. Where no meaningful changes to the policies have been proposed, annual review and approval should be unnecessary.

- **Proposed requirement: The CISO's report to the senior governing body should include, inter alia, plans remediating inadequacies in the program (Section 500.4(b)).** Absent special considerations, the NYDFS is encouraged to clarify and/or adopt the position that, as a general matter, materiality standards (i.e., from a board reporting perspective) should be applicable to any risk, audit or comparable reports or related information required to be presented to the board (or senior governing body) under the regulations. For example, mandatory board review of reports identifying any process issues or weaknesses (i.e., irrespective of the significance of the identified issues/ weaknesses) could unnecessarily divert board attention from its critical core functions. We would expect that senior management would establish a process to inform the board, or an appropriate board committee, of material findings, which may include thematic summaries.

- **Proposed requirement: 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 (Section 500.4(d)**). The pre-proposal appropriately recognizes that the role of the board of directors is one of oversight.[2] In addition, the pre-proposal also recognizes that an assessment of the collective capabilities of the board is more meaningful than an assessment of individual skills. The NYDFS is encouraged, however, to clarify that the boards themselves should

[1] See Bank Policy Institute's "Guiding Principles for Enhancing U.S. Banking Organization Corporate Governance," (2021).

[2] Id.

make their own determinations on how best to ensure an appropriately knowledgeable perspective on cyber-related matters for purposes of carrying out their oversight responsibilities.[3] This could mean, for example, that the board either retain third party external experts for briefings or guidance or education and/or the board rely on their access to the financial institution's own resources or staff with such expertise. More generally, the NYDFS is encouraged to clarify that the board should have the flexibility to choose which source(s) to draw upon, in light of the facts and circumstances, to ensure it has an appropriately knowledgeable perspective to carry out its oversight role.

- **Proposed requirement: A committee or subcommittee is assigned responsibility for cybersecurity (Section 500.4(d))**. The pre-proposal appropriately recognizes the ability of a board of directors to delegate functions to a board committee or subcommittee which is a fundamental concept of corporate law. The precise structures through which a particular board determines to carry out core functions of oversight will appropriately differ. For example, some institutions may appropriately establish a stand-alone committee (or committee that integrates oversight of cyber risk and resilience with discussions around strategic technology investment and innovation) while others may assign a committee with a broader remit (e.g., a risk committee) for cybersecurity. A board may also determine, depending on the committee structure and the organization's particular circumstances, that the same committee or different committees are best suited to oversee and address processes and controls designed to identify and manage cyber risks, on the one hand, and specific risk incidents, on the other (e.g., a special-purpose committee). The NYDFS is encouraged to clarify that boards have appropriate flexibility to delegate oversight responsibilities to a single committee or multiple committees as deemed appropriate.

IV. Ransomware

We are supportive of confidential notification and reporting to regulators regarding significant cybersecurity events soon after they occur. It is important that information is shared, and efforts by both the public and private sectors are coordinated to defend against the ever-present threat of a significant cyber event. However, we have significant concerns with the proposed amendment to section 500.17 requiring that covered entities provide explanation of a ransomware or extortion payment made in connection with a cybersecurity event within 30 days of the payment.

As with the existence of a cybersecurity or ransomware insurance policy, the occurrence of a ransomware and other extortive cybersecurity event is not necessarily or inevitably correlated to

[3] See Joint BPI, ABA, ICBA, MCBA Comment Response to Securities and Exchange Commission Proposed Rules Regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Requirements (File No. S7-09-22), available at: https://www.sec.gov/comments/s7-09-22/s70922-20128336-291093.pdf. ("Pressure from the SEC for public companies to designate directors with expertise in any single area may adversely impact their ability to identify and appoint directors with other experience, expertise, or capabilities they believe are appropriate for the oversight of the particular risks and opportunities the institution encounters, and may not result in more effective cyber risk oversight for the institution.")

an inadequate cyber defense. The requirement to submit a prescriptive written description of the reasons payment was necessary along with other internal deliberative and diligence considerations can be construed as second-guessing a victim of an attack and may have a chilling effect on future prudent decisions made and actions taken in pursuit of a successful incident response and recovery.

If the NYDFS chooses to keep the language of the amendment to section 500.17 as proposed, it is critical that the information specified by the NYDFS to be reported be treated as confidential and secured from public disclosure. Given the level of detail required together with the otherwise internal deliberative nature of the information sought by the NYDFS, any public disclosure of this information could result in further victimization at the hands of the very same, or other cyber threat actors, as well as unjustified reputational risk. We therefore urge the NYDFS to consider revising the amendment to Section 500.17 to facilitate a more collaborative information sharing relationship which avoids the potential for double victimization and inadvertent disclosure of a firm's most closely held internal deliberations around its strategic business decisions in pursuit of effective cybersecurity.

Conclusion

Once again, we look forward to working with you to ensure effective regulation that works to help secure the financial sector. Thank you for the ongoing opportunity to contribute to the development of the proposed amendments to 23 NYCRR 500.

Sincerely,

/s/

Gregg Rozansky
Senior Vice President, Senior Associate General Counsel
Bank Policy Institute

/s/

Brian Anderson
Senior Vice President, Technology Regulation (BITS)
Bank Policy Institute