August 14, 2023

New York State Department of Financial Services
c/o Cybersecurity Division, Attn: Joanne Berman
One State Street, 19th Floor
New York, NY 10004

Re: Updated Proposed Second Amendment to 23 NYCRR 500

Dear Ms. Berman:

On behalf of the American Financial Services Association ("AFSA")[1] thank you for the opportunity to provide comments on the Department of Financial Services' ("the DFS") updated proposed second amendment to the Cyber Security Requirements for Financial Services Companies (23 NYCRR 500). We appreciate the DFS considering our comments on the previous draft of this rulemaking, and we look forward to engaging with the DFS throughout the remainder of this rulemaking process. While we are supportive of some of the changes to this draft, we are concerned that other sections continue to present significant compliance challenges for covered entities.

500.1(c) Definition of "Chief Information Security Officer"

The definition of "CISO" requires that the individual have adequate authority to ensure cybersecurity risks are appropriately managed, including the ability to direct sufficient resources to implement and maintain a cybersecurity program. This is a vague standard that does not provide covered entities with enough direction. We request that the DFS provide guidance to clarify what exactly constitutes "adequate authority" and "sufficient resources" in the definition of CISO. These are difficult to ensure with only subjective measures.

500.1(f) Definition of "Independent Audit"

We appreciate and support the changes to the definition of "independent audit" to allow for internal auditors. Many financial institutions may employ internal auditors that operate independently and report directly to the company's board of directors, and these internal auditors are able to operate free of internal influence, similar to external auditors.

500.2(d) Affiliate Cybersecurity Program

Section 500.2(d) allows a covered entity to meet the requirement by adopting the relevant and applicable provisions of a cybersecurity program maintained by an affiliate. We request that the rules be amended

[1] Founded in 1916, the American Financial Services Association (AFSA), based in Washington, D.C., is the primary trade association for the consumer credit industry protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including direct and indirect vehicle financing, traditional installment loans, mortgages, payment cards, and retail sales finance. AFSA members do not provide payday or vehicle title loans.

to allow for similar provision allowing covered entities to meet the requirements through certification of an international cybersecurity standard with similar requirements (e.g. ISO/IEC 27001 for information security management systems (ISMS)).

500.4(b) & (c) Material Cybersecurity Issues

Section 500.4(b) & (c) require the CISO to report plans for remediating material inadequacies and timely report material cybersecurity issues to the senior governing body. We request that the final rules clarify what "material inadequacies," "timely" and "material cybersecurity issues" mean for the purposes of the CISO reporting to the board.

500.4(d)(3) Sufficient Understanding

Section 500.4(d)(3) requires that senior governing body "have sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors." Sufficient understanding is a vague standard, and we request that the DFS clarify what qualifies as sufficient understanding. We also request that senior governing body be able to use internal or external advisors. Internal advisors would be better suited to provide such guidance as they have the knowledge of a covered entities specific risks and controls and would also prove to be more cost effective. Furthermore, the amendment does not clarify how governance should be affected where the licensed entity is a subsidiary of a holding company. We ask that the amendment clarify that a senior officer of the licensed entity be a sufficient substitute where there is no board at the subsidiary level.

500.16(d) Senior Officer Involvement in Annual Testing of Incident Response Plan and BCDR Plan

Section 500.16(d) requires a covered entity to annually test its incident response plan with senior officers and the highest-ranking executives and its BCDR Plan with senior officers. Requiring participation in a lengthy exercise, regardless of the officer or executive's actual role in the incident response process, unnecessarily and inefficiently burdens covered entities. This requirement is overly burdensome because others in the organization are more likely to have the responsibility for executing the plans that these senior executives have approved. We respectfully request the DFS remove this requirement from the regulations or, at least, change the requirement to every three years.

500.17(a)(1) Cybersecurity Event at Affiliates

Amendments to Section 500.17(a)(1) require a covered entity to notify the DFS of a cybersecurity event at an affiliate within 72 hours. Many covered entities are large multinational corporations with parent companies and affiliates located around the globe. It is not feasible for such entities to report to the Superintendent every cybersecurity event at any affiliated entity around the world, regardless of whether the event has any effect on or implications for New York consumers. This requirement is overly broad and exceeds the scope of the DFS' regulatory authority.

500.17(b)(3) Notice of Compliance

We request that the DFS strongly consider removing the requirement that the highest-ranking executive signs the notice of compliance. The covered entity's CISO is in a better position and has the requisite knowledge to attest to compliance. At the very least the DFS should provide guidance regarding Section 500.17(b)(3) to make clear whether a covered entity's highest-ranking executive must sign the notice of compliance on behalf of a covered entity's affiliates, in the event that the affiliates do not employ a similar executive.

Effective Date

We appreciate the addition of extended effective dates for certain requirements in Section 500.22(d), but we believe 180 days for compliance with the remainder of the changes, as provided in 500.22(c) is not enough time to make many of the required policy changes. The proposed rule amendments would require numerous updates to existing operational systems, including changes to contracts with third-party service providers, development of new policies and procedures, and training staff to implement the new requirements. Therefore, we request that the final rules include a delayed effective date for all requirements, of at least 12 months after adoption of the final rule, which will allow affected financial institutions adequate time to implement the new requirements.

Thank you in advance for your consideration of our comments. We encourage the DFS to keep these requests in mind as it reviews comments submitted throughout this process. If you have any questions or would like to discuss it further, please do not hesitate to contact me at mkownacki@afsamail.org or at (202) 469-3181.

Sincerely,

Matthew Kownacki
Director, State Research and Policy
American Financial Services Association