January 9, 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: 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") proposed second amendment to the Cyber Security Requirements for Financial Services Companies (23 NYCRR 500). We appreciate the DFS considering our comments on previous rulemakings related to the cyber security requirements, and we look forward to engaging with the DFS throughout this rulemaking process.

500.1(f) Definition of "Independent Audit"

The proposed amended rules define an "independent audit," in part, as being conducted by external auditors. Many financial institutions may employ internal auditors that operate independently and report directly to the company's board of directors. While these internal auditors may be able to operate free of internal influence, similar to external auditors, their audits would not meet the requirements of the rules for the sole reason of the internal/external distinction. Accordingly, we request the definition of "independent audit" be amended to remove the requirement that the auditors be external.

500.2(c) Annual Audit of Cybersecurity Program

Section 500.2(c) would require an independent audit, as defined in 500.1(f), be conducted annually. While audits can more easily be conducted by independent *internal* auditors, an annual audit by *internal or external* auditors will come at significant costs and create compliance challenges. If the DFS accepts our above proposed change to the definition in 500.1(f), then this requirement will be manageable; however, we recommend changing the audit requirement to every three years in order accommodate the compliance challenges and clarifying that the audit requirement can be met through industry-standard independent audits, such as a SOC 2 Type 2 Report.

500.3 Cybersecurity Policy

[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.

Section 500.3 requires that "Procedures…be developed, documented and implemented in accordance with the written policy or policies." It is not clear whether this section would require a separate set of written "procedures" in addition to the written "policies." Accordingly, we request that the DFS clarify whether separate procedures are necessary or if policy documents can satisfy this requirement.

500.4(a) Adequate Authority

Section 500.4(a) requires that the CISO 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 licensees with enough direction. We request that the final rules clarify what "adequate authority" and "sufficient resources" means for the purposes of managing cybersecurity risks.

500.4(c) & 500.5(d)Timely Reporting and Material Cybersecurity Issues

Section 500.4(c) requires the CISO to timely report material cybersecurity issues to the senior governing body. Section 500.5(d) also requires that material issues be documented and reported to the senior governing body. We request that the final rules clarify what "timely" and "material cybersecurity issues" mean for the purposes of the CISO reporting to the board.

500.4(d)(3) Sufficient Expertise and Knowledge

Section 500.4(d)(3) requires that the board of directors "have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge, to exercise effective oversight of cybersecurity risk management." Sufficient expertise and knowledge is a vague standard, and similar to our above request regarding 500.4(c), we request that the DFS clarify what qualifies as sufficient expertise and knowledge. Furthermore, the amendment does not clarify how governance should be effected 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.

500.9(d) Risk Assessment

Section 500.9(d) requires Class A companies to use external experts to conduct a risk assessment at least once every three years, but the rules are not clear when the three-year clock begins. We that the DFS provide guidance as to whether the three-year clock starts to run on the effective date of the proposed amendment or from an alternative date and specify the date.

500.16(a)(2) Business Continuity and Disaster Recovery Plan

Section 500.16(a)(2) requires covered entities to establish a business continuity and disaster recovery plan ("BCDR plan"). While the requirement in part (a)(1) to establish an incident response plan is specific to a data breach or cybersecurity incident, the BCDR requirement extends far beyond the scope of the rules and would have significant implications and compliance burdens for covered entities. We respectfully request the DFS remove the BCDR requirement from the regulations.

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. 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)(3) Cybersecurity Event at Third-Party Service Provider

New Section 500.17(a)(3) requires a covered entity to notify the DFS of a cybersecurity event at a third-party service provider within 72 hours. While certain notifications for cybersecurity events outlined in 500.17(a)(1) only trigger with "material harm" or effect on a "material part" of the system or operations, it is not clear whether cybersecurity events at a third-party service similarly require a "material" effect. We request that the DFS update the rules to provide guidance whether third-party cybersecurity events must also have a "material" harm or effect.

500.17(b)(2) Notice of Compliance

We request that the DFS provide guidance regarding Section 500.17(b)(2) 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

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. While the rules generally provide 180 days for compliance, this is not enough time to make many of the required policy changes. Therefore, we request that the final rules include a delayed effective date, 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