January 27, 2017

Ms. Cassandra Lentchner
Deputy Superintendent for Compliance
New York State Department of Financial Services
One State Street
New York, NY 10004

Re: Revised Proposed Regulation 23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies

Dear Ms. Lentchner:

On behalf of the American Financial Services Association ("AFSA"),[1] thank you for the opportunity to comment on the Department of Financial Services'(NYDFS) revised proposed Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500). We appreciate your consideration of our comments regarding the previous version of the proposed regulation and the significant revisions reflected in the revised proposal.

Though AFSA shares the Department's goal of protecting New York citizens and financial institutions from the risks associated with cybercrime, we still have concerns with the revised regulation as proposed. As written, several of the revised proposal's provisions are unclear, unduly burdensome, and may subject financial institutions' information to added security risk.

Section 500.02 Cybersecurity Program

500.02(c) A Covered Entity may meet the requirements of this Part by adopting a cybersecurity program maintained by an Affiliate, provided that the Affiliate's cybersecurity program covers the Covered Entity's Information Systems and Nonpublic Information and meets the requirements of this Part.

We recommend amending this provision to read the following (additions underlined; removals struck through):

> A Covered Entity may meet the requirements of this Part by ~~adopting~~ <u>being subject to</u> a cybersecurity program maintained by an Affiliate, provided that the Affiliate's cybersecurity program covers the Covered Entity's Information Systems and Nonpublic Information and<u>, as applied to the Covered Entity,</u> meets the requirements of this Part.

[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.

500.02(d) All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

At many financial institutions, cyber defense tools, processes and capabilities are considered classified information and would put companies at great risk if the information were to fall into the wrong hands, as cyber threat actors could use this information to exploit institutions' defenses. Notwithstanding the fact that the proposed regulation contains a confidentiality provision which exempts disclosure of shared information under various state or federal laws, we strongly recommend limiting sharing of tools, processes or technologies due to the concern that recipients of the documentation may be subject to security breaches of their own. A financial institution has no control over information on its own cybersecurity program once that documentation has been shared, regardless of confidentiality clauses, and the institution must rely on the effectiveness of the recipient's cybersecurity programs in place. We recommend continued discussions with the regulator to advise on the measures in place, with limited sharing of documentation.

Section 500.04 Chief Information Security Officer

We request clarification whether there are any requirements for CISO reporting and recommend that any such requirements allow for flexibility based on a Covered Entity's organizational structure.

Section 500.06 Audit Trail.

500.06(b) Each Covered Entity shall maintain records required by this section for not fewer than five years.

In large companies, five years of audit trail data may quickly amass into a large, costly, and potentially unsearchable set of data. The cost of maintaining five years' worth of Cybersecurity event logs could easily rise into the tens of millions of dollars due to the costs for storage, bandwidth to collect the data, and people to manage it, among other costs. The data retention period should also be risk-based and not a one-size fits all prescription that ignores the nature of the company's business and its IT systems. We request that this provision be amended to require a Covered Entity to retain records for a time period based on its Risk Assessment for a period of no less than one year.

Section 500.09 Risk Assessment

Covered Entities are required to perform periodic risk assessments which then impact various parts of their cybersecurity programs. Section 500.22(b)(1) extends the transitional period for Section 500.09 by an additional six months beyond the base transitional period, with a new compliance date of March 1, 2018. However, Section 500.17(b) requires Covered Entities to annually submit to the superintendent a written statement by February 15 of each year certifying compliance with the regulation. As the first certification of compliance is due to the superintendent prior to the compliance date for a Covered Entity to have completed its first risk assessment—the cornerstone of a majority of the entity's cybersecurity program— we request confirmation that the certification of compliance due by February 15, 2018, will be limited to certifying that the Covered Entity is in compliance with the aspects of the regulation in effect as of February 15, 2018, and not certifying compliance with all provisions of the regulation. We also request that, to the extent a Covered Entity is performing a risk assessment under other legal or regulatory requirements applicable to it, a separate risk assessment is not required under the regulation so long as the assessment done meets the requirements of Section 500.09.

Section 500.11 Third Party Service Provider Security Policy

500.11(b)(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or Non-public Information being held by the Third Party Service Provider;

The revised proposed regulation significantly narrowed the requirements for reporting Cybersecurity Events to those with material effects, but the requirements for Third Party Service Providers reporting to covered entities have not been similarly qualified to reflect materiality of the Cybersecurity Event. As written, it is unclear if Cybersecurity Events "directly impacting" a Covered Entity will include unsuccessful attempts or be limited to material Cybersecurity Events.

Section 500.17 Notices to Superintendent

500.17(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event as follows has occurred:

> *(1) Cybersecurity Events of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; and*
> *(2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.*

We request that this section be amended to reflect existing New York law, which allows for notification "in the most expedient time possible and without unreasonable delay." A 72-hour time period does not allow the affected institution adequate time to appropriately understand the relevant facts as well as the size, scope, and materiality of such a Cybersecurity Event and would limit the usefulness of the information reported. Notification under the existing standard would allow for the most efficient use of resources at both the NYDFS and Covered Entities at a time when resources are most strained dealing with a Cybersecurity Event.

We also request clarification regarding whether the notification requirements include notifying the Superintendent of Cybersecurity Events affecting non-New York residents.

Section 500.19 Exemptions

The revised proposed rule, if adopted, will be the second or third set of cybersecurity requirements applicable to most of AFSA's members, as our members are subject to various rules set forth by the Federal Trade Commission (FTC) and Federal Financial Institutions Examination Council (FFIEC). NYDFS now proposes to establish an additional set of cybersecurity standards for many of our members that provide credit to New York residents, which will unnecessarily burden financial institutions and divert resources to compliance with multiple different cybersecurity requirements. We request that the regulations provide that otherwise Covered Entities that are also federally regulated subsidiaries or affiliates of federally chartered banks or are banks chartered by others states be exempted from the Rule.

As proposed, the scope of the revised regulation is not limited to banks or to financial institutions that hold customer assets, but also includes creditors who purchase consumer retail installment contracts from New York retailers and automobile dealers, or who make installment loans. Those credit

providers hold comparatively less customer information and do not act as stewards for the assets of the customer. We request that small loan and sales finance companies be excluded from the scope of the revised proposed rules.

The revised rules also are not limited to protecting information regarding New York residents. We request the scope of the proposed regulation be limited to customers served, or activity conducted, pursuant to the NYDFS license or similar authorization under the named New York laws.

The partial exemption for small entities is not sufficient to reflect the reduced cybersecurity risk and the reduced ability to fund extensive cybersecurity programs of smaller entities. The gross annual revenue component of that exemption is also not limited to income from customers served, or activity conducted, pursuant to the NYDFS license or similar authorization under the named New York laws. We request that the gross annual revenue amount be increased significantly, to at least $50 Million, and include only revenue from customers served, or activity conducted, pursuant to the NYDFS license or similar authorization.

Thank you in advance for your consideration of our proposed revisions to requirements of a Cybersecurity Program; our requests for clarification regarding CISOs, Risk Assessment compliance, and Third Party Service Provider reporting; and our request to broaden the exemptions for certain covered entities. If you have any questions or would like to discuss this further, please do not hesitate to contact me at 202-469-3181 or mkownacki@afsamail.org.

Sincerely,

Matthew Kownacki
Manager, State Research and Policy
American Financial Services Association
919 Eighteenth Street, NW, Suite 300
Washington, DC 20006-5517