November 14, 2016

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

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

Dear Ms. Lentchner:

The American Financial Services Association (AFSA)[1] supports the New York State Department of Financial Services' (NYDFS) goal of protecting New York citizens and financial institutions from cybercrime and appreciates the opportunity to comment on the proposed Cybersecurity Requirements for Financial Services Companies (proposed regulation).

Though we support the goal of the proposed regulation, we have significant concerns with the regulation as proposed, as some of the requirements would impose significant system, human capital and financial burdens for financial institutions without commensurate gains in the safety and security of consumers or our members' businesses.

This proposal is causing tremendous stress within our membership due to the proposed regulation's requirements, which are so prescriptive and extensive that institutions will be hard-pressed to not run afoul of the requirements even though they are leaders in thwarting cyberattacks. Therefore, we respectfully request that the regulation (1) embody a risk-based approach; (2) be reframed as guidance with a consistent set of best practice standards, rather than a formal rule; (3) program certification have a safe harbor from civil or criminal liability if conducted in a reasonable manner; (4) be implemented with time for responsible compliance over an extended, rolling implementation period; and (5) further adopt the other language and related suggestions described below.

One significant industry concern is that this proposed regulation deviates from existing federal cybersecurity standards in that it includes numerous prescriptive requirements not tied to the existence or level of the risks they purport to address. This could result in many expensive controls being implemented and maintained that, for some financial institutions, provide little or no additional value or protection to the institution or its customers. Cybersecurity is an expensive and continuous struggle for our members, as the nature and level of cybersecurity threats continually grow. Therefore, flexible, risk-based standards, like those in the National Institute of Standards and Technology (NIST) Cybersecurity Framework and other existing federal standards, are needed to allow cybersecurity resources to be deployed, for each institution, in a manner that will best protect its customers.

[1] Founded in 1916, the American Financial Services Association (AFSA) 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 and other retail sales finance, traditional installment loans, mortgages, and payment cards. AFSA members do not provide payday or vehicle title loans.

AFSA members provide credit in all 50 states. The development of differing state-specific prescriptive cybersecurity standards may cause financial institutions to devote more resources toward meeting differing standards, rather than focusing those resources on a risk-based approach that would best protect consumers. Accordingly, we suggest the NYDFS modify its proposal to adopt a risk-based approach that can adapt to and account for changes in technology, differences across firms, marketplace differences, and the cybersecurity threat landscape. This risk-based approach would allow for strategic prioritization and revision of controls to respond to technical developments and evolving threats.

Our specific concerns and suggestions follow.

Definition of Covered Entity

As proposed, the scope of the 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 have comparatively less customer information and do not act as stewards for the assets of the customer.

We request that the rule be clarified to provide that it applies only to information of a "Covered Entity" that relates to the customers served, and the activity conducted, pursuant to the license, registration, charter, certificate, permit, accreditation, or similar authorization under the New York banking law, the insurance law, or the financial services law.

The limited exemption in Section 500.18 of the proposed regulation should also be clarified to either exempt or partially exempt those entities whose activity conducted pursuant to the license, registration, charter, certificate, permit, accreditation or similar authorization is within those limits. Given the significant economic costs of compliance with the proposed regulation, we request that those limits also be significantly increased.

In order to prevent inconsistent overlapping cybersecurity requirements, we ask that the definition of "Covered Entity" in Section 500.01(c) of the proposed regulation exclude subsidiaries and affiliates of federally regulated banks.

Definition of Cybersecurity Event

Section 500.01(d) defines "Cybersecurity Event" as "any act or ***attempt***, successful or ***unsuccessful***, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System." (emphasis added). AFSA members are very concerned that the near-constant barrage of unsuccessful attacks they thwart on a daily basis would be included in this broad definition, thus replacing an institution's primary priority of fighting serious threats with reporting minor ongoing attempts already thwarted by existing safeguards.

Since financial institutions experience numerous attempts at unauthorized system access on a daily basis that are unsuccessful due to the existing cybersecurity programs and controls that institutions already have in place, this overly broad definition would require virtually any cyber event (materialized or *potential*) to be reported to the NYDFS within 72 hours (as required by Section 500.17 of the proposed regulation). To comply, financial institutions would have to expend a significant amount of resources to report to the NYDFS the ongoing unsuccessful attacks these institutions may

experience on a daily basis. This would drive extensive and inefficient reporting mechanisms because the proposed regulation does not discriminate between minor unsuccessful attempts and serious, actual attacks. This over-reporting would impose a tremendous administrative burden on both financial institutions and the NYDFS, which would be inundated with notices about attacks that do not require action and a misdirection of critical resources to reporting of "non-events" instead of focusing those same resources on continuing to fight unauthorized system access.

Furthermore, if a sophisticated cybercriminal were to gain access to the NYDFS's own system, the mere reporting of these events and non-events, and the company's response, would provide a roadmap of the types of attempts financial institutions are aware of and what works and what doesn't. This unintended consequence is hypothetical, but could be catastrophic if realized.

For these reasons, we recommend redefining "Cybersecurity Event" to exclude unsuccessful attempts at system access and refer only to confirmed attacks resulting in the confirmed unauthorized access, theft or manipulation of personally-identifiable nonpublic information about New York consumers.

Definition of Information System

Many AFSA members operate multiple business units under one corporate structure. As proposed, Section 500.01(e) of the regulation does not clarify which Information Systems of a Covered Entity are included within the scope of the proposed regulation (*i.e.,* all Information Systems of a Covered Entity or only those Information Systems directly involved in activities regulated by NYDFS). As such, we respectfully request that the NYDFS provide clarity as to which Information Systems of a Covered Entity are included within the scope of the regulation and be reasonable about which are realistically necessary to protect New York consumers.

Definition of Nonpublic Information

With tremendous and due respect, the Department's concerns and duties, which we appreciate and share, are with New York consumers. As proposed, the Department is seeking encryption of a massive amount of data, including data at rest, a request that would be extremely expensive and time consuming to implement without commensurate gains in protections to critical consumer information. The proposed regulation protects information that is not personally identifiable to a consumer. For example, the definition includes "information about an individual used for marketing purposes" in the definition of Nonpublic Information. As Section 500.15(a) requires all Nonpublic Information to be encrypted at rest and in transit, this would require cookie level information, IP addresses, and general marketing information to all be encrypted. Requiring encryption of this information is unnecessary.

We believe the definition of Nonpublic Information should be narrowed, consistent with New York State law and the Gramm-Leach-Bliley Act (GLBA), to *only* concern itself with nonpublic *personally identifiable* information about New York consumers that is sensitive.[2] Accordingly, we recommend that NYDFS adopt the following definition:

> "Nonpublic Information" means all electronic information that is not Publicly Available Information and is: (1) Any business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity; (2) Any information that

[2] N.Y. Gen. Bus. Law § 899-AA(1)(b).

an individual provides to a Covered Entity in connection with the seeking or obtaining of any financial product or service from the Covered Entity, or is about an individual resulting from a transaction involving a financial product or service between a Covered Entity and an individual, or a Covered Entity otherwise obtains about an individual in connection with providing a financial product or service to that individual; or (3) Any personal information consisting of any information in combination with any one or more of the following data elements: (a) social security number; (b) driver's license number or government-issued identification card number; (c) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (d) biometrics or health care data.

Cybersecurity Program

As proposed, Section 500.02(b)(2) requires the use of "defensive infrastructure" to protect a Covered Entity's information systems and the Nonpublic Information stored in them from being accessed. However, no definition of "defensive infrastructure" is provided in the proposed regulation. We are concerned by this vague and broad term, and AFSA requests more specificity and a roadmap, so that our members can ensure they do not run afoul of these requirements.

Similarly, we ask that the NYDFS clarify whether the review to determine if negative effects of Cybersecurity Events are mitigated, as provided in 500.02(b)(4), can be done by internal employees or departments or if there is a requirement to have independent third parties test the effectiveness of a Covered Entity's Cybersecurity Program.

Material Cybersecurity Events and Notices to the Superintendent

Section 500.03(b) of the proposed regulation requires the cybersecurity policy to be reviewed by the board of directors or equivalent governing board and approved by a senior officer of the Covered Entity no less than annually. As proposed, the report must also include a summary of all material cybersecurity events. However, the proposed regulation does not define what is considered "material." We ask that the NYDFS define the term "material" in order to clarify which information must be included, so that our members have a clear roadmap as to what raises to the level of "material."

We also are concerned with the provision's requirement that notice be provided to the Superintendent no later than 72 hours from the time the Covered Entity becomes aware of such a Cybersecurity Event. This time frame does not provide adequate time for a Covered Entity to determine the relevant facts, whether the event is indeed related to security threats, the event's size, scope and materiality, and to contact law enforcement.

In the event of a security breach, institutions should be able to focus efforts on identifying and mitigating a security incident, rather than prioritizing efforts to report all cases and meet differing state and federal security breach notification requirements. Accordingly, we recommend that the requirement to notify the NYDFS within 72 hours be revised to align with the existing New York State requirement that notification be provided "in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable

integrity of the system."[3] This non-prescriptive reasonable timeframe would allow a covered entity to focus on thoroughly investigating, understanding, and mitigating an incident.

Additionally, we ask that the NYDFS clarify the threshold for impact necessitating notifying the Superintendent (*i.e.*, 100 affected consumers or is notification required even if only one consumer was affected) and the preferred method of providing notices to the Superintendent (*i.e.*, should the notice be written, emailed, faxed, mailed, etc.), as that is not specified in the proposed regulation. To provide clarity, and ensure consistency with current New York law, we suggest that the NYDFS adopt the requirements of the New York data breach notification law, N.Y. Gen. Bus. Law § 899-AA (8)(a)(b).

Certification Safe Harbor or Removal

AFSA and its membership have significant concerns with the proposed regulation's required certification of compliance,[4] in that it does not enable the board of directors or designated senior officer to note any areas, processes, or systems that may not be in total compliance at the time but have been identified for remediation. As proposed, this certificate could create potential liability for the chairperson of the board of directors or senior officer if the controls are subsequently found to be inadequate, or if any innocent mistakes are made. Financial institutions should not be required to operate under standards that may inadvertently create significant civil or criminal liability. Civil or criminal liability should be limited only to the most egregious and knowing acts where such person was acting with reckless disregard. We recommend that the NYDFS remove this extreme requirement, or explicitly include a safe harbor for certifications made with reasonable care based on knowledge available at the time the certification was made.

Penetration Testing and Vulnerability Assessments

Section 500.05 requires the cybersecurity program to include penetration testing at least annually and vulnerability assessments at least quarterly on the Information Systems of a Covered Entity. As proposed, the scope of this seems to include all information systems belonging to a Covered Entity or for those of a third-party service provider. Financial institutions often have massive and complex information technology environments that this general scope description would introduce significant regulatory risk to, as valuable resources would be expended on low-value targets.

AFSA requests the NYDFS narrow the scope of the Covered Entity's information systems that fall within this regulation. The scope should reflect a risk-based approach that a Covered Entity would have to document in its policies and procedures, but one that would allow a Covered Entity to conduct testing and assessments in a manner and frequency that aligns with the assessed level of risk for the system. Additionally, we ask the NYDFS to define "vulnerability assessments," as this definition is not provided in the proposed regulation. We also ask that the NYDFS clarify whether the vulnerability assessments can be conducted internally.

Audit Trail

Section 500.06 requires a Covered Entity's Cybersecurity Programs to include implementing and maintaining audit trail systems that allow for complete and accurate reconstruction of all financial transactions and accounting necessary to enable the Covered Entity to detect and respond to a

[3] N.Y. Gen. Bus. Law § 899-AA(2).
[4] Proposed regulation, §§ 500.03, 500.04 (*See also* proposed regulation Appendix A).

Cybersecurity Event for six years. Read broadly, this audit trail would include log system events, including access and alterations made to the audit trail systems by the systems or by an Authorized User, as well as all system administrator functions performed on the systems.

The language of the proposed regulation reads to include *all* financial transactions, but "financial transaction" is not defined. We ask that the NYDFS clarify what financial transactions must be included, as implementing and maintaining an audit trail of this broad scope is unnecessary and would unduly strain existing systems.

We also ask that the NYDFS allow a Covered Entity to maintain audit trail records under its record retention schedules, rather than requiring a six year hold period, and to conduct investigations to potential incidents as appropriate so that they are commensurate with the financial institutions assessed level of risk for its financial transactions and information systems. Complying with the regulation as proposed would require a Covered Entity to waste resources to store data that is no longer of use to the institution and also increase the risk exposure by storing sensitive data longer than it is useful.

Third-Party Information Security Policy

Section 500.11 requires each Covered Entity to implement written policies and procedures designed to establish a comprehensive due diligence program for third-party service providers, including preferred provisions to be included in contracts and information system controls third-party service providers must implement, including provisions addressing the use of encryption to protect Nonpublic Information in transit and at rest.

We ask that the NYDFS clarify that the contractual provisions listed therein are recommendations and not absolute requirements. There may be instances when negotiating the contractual agreement that the third-party service provider is not willing to agree to the preferred provisions, but that through completing the due diligence process a Covered Entity agrees to assume the risk and enter into a contract with the service provider without the preferred provisions in the final executed agreement.

In addition, AFSA requests that the encryption requirements match the encryption requirements for the Covered Entity under the final regulation. Specifically, AFSA requests that encryption requirements be driven by the data classification to a more granular level than a blanket control requirement for all Nonpublic Information. Encryption should be viewed as a control and should not be prescribed as the general one-size fits all control applied to all states and conditions where data may reside. We respectfully request that the NYDFS align with the Office of the Comptroller of the Currency and Federal Financial Institution Examination Council (FFIEC) standards and best practices prescribing appropriate cryptography procedures.

Multi-Factor Authentication

Section 500.12(c) requires multi-factor and risk-based authentication for any individual accessing any web-based applications that capture, display or interface with Nonpublic Information. As proposed, the regulation does not differentiate between internal and external facing web-based applications, nor does it define "individual," which could unnecessarily include customers; as discussed earlier, we believe the proposed approach to Nonpublic Information is overly broad and should be limited to Nonpublic personally identifiable information.

Requiring multi-factor authentication on all internal and external web applications across a Covered Entity adds unnecessary costs for financial institutions and would result in limited or no value added to the institution's overall security, as it fails to differentiate between high and low value assets. This approach would also introduce significant regulatory risk due to the open interpretation of the proposed regulation.

We recommend that the NYDFS allow for selection of the levels of authentication controls at the discretion of the Covered Entity based on its risk management framework, provided that it is following existing regulatory requirements and industry best practices.

Encryption of Nonpublic Information

Section 500.15 of the proposed regulation requires all Nonpublic Information held or transmitted by a Covered Entity to be encrypted both in transit and at rest. This includes education, financial, occupational, employment, and marketing information about a person. All of those data elements, while arguably nonpublic in nature, would not result in harm to a person's identity or credit if breached. Requiring encryption of this type of information is unnecessary, expensive, and overly burdensome without a commensurate gain in consumer protection.

The proposed regulation also does not address whether the data must be encrypted at rest in an unstructured format such as excel or CSV or a structured format such as SQL or oracle. Encrypting all unstructured data at rest would disrupt business processes and be impossible to verify. If the NYDFS does not remove the requirement for encryption of data at rest, AFSA recommends that it only require encryption for structured databases. Additionally, the regulation should not require encryption of data in transit when transit is entirely within the company's internal system. Encryption in transit for all data moving intracompany would be exceedingly burdensome for financial institutions without any measurable gain in consumer protection.

In addition, while Section 500.15(b)(2) indicates that an entity may utilize other protective controls approved by the CISO in the event that encryption of the data is infeasible, it only provides a grace period of one year for data in transit and five years for data at rest, after which time it is assumed that the entity must have enabled encryption.

Encryption requirements should be driven by the data classification to a more granular level rather than a blanket control requirement for all Nonpublic Information. There are multiple security controls that are being applied to protect the confidentiality and integrity of data. Encryption should not be prescribed as a one-size-fits-all approach applied to all states and conditions where data may reside. Furthermore, AFSA members request that if a Covered Entity has compensating controls in place, encryption not be required, but rather be treated as a suggested tool. As previously stated, AFSA hereby requests that the NYDFS align with the FFIEC standards and best practices prescribing appropriate cryptography procedures

Effective Date and Transitional Period

For the reasons stated above, complying with the regulation's effective date of January 1, 2017—especially given that the transition period provided in Section 500.21 is only 180 days—is unreasonable, impractical and likely impossible for Covered Entities to meet. As currently proposed, many of the regulation's necessary changes will take over a year for entities to implement. In addition, given that the regulation was proposed on September 28, 2016, and final comments are due 45 days

from that date (*i.e.*, November 14, 2016), the NYDFS will only have approximately six weeks to review and consider comments and make any changes to the regulation. Therefore, the January 1, 2017, effective date is not practical. In order to provide for enough time to complete financial and operational plans to meet these standards, transition all systems, and negotiate any necessary changes to contracts with third party service providers, we recommend the effective date be extended to at least January 1, 2018, and the transitional period be extended an additional 24 months with the final recommended standards to be implemented on a rolling basis over the course of the 24 month period, so financial institutions may be permitted to prioritize implementation of necessary technological, operational and contractual solutions to ensure compliance with the proposed regulation.

Please keep in mind that existing systems upgrades and other priority developments are already scheduled out, sometimes 12-48 months in advance. Complying with new requirements means increased human capital to facilitate those changes and potentially delaying other critical systems changes which are already scheduled. Further, because our members operate during business hours across multiple time zones, systems changes may only be tested and implemented during brief periods at night or on weekends, significantly narrowing the time for multiple other technical needs to be met. Our request for additional time is not a stalling tactic—it is to make sure that our member financial institutions are able to meet existing identified critical needs *AND* the NYDFS' requirements responsibly.

Conclusion

Thank you sincerely for your consideration of our concerns and suggestions. AFSA again respectfully requests that the Department avoid prescriptive requirements not based on the financial institution's risk, set a rolling implementation period, that only personally-identifiable personal information be protected at the highest level, that program certification have a safe harbor from civil or criminal liability if conducted in a reasonable manner, and that the regulation itself be reframed as guidance with a consistent set of best practice standards, rather than a formal rule.

If you have any questions, or if we can provide further information or explanations to assist you, please do not hesitate to contact me.

Respectfully,

Danielle Fagre Arlowe
Senior Vice President
American Financial Services Association
919 18th Street NW, Suite 300
Washington, DC 20006
952-922-6500 (office)
202-412-3504 (cell)
dfagre@afsamail.org