August 2, 2019

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Standards for Safeguarding Customer Information
16 CFR Part 314, Project No. 145407

Dear Commissioners:

The American Financial Services Association (AFSA)[1] respectfully requests that the Federal Trade Commission (FTC) make substantial changes to the proposal (Proposed Rule) to amend the Standards for Safeguarding Customer Information (Safeguards Rule or Rule) before it is finalized.

I. Introduction.

AFSA members do their best to protect their customers' information, as they have every incentive to do. No financial institution wants to be the next headline for a massive data breach. Thus, we support the FTC's goal of safeguarding consumers' information. We believe that the FTC can meet that goal and maintain the flexibility that is a crucial part of the current Rule by incorporating several changes to the Proposed Rule. First, we ask that the FTC include a safe harbor in the Rule. Second, we encourage the FTC to ask Congress for the authority to preempt state laws. Third, we suggest that the FTC broaden the exemption for smaller financial institutions. And lastly, we ask that the FTC use a risk-based approach in the Rule. The Safeguards Rule must continue to strike the right balance between providing guidance to financial institutions and preserving flexibility to address threats.

II. AFSA members have every incentive to do their absolute best to protect their customers' information.

AFSA understands and agrees with the importance of safeguarding customer information. Cybersecurity remains a top priority for AFSA's members. Given the well-known risks of reputational damage and financial costs resulting from data breaches, every financial institution has a strong incentive to protect its customers' information.

Financial institutions expend significant resources to safeguard consumer data and protect against cyber-attacks. Both large and small financial institutions develop and use information-security plans and they deploy all manner of defensive software. Larger financial institutions may spend over $500 million per year to do so.

A great deal of time and attention is invested in complying with state and federal information security regulations. In addition to developing and using protective software, financial institutions engage in extensive employee

[1] Founded in 1916, AFSA is the national trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including traditional installment loans, mortgages, direct and indirect vehicle financing, payment cards, and retail sales finance.

information security training and monitoring. Interestingly, some financial institutions report that just under half of corporate information security activities are not security-oriented, but rather compliance-oriented.[2]

III. Including a safe harbor in the Proposed Rule will preserve flexibility while maintaining strong safeguards.

The Proposed Rule states that, "The Commission continues to believe that a flexible, non-prescriptive Rule enables covered organizations to use it to respond to the changing landscape of security threats, to allow for innovation in security practices, and to accommodate technological changes and advances."[3] AFSA agrees that flexibility in the Rule is crucial to enable financial institutions to use innovation to respond to new threats.

Moreover, the FTC writes, "The proposed amendments are designed to preserve that flexibility while doing more to ensure that financial institutions develop information security plans that are appropriate, reasonable, and designed to protect customer information. Although the Commission believes the proposed approach is sufficiently flexible, it seeks comment on whether the approach creates unintended consequences for businesses…"[4]

In order to better meet the dual goals of ensuring that financial institutions have information security plans that protect customer information and preserving flexibility in the Rule, AFSA urges the FTC to include a safe harbor in the Rule. Specifically, the Rule should include a safe harbor for companies complying with one or more of the following standards: the Federal Financial Institutions Examination Council (FFIEC) Interagency Guidelines, the cybersecurity regulations issued by the New York Department of Financial Services (Cybersecurity Regulations), or the Payment Card Industry Data Security Standard (PCIDSS).

The inclusion of a safe harbor will reduce the compliance burden on financial institutions while still providing protection for consumers. We suggest that because the FTC modeled the Proposed Rule on the Cybersecurity Regulations, the safe harbor cover financial institutions complying with the Cybersecurity Regulations. Additionally, including the FFIEC Interagency Guidelines and the PCIDSS in the safe harbor is appropriate because requirements in those standards are strong and approved by prudential banking regulators with safety and soundness concerns. If regulators concerned with a bank's safety and soundness believe that the safeguards included in the FFIEC Interagency Guidelines and the PCIDSS sufficiently protect consumers, we see no reason why the FTC would disagree.

Thus, AFSA strongly encourages the FTC to include a safe harbor in the Rule.

IV. A national data security rule may be appropriate, but only if it preempts state laws.

While AFSA recognizes the role states have in consumer protection—indeed most AFSA member companies operate subject to state licensure and regulation—we believe data security and privacy is so significant a public policy issue that it transcends state borders, and that consumers and industry alike are best served by a transparent, non-duplicative regulatory regime.

---

[2] PwC, "Global State of Information Security Survey 2016. Oct. 9, 2015. Available at: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.
[3] 84 FR 13160.
[4] *Ibid.*

Operational and compliance issues arise when an individual state promulgates requirements unique to that state without demonstrating a security challenge unique to that state. In reality, information processing flows across state borders—often on the cloud—and protecting privacy and enhancing information security is not only a multi-state, but a global, transnational issue.

Along with existing federal law, regulation, and agency guidance, practical data security and privacy are based on national standards developed by the FFIEC and the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) Cybersecurity Framework. Additionally, self-regulatory and standards-setting bodies draft standards on an often global basis. See, for example, the PCIDSS, which imposes comprehensive control objectives relating to information security.

AFSA strongly supports a single, federal, risk-based standard that preempts state law. Inconsistent state laws regarding data security and the lack of a national standard for businesses have resulted in uneven consumer protection, as well as higher compliance costs for financial institutions.

We realize, of course, that the Gramm-Leach-Bliley Act (GLBA) does not grant the FTC the authority to preempt state law. AFSA believes that Congress should give the FTC the authority to preempt state laws before the FTC's Safeguards Rule becomes a floor for state data breach laws and not a ceiling.

While some existing federal laws relating to privacy do not preempt state law, federal preemption in this area is not uncommon.

Currently, three federal privacy statutes preempt state law: the Children's Online Privacy Protection Act of 1998;[5] the CAN-SPAM Act of 2003;[6] and the 1996 revision of the Fair Credit Reporting Act, as well as further updates to that statute enacted in the 2003 Fair and Accurate Credit Transactions Act.[7]

V. Smaller financial institutions should be exempt from an amended Safeguards Rule.

In the commentary to the Proposed Rule, the FTC writes, "As to the commenters that stated that the current Rule works well and that companies have already developed compliance programs under it, the Commission does not believe the proposed new requirements would require an overhaul of existing compliance programs."[8]

To the contrary, the Proposed Rule would require financial institutions, particularly smaller financial institutions, to implement a multitude of changes to their information security programs. While financial institutions have data security standards in place, they are scaled to the size of the institution. The Proposed Rule would impose national bank data security standards on companies with only a few branch offices.

For these institutions, the Proposed Rule would create significant compliance issues and increased costs, which may not be necessary. Such financial institutions would have to: create a new Chief Information Security Officer position and employ such a person, protect additional information (not just sensitive information), increase encryption levels, increase storage/server ability, create a different way to allow access to information, create

[5] 15 USC §6502(d).
[6] 15 USC §7707(b)(1).
[7] 15 USC §§ 1681m(a), 1681m(b), and 1681s-2.
[8] 84 FR 13160.

brand new audit trails, purge software systems in a way never done before, and increase internal audits and audit staff to do the additional work.

Basically, these smaller financial institutions would have to hire a top-level IT person in-house, presumably one at the same level as national financial institutions. Given the current demand for such personnel, such an individual's salary level, plus the costs of additional support staff, along with adding, updating, or replacing information security software and procedures and the situation quickly becomes unduly expensive for small institutions. The Proposed Rule would allow financial institutions to designate a service provider to fulfill this role, but that too is a significant expense. And of course, because the financial institution is still responsible for its own information security, someone must oversee the service provider. For the oversight to be effective, the person overseeing the service provider would still need extensive IT experience.

It took companies thousands of hours to comply with the Cybersecurity Regulations, hours that smaller companies simply do not have. The FTC recognizes that some of the requirements in the Proposed Rule would place an undue burden on smaller financial institutions. However, the proposed exemption is too narrow. Currently, the exemption would apply to financial institutions that maintain customer information concerning fewer than 5,000 customers. The California Consumer Privacy Act applies to entities that have the personal information of 50,000 or more consumers. We suggest that the FTC adopt that standard.

VI. The Rule should incorporate a risk-based approach, which leads to better privacy protection than a prescriptive, one-size-fits-all standard.

AFSA recommends that the FTC reevaluate the prescriptive standards outlined in the Proposed Rule. Prescriptive standards run the risk of becoming a mere "check the box" exercise, as opposed to truly enhancing security. Through the implementation of the flexible standard currently laid out in the Safeguards Rule, financial institutions have developed different administrative controls to satisfy information security objectives.

Financial institutions should be able to use a risk-based approach to focus on the likelihood that an event will occur and what the resulting impact would be. By taking this information into account, institutions can prioritize information security activities.[9] A risk-based approach enables organizations to make informed decisions about information security expenditures and develop methods to handle the unique risks faced by different institutions. Regulations that allow for flexibility give institutions the ability to mitigate, transfer, avoid, or accept risk, depending on the potential impact.

Inflexible requirements, on the other hand, could prevent financial institutions from taking advantage of new technologies or methods that may provide better protection. Prescriptive requirements undermine the ability of information security personnel to prioritize sensitive or vulnerable information systems and significant threats. They force institutions to reallocate limited resources to fulfilling regulatory obligations and away from targeting high-priority information security issues. Any final rule should not require firms to implement specific technology methods that may be superseded or may be infeasible, especially where there are equally secure compensating controls.

[9] For example, some financial institutions, such as installment lenders or vehicle finance companies, do not hold customer deposits and do not offer open lines of credit or credit cards. Unauthorized access to a customer account at such a financial institution certainly has privacy implications, but is unlikely to result in financial harm to the consumer as there can be no unauthorized withdrawals from or charges to a customer account at such a financial institution.

We outline our specific suggestions to achieve a risk-based approach below.

A. The Proposed Rule should be limited to sensitive information that is stored electronically.

Primarily, the Proposed Rule should be limited to sensitive information and electronic information. It should not apply to all customer information, nor should it apply to paper records.

The definition of "customer information" in the Proposed Rule includes both sensitive and non-sensitive information. It would be impractical to apply several sections of the Proposed Rule to non-sensitive information. Specifically, non-sensitive information does not need to be encrypted or disposed of in the manner outlined in the Proposed Rule. Moreover, customers should not be required to use multi-factor authentication to access non-sensitive information. AFSA asks that the FTC clarify that these requirements apply only to sensitive information.

Similarly, parts of the Proposed Rule would be impractical if they applied to customer information in both paper and electronic form (*e.g.*, multi-factor authentication and monitoring). It should be clarified that the requirements apply only to electronic information.

B. AFSA recommends several changes to the Proposed Rule.

Our recommendations are outlined by section below.

Section 314.4(c)(2)—This requires financial institutions to identify and manage the data, personnel, devices, systems, and facilities that enable an institution to achieve business purposes in accordance with their relative importance to business objectives and risk strategy. AFSA recommends that this section be removed because it is not clear what the management standard would be.

Section 314.4(c)(4)—This requires that all customer information held or transmitted, both in transit over external networks and at rest, be encrypted. Currently, financial institutions encrypt sensitive information in transit over external networks. Also, it should be necessary to encrypt only sensitive information. There is no reason to encrypt all information.

The FFIEC Cybersecurity Assessment Tool, which is based on the FFIEC Information Technology Examination Handbook (IT Handbook) and the NIST Cybersecurity Framework, as well as industry accepted information security practices, does not require encryption of data at rest, other than passwords. It suggests that only financial institutions with a higher risk profile that triggers the most burdensome advanced information security maturity level determine if encryption of data at rest is justified.

Section 314.4(c)(6)—This requires financial institutions to implement multi-factor authentication for any individual accessing customer information. As noted above, this section should be limited to sensitive information for the convenience of the customer. Customer convenience needs to carefully be weighed against the value of safeguarding all information. Furthermore, while many large financial institutions already require multi-factor authentication for customers, smaller ones do not. Multi-factor authentication is an unnecessary safeguard for smaller institutions and so this requirement should be limited to larger institutions.

In addition, this section should be limited to individuals accessing the financial institution's internal networks from an external network. It would be unnecessary and costly to require multi-factor authentication for individuals

accessing an internal network from an internal network (*i.e.*, multi-factor authentication should not be required for a financial institution's employees to access its own internal networks from an internal network, but should be required to access the financial institution's internal networks from an external network).

Section 314.4(c)(7)—This requires financial institutions to include audit trails within an information security program designed to detect and respond to security events. It is crucial that this requirement either be removed or appropriately tailored. The cost to maintain audit trails on all parts of a business over many years would be enormous and would not add particular value to the information security program.

Audit trails should be maintained in accordance with a financial institution's risk assessments. AFSA suggests that the FTC limit the size and scope of the requirement. For example, audit trails should not be required to be kept for more than one year. The Cybersecurity Regulations data retention period has resulted in an exponential increase in data retention, with a significant implementation burden and no material improvement to information security. It would require costly modifications to institutions' legacy systems, which are not designed to record information relating to every financial transaction. We suggest that the FTC only require preservation of data that the institution itself decides needs to be maintained in order to fulfill auditing needs. In addition, this requirement should not be imposed on smaller institutions.

Section 314.4(c)(8)—This requires financial institutions to develop, implement, and maintain procedures for the secure disposal of customer information in any format that is no longer necessary for business operations or for other legitimate business purposes. This requirement exceeds federal banking standards. The FFIEC Cybersecurity Assessment Tool does not require destruction of customer information once it is no longer necessary for business operations or for other legitimate business purposes. It requires only that financial institutions have "data is disposed of or destroyed according to documented requirements and within expected time frames." Requiring targeted disposal will be technically infeasible in many circumstances due to the manner in which information is maintained within individual systems, particularly legacy systems and those where data is commingled. Data stored on magnetic tapes and commingled data on servers presents significant feasibility challenges with respect to any requirement for data destruction. Accordingly, we ask that this requirement be revised to recognize that financial institutions may retain data pursuant to the records retention policy of the business or where disposal is not reasonably feasible. In addition, this requirement should not apply to non-sensitive information.

Section 314.4(c)(10)—This requires financial institutions to implement policies, procedures, and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users. This section should apply only to information stored electronically. It would be impossible to monitor the activity of users accessing paper files.

Section 314.4(d)(1)—This requires financial institutions to regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems. Because it would be impossible, and because it is not as vulnerable to theft, this requirement should not apply to paper files, but should apply instead only electronic data.

Section 314.4(e)—This requires financial institutions to implement appropriate training and education, including verifying that personnel take steps to maintain current information security knowledge and use qualified security personnel. The FTC should acknowledge that meeting these requirements will look very different for a small financial institution than a large, multi-national one.

Section 314.4(f)—This expands the requirement to oversee service providers to require financial institutions to periodically assess such service providers based on the information security risk they present. The FTC needs to better define which service providers need to be overseen. For example, under the current definition, the three large credit bureaus could be defined as service providers, but of course a small financial institution could not assess the security risk one of the bureaus presents. AFSA suggests that if a service provider is directly supervised by a federal financial regulator, it be exempt from being overseen by this requirement.

C. The FTC should delay the effective date.

The Proposed Rule puts forward an effective date of six months after publication of the final rule. While this may be possible for larger institutions who are already complying with the Cybersecurity Regulations, it is inconceivable for smaller institutions. Those institutions would have to: employ or designate and train a chief information security officer, encrypt all customer information, implement multi-factor authentication, set up audit trails, redo disposal procedures, etc. within half a year.

During this timeframe, financial institutions are also coming into compliance with other standards, such as the California Consumer Privacy Act and the Nevada internet privacy law.

We respectfully request that the FTC provide an implementation period of two years. There were a number of problems that financial institutions faced complying with the Cybersecurity Regulations. The FTC could prevent, or at least reduce, these implementation issues with a longer timeframe in which to comply.

VII. Conclusion.

AFSA understands that the FTC has issued the Proposed Rule in an attempt to provide more detailed guidance as to what an appropriate information security program entails, while still giving companies with flexibility. AFSA suggests that that the FTC can better achieve that balance with some modifications to the Proposed Rule. Perhaps most importantly, the FTC should include a safe harbor in the Rule for compliance with certain data security standards. Additionally, the FTC should exempt financial institutions from the Rule if they serve less than 50,000 customers. We also believe that the FTC should modify the proposed rule so that it strikes a better balance between providing guidance to financial institutions and preserving flexibility to address threats. And lastly, we believe that such a strong, federal standard should preempt a potential myriad of state laws.

If you have any questions, please do not hesitate to contact me by phone at 202-776-7300 or e-mail at cwinslow@afsamail.org.

Sincerely,

Celia Winslow
Vice President, Legal & Regulatory Affairs
American Financial Services Association