

November 21, 2016

Federal Trade Commission  
Office of the Secretary  
Constitution Center  
400 7th Street SW, 5th Floor  
Suite 5610 (Annex B)  
Washington, DC 20024

**Re: *Safeguards Rule, 16 CFR 314, Project No. P145407***

To whom it may concern:

The American Financial Services Association (“AFSA”)<sup>1</sup> appreciates the opportunity to comment on the Federal Trade Commission’s (“FTC”) Standards for Safeguarding Customer Information (the “Safeguards Rule” or “Rule”). AFSA urges the FTC to keep the flexible guidelines in the current Rule in place. Where appropriate, AFSA encourages the FTC to provide a safe harbor.

Many AFSA members are federally-chartered banks or thrifts. As such, they already have extensive cybersecurity examinations from either the Office of the Comptroller of the Currency or the Federal Reserve. The FTC’s Safeguards Rule and similar rules by the banking agencies are the basis for almost all credit cybersecurity requirements in the United States. These requirements should continue to be flexible and consistent. Complying with inconsistent federal information security rules will be wasteful and will divert resources away from genuine risk based information security improvements.

The Safeguards Rule should continue to establish reasonable standards that allow each financial institution the discretion to design an information security program that suits its particular size and complexity and the nature and scope of its activities, and to allow financial institutions to adapt to a changing environment more quickly than regulations, which may become dated. They should not include fixed prescriptive standards and should not impose standards that go beyond those required by the banking agency guidelines and Federal Financial Institutions Examination Council (“FFIEC”) handbooks and guidance.

In fact, it would be appropriate to reference the FFIEC’s Cybersecurity Assessment Tool<sup>2</sup> in the Safeguards Rule. It could also bring clarity to the Rule by including references to other information security standards or frameworks in the Rule. Suggested reasonable security standards or frameworks include: the National Institute of Standards and Technology’s Cybersecurity Framework, the International Organization for Standardization 27001 or 27002, COBIT, or the SANS Institute Top 20 Critical Security Controls. To be clear, these could be included in the Safeguards Rule as reasonable suggestions. They should not be mandatory requirements.

---

<sup>1</sup> 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.

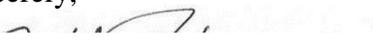
<sup>2</sup> Available at <https://www.ffiec.gov/cyberassessmenttool.htm>.

These standards/frameworks could be included in the Rule as a safe harbor. Under the current Safeguards Rule, a lender's cybersecurity is deemed adequate if the lender "protects against any anticipated threats or hazards to the security or integrity of such information." While AFSA applauds the flexibility in the standards, we are concerned about the amount of subjectivity. AFSA suggests that to keep the flexibility, but lessen the subjectivity, the FTC deem compliance with any of the standards/frameworks listed in the preceding paragraph as a safe harbor.

If after its review of the comments received, the FTC decides to make changes to the Safeguards Rule, we urge the FTC to consider preempting state laws. This is important as states look more closely at implementing cybersecurity laws and regulations. Fifty different state cybersecurity laws or regulations – possibly with wide variations – would likely cause compliance problems. Just as complying with inconsistent federal information security rules would be wasteful and would divert resources away from genuine risk-based information security improvements, complying with a multitude of different state laws or regulations would also be wasteful and would harm customers by diverting resources away from genuine risk-based information security policies. In trying to meet all of the varying requirements, financial institutions could end up with policies that meet the different requirements, but not be ideal for safeguarding customer information.

AFSA thanks the FTC for the opportunity to comment. Please feel free to contact me with any questions at 202-466-8616 or [bhimpler@afsamail.org](mailto:bhimpler@afsamail.org).

Sincerely,

  
/Bill Himpler  
Executive Vice President  
American Financial Services Association