



November 7, 2016

Via Electronic Entry @ <https://ftcpublishcommentworks.com/ftc/safeguardsrulenprm>

Donald S. Clark  
Secretary  
Federal Trade Commission  
600 Pennsylvania Avenue NW  
Suite CC-5610 (Annex B)  
Washington, DC 20580

**Re: SIFMA Comment to FTC Proposed Amendments to Safeguards Rule, 16 CFR 314, Project No. P145407**

Dear Mr. Clark:

The Securities Industry and Financial Markets Association (*SIFMA*)<sup>1</sup> appreciates the opportunity to respond to the request for comment by the Federal Trade Commission (*FTC*) in the above-referenced Notice of Proposed Rulemaking and Request for Public Comments (*Notice*) regarding *Standards for Safeguarding Customer Information*, 16 CFR 314, Project No. P145407 (*Safeguards Rule Proposed Amendments*).

## **I. EXECUTIVE SUMMARY**

SIFMA historically has supported regulatory efforts designed to safeguard customer information. In May 2002, the FTC promulgated Standards for Safeguarding Customer Information Safeguards Rule, 16 CFR Part 314 (*Safeguards Rule*),<sup>2</sup> pursuant to section 501(b) of the Gramm-Leach-Bliley Act (*G-L-B Act*), which required that the FTC and other federal agencies establish

---

<sup>1</sup> SIFMA is the voice of the U.S. securities industry, representing the broker-dealers, banks and asset managers whose 889,000 employees provide access to the capital markets, raising over \$2.4 trillion for businesses and municipalities in the U.S., serving clients with over \$16 trillion in assets and managing more than \$62 trillion in assets for individual and institutional clients including mutual funds and retirement plans. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit <http://www.sifma.org>.

<sup>2</sup> See 67 FR 36483 (May 23, 2002).

standards for financial institutions relating to administrative, technical, and physical safeguards for certain information.

SIFMA supports the FTC's efforts to (i) ensure the security and confidentiality of customer records and information, (ii) protect against any anticipated threats or hazards to the security or integrity of such records, (iii) and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer. We believe that the Safeguards Rule in its current form accomplishes the intended purpose.

In addition to raising general issues regarding the Safeguards Rule's benefits and costliness, the above-referenced Notice specifically seeks comment on whether the Safeguards Rule should require information security systems to be enhanced, whether the Safeguards Rule should include more specific and prescriptive requirements, whether the Safeguards Rule should incorporate other industries' standards, and whether the Safeguards Rule's definitions should be changed.

Without detracting from the support stated herein, SIFMA submits comments on the Safeguards Rule Proposed Amendments to highlight why we find the proposed modifications unnecessary.

## II. COMMENTS

Our comments recognize that the FTC's authority to promulgate and amend the Safeguards Rule flows solely from Title V, Subtitle A of the G-L-B Act. Section 504(a)(7) of the G-L-B Act grants the FTC authority to regulate "any other financial institution or other person that is not subject to the jurisdiction of any agency or authority under the section's preceding paragraphs."<sup>3</sup>

### A. *The elements of an information security program need not include a response plan*

The Notice requests comment on whether the elements of an information security program should "include a response plan in the event of a breach that affects the security, integrity, or confidentiality of customer information."

While we avow that breach monitoring is essential in the financial industry, we do not believe that a breach monitoring program should have to exist in a separate "information security program." Our member firms already have breach monitoring programs in place, operating in various departments in their organizations, *e.g.*, Legal, Information Technology, and Compliance. Because companies are already allocating resources toward breach monitoring, it would be burdensome to require companies to eschew their existing practices to accommodate a logistical requirement about where breach monitoring programs must exist.

---

<sup>3</sup> Section 504(a)'s preceding paragraphs accounted for entities governed by the following statutes, under which the FTC may not regulate: (1) Federal Depository Insurance Act; (2) Federal Credit Union Act; (3) Securities Exchange Act of 1934; (4) Investment Company Act of 1940; (5) Investment Advisers Act of 1940; (6) State insurance laws.

Additionally, many states already implicitly require our industry to have effective breach monitoring operations in place. For example, Massachusetts requires all persons who own or license personal information about a Massachusetts resident to document “responsive actions taken in connection with any incident involving a breach of security,” and also requires “regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access or unauthorized use of personal information.” Each state requires our industry, at a minimum, to respond to breaches of personal information. Thus, the proposed modification to the Rule is redundant in light of existing state regulations.

*B. The Safeguards Rule should not include more specific and prescriptive requirements for information security plans*

The Notice requests comment on whether the Rule should “be modified to include more specific and prescriptive requirements for information security plans.”

We believe that this proposed modification is unnecessary, overly burdensome, and potentially harmful. When the FTC pioneered the original Rule, it was the first of its kind to both provide clear guidelines while also allowing our industry flexibility to implement risk-based safeguards. More specific requirements in the Rule would eliminate flexibility and harm both large and small companies. Small companies would be unduly burdened by the requirements, and large companies would have to redirect resources that could be better used for other regulatory compliance efforts.

*C. The Safeguards Rule should not be modified to reference or incorporate any other information security standards or frameworks*

The Notice requests comment on whether the Rule “should be modified to reference or incorporate any other information security standards or frameworks, such as the National Institute of Standards and Technology’s Cybersecurity Framework or the Payment Card Industry Data Security Standards.”

We do not believe that this modification is necessary, especially for the Payment Card Industry Standards. The securities industry and the payment card industry are two separate and wholly distinct entities. Further, there is no indication that our cybersecurity needs substantially overlap with the payment card industry in a way that would justify basing the Rule on a different industry’s standards. We also do not believe that reference to or incorporation of the NIST framework is necessary. The NIST framework, as well as other common security standards, already informs the industry as to what is reasonable with respect to safeguarding data.

*D. The Safeguard Rule’s existing definitions should not be altered*

The Notice requests comment on whether “the Rule should be modified to include its own definitions of terms, such as ‘financial institution,’ rather than incorporating the definitions found in the Privacy Act.” In addition, the Notice requests comment on whether the Rule’s definition of

Mr. Donald S. Clark  
Federal Trade Commission  
November 7, 2016  
Page 4

“financial institution” should “be modified to also include entities that are significantly engaged in activities that the Federal Reserve Board has found to be incidental to financial activities,” or “activities that have been found to be closely related to banking or incidental to financial activities by regulation or order in effect after the G-L-B Act.”

We are not in favor of altering the existing Rule’s definitions. The Rule already requires all safeguards to be “reasonable.” This reasonableness standard is elastic enough to encompass all companies to the extent that they are involved in the same activities as our industry. In satisfying this reasonableness standard, our industry regularly makes proactive efforts to become familiar with other regulatory frameworks’ definitions. Thus, the Rule already implicitly requires our industry to understand the Privacy Act, Federal Reserve Board guidance, and the G-L-B Act’s impact. Creating new, or modifying existing, definitions in the Rule would eliminate the Rule’s flexibility in this regard. We support the existing Rule and the incorporated definitions therein.

### III. CONCLUSION

SIFMA appreciates this opportunity to comment on the Proposed Rules. We reiterate our support for regulatory efforts to protect customer records and information is extremely important for financial institutions and we appreciate the FTC’s efforts to obtain public comment on potential modifications to the Safeguards Rule. We would be pleased to discuss any of these points further, and to provide additional information you believe would be helpful. If you have any questions or require further information, please contact me at (202) 962-7385 or [mmacgregor@sifma.org](mailto:mmacgregor@sifma.org).

Very truly yours,

/Melissa MacGregor/

Melissa MacGregor  
*Managing Director &  
Associate General Counsel*

cc: David Lincicum, *Division of Privacy and Identity Protection, Bureau of Consumer Protection, FTC*  
Katherine McCarron, *Division of Privacy and Identity Protection, Bureau of Consumer Protection, FTC*  
Marlon Q. Paz, *Seward & Kissel LLP*