



1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

November 7, 2016

Via electronic submission to <https://ftcpublishcommentworks.com/ftc/safeguardsrulenprm>

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

Re: Safeguards Rule, 16 CFR 314, Matter No. P145407

Dear Secretary Clark:

The Electronic Transactions Association (“ETA”)¹ appreciates this opportunity to provide comments regarding the Federal Trade Commission’s (“FTC” or “Commission”) Request for Public Comment on its Standards for Safeguarding Customer Information (“Safeguards Rule” or “Rule”).² ETA supports maintaining the Safeguards Rule as it currently stands, and recommends the FTC not change any definitions.

ETA is the leading trade association for the payments industry, representing nearly 550 companies worldwide involved in electronic transaction processing products and services. The purpose of ETA is to influence, monitor, and shape the payments industry by providing leadership through education, advocacy, and the exchange of information. ETA’s membership spans the breadth of the payments industry, and includes financial institutions, payment processors, independent sales organizations, and equipment suppliers. ETA’s members use data to provide a wide range of products and services designed to enhance and secure electronic transfers. Our members rely on data to help reduce fraud and to authenticate transactions to make transactions between businesses and consumers seamless and secure.

The Commission’s review seeks information about the costs and benefits of the Safeguards Rule and its regulatory and economic impact for the purpose of assisting the Commission in identifying elements that may warrant modification or rescission. More specifically, the Commission has solicited comments on what modifications to the Rule are needed (if any) to increase consumer benefits, reduce costs, or account for changes in relevant technology or economic conditions.

The Safeguards Rule is Effective As Is

ETA’s position is that the Safeguards Rule as currently written effectively promotes customer information security as applied to the financial services sector. Since taking effect in 2003, the

¹ <http://www.electran.org/>.

² Federal Trade Commission, 81 Fed. Reg. 61632 (September 7, 2016).

information security requirements imposed by the Safeguards Rule have been held up as a model set of elements for developing an information security program. These elements have served as a foundation upon which financial institutions and services companies have built leading cybersecurity programs, leveraging the inherent flexibility of the Rule to tailor information security practices and protocols that meet their unique business models, data use practices, and network environments.

Prescriptive Requirements Limit Flexibility and Innovation

As set forth in the Federal Register notice, the Commission asks whether the Rule should be “modified to include more specific and prescriptive requirements for information security plans?”³ In response, ETA cautions that additional prescriptive requirements would limit the flexibility currently built into the Rule; the current definitions are comprehensive enough and changing them could create a burdensome regime without any recognizable harm that warrants a change.

Prescriptive requirements would limit the ability of industry to develop new and innovative approaches to information security. The security best practices developed and implemented by the financial sector to date are the product of innovation and the deployment of new security technologies to protect financial information. As technology and innovation continue to shape how financial products are created and how these products are delivered and employed by customers, regulation in this space must remain adaptable and should not impose rigid rules that have the effect of unnecessarily restraining innovation. Further, regulation that adopts a checklist approach risks complacency among companies. Allowing companies to develop the specific mechanisms to anticipate new threats and thwart attacks is the better approach to achieve the common goal of securing consumer financial information.

Self-Regulation Works

In the electronic transactions industry, financial information data is governed by federal law, including the Gramm-Leach-Bliley Act, while other data and its uses are governed by robust self-regulatory programs, including the Payment Card Industry Data Security Standard (“PCI-DSS”), which sets forth requirements designed to ensure companies that process, store, or transmit credit card information maintain a secure environment for such data. Through a calibrated mixture of federal law and industry codes, policymakers have recognized that for certain data and uses, prescriptive federal laws could burden commerce and innovation. In these areas, industry has been encouraged to self-regulate to keep pace with the fast moving payments space.

To keep pace with consumer demand for better, faster, and more secure payment options, the payments industry has responded by developing a number of innovative solutions. For example, the payment card industry recently migrated to EMV or “chip” technology, which provides enhanced security to consumers while continuing to foster a payment system that facilitates seamless and timely electronic transactions. EMV and other measures, such as PIN and

³ 81 Fed. Reg. at 61635.

tokenization, are effective methods for safeguarding customer information, while enabling responsible and productive uses of data.

Given how quickly technology evolves in today's market, self-regulation is the appropriate tool through which prescriptive requirements, beyond those already included in the Safeguards Rule, could be developed as appropriate. Self-regulation allows for on-going review and modification to reflect an ever changing marketplace. By its very nature, the regulatory system is not designed for the constant evolution taking place today. Accordingly, ETA supports maintaining the existing information security requirements of the Safeguards Rule as is, and believes that any additional "specific or prescriptive requirements" are best addressed through established self-regulation.

Specific Question Addressed

B.3 Should the Rule 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?

ETA Response

The FTC should not incorporate any other information security standards or frameworks into the Safeguards Rule. Particularly, neither the Payment Card Industry Data Security Standards ("PCI DSS") nor the National Institute of Standards and Technology's Cybersecurity Framework (the "Framework") should be incorporated or referenced in the Safeguards Rule.

We note that PCI DSS are an essential part of securing the payments ecosystem, which is why card networks mandate compliance with PCI DSS for participants in their networks. PCI DSS, however, is enforced as a matter of private contract and should not be repurposed as a regulatory standard. In addition, PCI DSS are unique in that they were developed by the major card networks and apply specifically to participants in the card industry. Whereas the PCI DSS may be appropriate for payment card issuers and acquirers, for example, they would not necessarily apply to all financial institutions subject to the FTC's Safeguards Rule.

The Framework was designed to apply more generally to "critical infrastructure" but also on a voluntary basis to help organizations manage cybersecurity risk. The Framework is not designed to replace an organization's cybersecurity risk management. Rather, an organization may use the Framework as part of its systematic process of identifying, assessing and managing cybersecurity risk. Even the FTC staff has stated that the Framework "is not, and isn't intended to be, a standard or checklist" and that "there's really no such thing as 'complying with the Framework.'"

We believe that the FTC should continue to recognize that the Framework is not a binding set of obligations upon organizations. Indeed, the Framework is intended primarily to assist critical infrastructure participants. While the Department of Homeland Security has designated the financial services sector as a critical infrastructure sector, the Framework would surely not apply to all financial institutions over which the FTC has authority. While the Framework may represent a risk-based approach to managing cybersecurity, any reference in the Safeguards Rule to the Framework or to any other information security standards could suggest mandatory compliance.



1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

This is inconsistent with the purposes for which the Framework was developed and how it has been treated by industry. Therefore, we encourage the FTC not to incorporate or reference any information security standards or frameworks in the Safeguards Rule.

* * *

ETA thanks you for the opportunity to submit these comments.

Respectfully submitted,

Scott Talbott
Senior Vice President of Government Affairs
Electronic Transactions Association