ELECTRONIC TRANSACTIONS ASSOCIATION

1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

August 2, 2019

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

Re: Safeguards Rule, 16 CFR part 314, Project No. 145407

Dear Commissioners:

The Electronic Transactions Association ("ETA") appreciates the opportunity to provide comments on behalf of the payments and FinTech industry for the Federal Trade Commission's Notice of Proposed Rulemaking and Request for Public Comment on its Standards for Safeguarding Customer Information ("Safeguards Rule").

ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services. ETA's members include financial institutions, mobile payment service providers, mobile wallet providers, and non-bank online lenders that make commercial loans, primarily to small businesses, either directly or in partnership with other lenders. ETA member companies are creating innovative offerings in financial services, revolutionizing the way commerce is conducted with safe, convenient, and rewarding payment solutions and lending alternatives.

The Safeguards Rule is Effective

The Safeguards Rule as currently written effectively promotes customer information security as applied to the financial services sector. Since taking effect in 2003, the 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

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. To the extent the Commission proceeds with amending the Safeguards Rule, we provide specific comments below.

Additional Comments

Sensitive Customer Information

Under the proposed changes, ETA has concerns about the scope of what constitutes customer information. The mandates for encryption at rest for customer information with such a broad scope would mean that even data such as someone's name would need to be encrypted at rest. This is an extremely burdensome requirement that does not reflect the risk-based approach of the Safeguards Rule. To that end, ETA recommends a few amendments to the proposed rule to ensure that "sensitive customer information," as opposed to all customer information, is subject to increased requirements for security, which would harmonize a concept presently required as part of New York's cybersecurity regulations.

Recommended language is in bold and underlined.

314.2 Definitions

(k) "Sensitive customer information" means non-public electronic customer information which because of name, number, personal mark, or other identifier can be used to identify such customer, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records.

(~~K~~**L**) *Service provider* means (…)

314.4 Elements
(…)
(c) Design and implement safeguards to control the risks you ***identify*** *through risk assessment, and including:*

> *(1) Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals* ***designed*** *to protect against the unauthorized acquisition of customer information and to periodically review such access controls;*

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;

(3) Restrict access at physical locations containing customer information only to authorized individuals;

*(4) Protect by encryption all **sensitive** customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of **sensitive** customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such **sensitive** customer information using effective alternative compensating controls reviewed and approved by your CISO;*

*(5) Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing **sensitive** customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store **sensitive** customer information;*

*(6) **Implement multi-factor authentication for any individual accessing sensitive customer information on your internal network when connecting from an external network. In addition, based on the risk assessments performed under paragraph (b)(2) of the section, implement multi-factor authentication to protect against unauthorized access to sensitive customer information, unless your CISO has approved in writing the use of alternative compensating controls**;*[1]

(7) Include audit trails within the information security program designed to detect and respond to security events:

(8) 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, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained;

(9) Adopt procedures for change management; and

*(10) Implement policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, **sensitive** customer information by such users.*

[1] We recommend this language, rather than the language in the proposed rule, because multi-factor authentication would not be necessary for access through an internal network, as other safeguards would be in place. In addition, our proposed language would track the CISO-related reference that is in the proposal rule as it relates to encryption. The same requirement – "alternative compensating controls" approved by the CISO should be both in the encryption requirement and the multi-factor authentication requirement.

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

(…)

*(h) Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of **sensitive** customer information in your possession. Such incident response plan shall address the following (…)*

Multi-Factor Authentication

Increasingly cybersecurity best practices, including the safeguards rule, are calling for multi-factor authentication as a means for identity verification and increased security. It is important to include flexibility and choice for customers to verify their authentication through means they use regularly without providing additional prescriptive requirements. One way of doing that is to allow for one of the factors of authentication to be done through text message on a mobile phone. ETA recommends the following amendment language below to add that option.

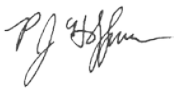
Recommended language is in bold and underlined.

314.2 Definitions
(…)
(i) (i) Multi-factor authentication means authentication through verification of at least two of the following types of authentication factors:
(1) Knowledge factors, such as a password;
*(2) Possession factors, such as a token; or **text message on a mobile phone or***
(3) Inherence factors, such as biometric characteristics.

* * *

We appreciate you taking the time to consider these important issues. If you have any questions or wish to discuss any issues, please contact me or ETA Senior Vice President, Scott Talbott at Stalbott@electran.org.

Respectfully submitted,



PJ Hoffman,
Director of Regulatory Affairs
Electronic Transactions Association
(202) 677-7417
PJHoffman@electran.org