PUBLIC SUBMISSION

Comment Submitted by Electronic Transactions Association

Posted by the **Federal Trade Commission** on Feb 7, 2022

View More Comments 21 (/document/FTC-2021-0071-0001/comment)

View Related Comments 21 (/docket/FTC-2021-0071/comments)

Share

Comment

See attached file(s)

Attachments 1

ETA Comment Letter - Standards for Safeguarding Customer Information - 2.7.22

Download (https://downloads.regulations.gov/FTC-2021-0071-0017/attachment_1.pdf)

Comment ID

FTC-2021-0071-0017

Tracking Number

kzd-734z-esmb

Comment Details **Submitter Info**

Received Date

Feb 7, 2022

Your Voice in Federal Decision Making

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

February 7, 2022

Via eRulemaking Portal

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

Re: Comments Regarding Amending the Safeguards Rule – Safeguards Rule, 16 CFR part 314, Project No. P145407

Dear Commissioners:

On behalf of the Electronic Transactions Association (ETA), we appreciate the opportunity to provide comments on behalf of the payments and fintech industry for the Federal Trade Commission's (FTC) request for public comment on its proposal to further amend the Standards for Safeguarding Customer Information (Safeguards Rule).

Who We Are

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 banks, mobile payment service providers, mobile wallet providers, money transmitters and non-bank financial technology companies ("FinTech") that provide access to credit, 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 – facilitating over $22 trillion in payments in 2019 worldwide.

Comments

<u>The Safeguards Rule is Effective</u>
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.

<u>Prescriptive Requirements Limit Flexibility and Innovation</u>
ETA encourages the FTC to focus on a regulatory framework that ensures a positive regulatory environment - encouraging growth and innovation governed by common principles but tailored

appropriately to a company's particular risk profile. Additionally, as companies increasingly offer a wide variety of products and services to reach a broad spectrum of consumers and businesses, we encourage an intentional effort toward regulatory harmony. ETA encourages the FTC to clarify that non-banking financial institutions subject to FTC oversight but subsidiaries of a prudentially regulated companies and who are already subject to the info security requirements of another federal regulator are not subject to the FTC's Safeguards Rule and incident reporting requirement.

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.
If there is a new reporting requirement to be issued, ETA suggests it be through a flexible principles-based framework and it should probably be strictly limited to incidents that only: i) Involve Personal Identifiable Information; ii) Involve only actual loss or unauthorized access; iii) It is reasonably likely to cause substantial harm to the individuals to whom the information relates; iv) The breach must be a "confirmed" breach and not a "threatened" breach; and v) Involve a "compromise" of PII meaning exposure to third parties and more than mere unauthorized access. This would reduce the number of notices that do not result in actual harm should not give rise to a notification incident given the stated objectives of the proposed rule. The inclusion of these less significant occurrences would place unnecessary burden on bank service providers and financial institutions and the unintended result would be over-reporting to the FTC.

We advise that any new standards that may be issued, strike the proper balance between regulatory and market needs, by continuing to enable innovation, promoting consumer protection, and strengthening competition through a flexible principles-based framework, and not prescriptive programs. Technology is ever evolving, and any guidelines may become obsolete prior to their implementation. A flexible, principal-based approach provides a common framework is more sustainable in that it adjusts to changes in the market and technology, which allows any new guidelines to be tailored based to the risk profile of the participant. This strikes the necessary balance among principles of safety and soundness, consumer protection, innovation and promoting competition.

A principle framework also recognizes the payments industry's long history of meaningful self-regulation including, for example, developing innovative solutions to ensure privacy and security in transactions and encourages a collaborative approach that relies on existing standards. In addition to the legal framework outlined above, the payments industry has implemented robust and sophisticated self-regulatory programs to further protect the integrity of the payments ecosystem and the consumers and businesses that rely on it with every transaction.

Likewise, the payments industry has a long history of fighting fraud through robust underwriting and monitoring policies and procedures. Working with its members and industry and government stakeholders, ETA has published various guidelines that provide underwriting and diligence best practices for merchant and risk underwriting, including the "Guidelines on Merchant and ISO Underwriting and Risk Monitoring" and "Payment Facilitator Guidelines." These documents

provide industry with underwriting and diligence guidance, including information on anti-fraud tools, security, and related issues.

Standardizing Reporting Format

ETA members appreciate the importance of early detection of significant security incidents and support the goal of ensuring early detection of emerging threats to individual banking organizations and the broader financial system.

In addition, to eliminate the burden of over-reporting that fall below the reporting threshold after appropriate review or investigation is performed, we believe it is critical that bank service providers and financial institutions understand that they can conduct such review or investigation, consistent with the proposed rule's reporting requirements, before determining that a notification incident has occurred.

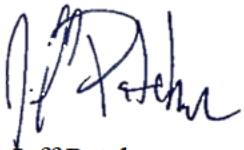
We believe that simplicity of the notification is critical to the effectiveness of the Amended Rule, and that requiring any specific information or assessment would result in a complex, uncertain, and burdensome process at a sensitive time. Additionally, any requirements for information that need to be included in the notification should be standardized, pre-defined, and clearly identified to help ensure bank service providers and financial institutions are communicating the expected information, if available, in order to minimize repeated follow-up questions from the FTC.

We also welcome further discussion about how the FTC intend to share and secure any information provided by an organization in connection with an incident, an issue of critical importance to our members. For example, will or under what circumstances the FTC shares the information with other authorities and Agencies while ensuring the reporting data is safe and secure.

* * *

ETA appreciates the opportunity to provide input on this important issue. If you have any questions, please contact me or ETA's Senior Vice President of Government Affairs, Scott Talbott at stalbott@electran.org.

Sincerely,



Jeff Patchen
Manager of Government Affairs
Electronic Transactions Association
jpatchen@electran.org
(202) 677-7418