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

November 3, 2021

The Honorable Ed Perlmutter
Chairman, Subcommittee on Consumer Protection and Financial Institutions
Committee on Financial Services
House of Representatives
Washington, DC 20515

The Honorable Blaine Luetkemeyer
Ranking Member, Subcommittee on Consumer Protection and Financial Institutions
Committee on Financial Services
House of Representatives
Washington, DC 20515

Dear Chairman Perlmutter and Ranking Member Luetkemeyer:

On behalf of the members of the Electronic Transactions Association (ETA), we appreciate the opportunity to submit this statement for the record before the Subcommittee's hearing, "Cyber Threats, Consumer Data, and the Financial System."

The Electronic Transactions Association (ETA) is the world's leading advocacy and trade association for the payments industry. Our members span the breadth of significant payments and fintech companies, from the largest incumbent players to the emerging disruptors in the U.S and in more than a dozen countries around the world. ETA members make commerce possible by processing approximately $22.5 trillion annually in purchases worldwide and deploying payments innovation to merchants and consumers.

ETA and its members are dedicated to working with federal and state regulators to address the important and growing issue of cybersecurity. The prevailing cybersecurity best practices developed and implemented in the financial and payments industries are the product of innovation and cooperation between industry and government. ETA strongly encourages policymakers to be sensitive to the risk of applying a prescriptive regulatory framework that undermine the federal and self-regulatory efforts that have made in combatting cybersecurity threats in the financial industry.

To the extent additional cybersecurity requirements are necessary, ETA supports an industry-led and principles-based framework that promotes innovation and competition among all industry participants in the financial data marketplace that provides industry with flexibility to keep pace with innovation in cybersecurity technology and emerging cyber threats.

ETA Supports a Flexible Uniform National Standard for Cybersecurity
ETA believes that a flexible uniform national framework is the most effective approach for addressing cybersecurity risks. In the electronic transactions industry, financial information data is governed by federal law, including the Gramm-Leach-Bliley Act (GLBA), the Federal Trade Commission's Safeguards Rule, and 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.

Since taking effect in 2003, for example, the information security requirements imposed by the Safeguards Rule have been held up as a model set of elements for developing an information

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

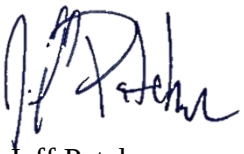
security program. These elements have served as a foundation upon which financial institutions and services companies have built leading cybersecurity programs, leveraging the inherent flexibility of the Safeguards Rule to tailor information security practices and protocols that meet their unique business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

The existing framework of state laws undermines the effectiveness of a federal and self-regulatory framework. The development of separate state regimes not only increases the compliance burden of regulated entities, but also will undermine federal efforts to develop additional national best practices and standards for cybersecurity. If states continue to develop their own cybersecurity regimes, the focus of cybersecurity in the private sector will shift from developing new and innovative best practices to managing and complying with overlapping, or worse, conflicting, state and federal requirements.

For example, in January 2021, the prudential financial regulators proposed a rule relating to computer-security incident notification requirements for banking organizations and their bank service providers.[1] Additionally, Incident Reporting legislation pending in Congress, and when harmonized with the requirements of Section 2 of President *Biden's Executive Order on Improving the Nation's Cybersecurity*[2], have the potential to improve the nation's cybersecurity posture if appropriately developed and implemented. These efforts to streamline reporting requirements would ensure resources are used to combat malicious cyber threat activity, rather than customizing reports for various states.

We appreciate the opportunity to submit this letter for the record and the Subcommittee's leadership on this topic. 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
Senior Manager of Government Affairs
Electronic Transactions Association

[1] https://www.regulations.gov/document/OCC-2020-0038-0001
[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/