ELECTRONIC TRANSACTIONS ASSOCIATION

1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

March 15, 2019

The Honorable Mike Crapo
Chairman
Committee on Banking, Housing, and Urban Affairs
United States Senate
Washington, DC 20515

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate
Washington, DC 20515

Dear Chairman Crapo and Ranking Member Brown:

On behalf of the Electronic Transactions Association ("ETA"), we appreciate the opportunity to share our thoughts on the collection, use and protection of sensitive information by financial regulators and private companies.

ETA is the leading trade association for the payments industry, representing over 500 payments and FinTech companies that offer electronic transaction processing products and services and commercial loans, primarily to small businesses. During 2018 in North America lone, ETA members processed over $7 trillion in consumer purchases. ETA's members include financial institutions, payment processors, FinTechs, and all other parts of the payments ecosystem.

ETA and its members support U.S. and international efforts to strengthen privacy laws in ways that help industry combat fraud and help consumers understand how their data is being used. As lawmakers and regulators explore additional ways to protect consumers, it is critical that government coordinate with the payments industry to combat fraud and cybercrime so that all consumers have access to safe, convenient, and affordable payment options and other financial services.

ETA understands the importance of protecting consumers, networks and data. ETA members have a long history of developing innovative solutions to ensure privacy and security in transactions and payments. The United States should adopt a national privacy law that protects consumers by expanding their current rights without discouraging competitiveness and innovation.

1) What could be done through legislation, regulation, or by implementing best practices that would give consumers more control over and enhance the protection of consumer financial data, and ensure that consumers are notified of breaches in a timely and consistent manner?

Congress should include risk-based data security and breach notification provisions that protect sensitive personal information pertaining to individuals. Consumers have the right to be notified within a reasonable timeframe if they have been subjected to a personal data breach. ETA understands security is different for individual businesses and an all-encompassing one sized approach is not effective. Companies should have flexibility in implementing reasonable technical and physical security practices.

By providing consumers and businesses with strong, consistent, and predictable protections through a uniform national standard for breach notification, consumers and businesses will benefit. Enacting such a standard will provide certainty and consistency to businesses and consumers alike without having to navigate the patchwork of state laws, which are inconsistent and sometimes contradictory. A federal

standard would also reduce the complexity and costs associated with the compliance and enforcement issues resulting from different laws.

2) What could be done through legislation, regulation, or by implementing best practices to ensure that financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) provide adequate disclosure to citizens and consumers about the information that is being collected about them and for what purposes?

Businesses must promote transparency with their customers and transparency is also important when engaging with regulators or other appropriate authorities. Regulators and government officials should be appropriately transparent about their objectives.

With respect to personal data, consumers should have reasonable access to clear and understandable statements about businesses practices and policies. Businesses should be transparent about: the types of personal data collected, how the personal data will be used, and if personal data may be disclosed and/or shared. Businesses should also provide clear privacy notices to consumers and provide appropriate procedures for individual control, including the opportunity to control data sharing.

Individuals must have a reasonable right access their personal information that they have provided to a company, and where practical, have that information corrected. Individuals should also have the ability to request the deletion of personally identifiable information provided to companies, unless there is a legitimate or legal obligation to maintain that information.

3) What could be done through legislation, regulation, or by implementing best practices to give citizens and consumers control over how financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) use consumer data?

The payment industry has a long commitment and history of fighting fraud. The industry is constantly developing and deploying new technologies to detect, deter, and eliminate fraud. New and enhanced technologies have amplified the payments industry's ability to offer new fraud solutions and strengthen our on-going efforts.

The legal frameworks in Europe and Canada respect the need for industry to share information in order to protect consumers from fraud. In Europe, the recently enacted General Data Protection Regulation (GDPR) recognizes the important role that industry plays in fighting fraud and expressly permits (a) "the processing of personal date strictly necessary for the purposes of preventing fraud," and (b) "decision-making based on profiling that is used for fraud monitoring and prevent consistent with law." In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) allows for the sharing of personal information without consent if it is "made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud. . ."

Credit card companies use technology to fight fraud, by employing automated fraud detection algorithms across massive amounts of data collected from millions of customers and hundreds of millions of cards. Any privacy or data protection standard should include provisions for permissible uses of data to prevent fraud and protect consumers.

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

There are numerous existing privacy-related laws in the U.S. and around the globe that addresses the permissible uses of data which aligns with the payments industry's fraud fighting efforts. In the U.S., for example, 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. All of these laws and self-regulatory efforts recognize the role played by industry, including the need for financial institutions and payments companies to share information as needed to combat fraud.

In the U.S., for example, laws have been passed to protect health information (HIPAA) and financial information (GLBA and Fair Credit Reporting Act), and marketing activities are regulated through federal and state competition laws, as well as industry and activity specific laws, such as the Telephone Consumer Protection Act, Telemarketing Sales Rule, and CAN-SPAM regulations. In almost every case, these laws recognize the important role that industry plays in combatting fraud and provide exceptions or similar provisions that allow for the use and sharing of data to protect consumers or prevent actual or potential fraud from occurring in the first instance.

Under the GLBA, financial institutions must provide customers an initial privacy notice and, for the duration of a customer relationship, an annual privacy notice that describes the company's information-sharing practices. The GLBA also regulates financial institutions' management of nonpublic personal information, which is defined as personally identifiable financial information: 1) provided by a consumer to a financial institution; 2) resulting from any transaction with the consumer or any service performed for the consumer; or 3) otherwise obtained by the financial institution.

With the existence and function of data privacy protections for financial institutions that are already on the books, it is important to continue to allow a permissible use standard for these businesses. Financial institutions have demonstrated the success of GLBA and FCRA to show that the gathering and use of data should not be subject to rules that apply to health information, advertising, or other data.

We appreciate your leadership on this important issue. If you have any questions, please feel free to contact me directly at stalbott@electran.org.

Sincerely,

Scott Talbott
Senior Vice President of Government Affairs
Electronic Transactions Association