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

February 27, 2019

The Honorable Roger Wicker
Chairman
Committee on Commerce, Science, & Transportation
United States Senate
Washington, DC 20515

The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, & Transportation
United States Senate
Washington, DC 20515

Dear Chairman Wicker, Ranking Member Cantwell, and Members of the Committee:

The Electronic Transactions Association ("ETA") appreciates the opportunity to submit this statement for the record for the subcommittee's hearing, "Policy Principles for a Federal Data Privacy Framework in the United States."

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.

From the technology perspective, ETA's members are constantly developing and deploying new technology and tools to detect, deter, and eliminate fraud. Just a few examples of these efforts include the following:

- **Data Encryption.** The payments industry has introduced point-to-point encryption (P2PE) and the tokenization of data to minimize or eliminate the exposure of unencrypted data in connection with a purchase.
- **Improved Authentication.** The use of new authentication methods to verify and authenticate transactions helps minimize potentially fraudulent transactions. These new tools include the use of the following types of advanced tools:
    - biometric authentication, including the use of thumbprints, facial, and voice recognition

  - geolocation that compares the merchant's location with the location of the consumers phone
  - behavioral biometrics (e.g., monitoring keystrokes)
- **Fraud Scoring / Suspicious Activity Monitoring.** The payments industry continues to refine tools for monitoring and analyzing payment data for suspicious activity. With improvements in machine learning and artificial intelligence, payments companies are gaining additional tools for identifying suspicious patterns in transaction data.
- **Chip Cards and EMV**. The payments industry has worked to replace magnetic stripes for credit and debit cards with a computer chip card, also called EMV. Chip cards make our payments system stronger by protecting against theft, counterfeit cards, and unauthorized use of cards in a store.

These are just some of the tools that the payments industry has developed in recent years to fight fraud, protect consumers, and ensure the integrity of the payments ecosystem. These efforts have been remarkably successful in reducing fraud while ensuring that consumers have access to fast, reliable, and safe payment options.

A robust financial system is integral to the economy because it enables the fundamental functions of economic activity, including connecting borrowers with savers, facilitating investments, processing payments, and the safekeeping of financial assets. For the U.S. financial system to remain competitive in the global economy, the United States must continue to prioritize consumer protection, safety, and reliability, while also continuing to lead in innovation.

ETA looks forward to encouraging a collaborative approach and believes a national framework should include the following principles:

- **Data Security and Breach Notification**
  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 a uniform national data breach framework should permit flexibility in implementing reasonable technical and physical security practices.
- **National Standard**
  By providing consumers and businesses with consistent protections through an established national standard for breach notification preemptive of state laws, consumers and businesses will benefit. Enacting a federal preemption will provide certainty and consistency to businesses and consumers alike without having to navigate the patchwork of state laws. A federal preemption would also reduce the complexity and costs associated with the compliance and enforcement issues resulting from different laws.
- **Maximize Transparency**
  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.

- **Access to Data**
  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.
- **Permissible Uses**
  The payment industry has a long commitment and history of fighting fraud. The industry is constantly developing and deploying new technology 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. Any privacy or data protection standard should include provisions for permissible uses of data to prevent fraud and protect consumers.
- **Enforcement**
  To protect consumer rights and provide responsibility, enforcement needs to be consistent and coordinate between the federal government and the state's regulatory body. Congress should encourage collaboration between the appropriate federal agency and state attorney generals to enforce a national consumer privacy law. Strict coordination between the federal agency and state regulatory body should be followed to avoid duplicate or conflicting enforcement actions. Fines and other enforcements actions should be based on the harm directly caused. Other criteria that should be considered but not limited to include: the severity of the data breach, any actions taken by the business to avoid and alleviate the harm, if any negligence was found, and any negative previous history conduct involving business and personal data. However, a federal privacy law should not provide a private right of action for privacy enforcement.
- **Maintaining Flexibility**
  Technology that is involved in data processing evolves rapidly. A baseline law can provide clarity on achieving specific privacy principles, however, laws and regulations should undergo reviews and be flexible. A government should not mandate a specific technological solution or other instrument to implement consumer protections. Including a safe harbor within a federal privacy law would promote the development of adaptable, consumer-friendly privacy programs.
- **Industry and Sector Neutrality**
  A national privacy framework should be applied to all industry sectors that handle consumer data and such protections should be consistent for companies across products and services. It should also be technology neutral and allow organizations to adopt privacy protections that are appropriate to specific risks. Protections shouldn't interfere with innovation and economic competitiveness in an evolving technology landscape.
- **Global Leadership**
  Congress should adopt policies that facilitate international electronic commerce and promote consumer privacy – all which benefit, consumers, economic growth, and trade. Burdensome international regulations hamper the growth of new businesses and creates

conflict of law between jurisdictions. Businesses shouldn't have to worry about foreign regulators because a few people from another country navigate to their website or use their service. Having the United States establish a national privacy framework will facilitate an international data framework and reinforce U.S. leadership worldwide.

The payments industry never rests - working tirelessly to fight fraud and protect consumers, including by developing new tools to prevent or identify fraud through the analyzing data and frequently introducing new fraud fighting solutions. Privacy laws should continue to recognize these goals and the important role the payments industry plays in combatting fraud. By working together, lawmakers, regulators, and industry can protect consumers while providing them with access to the safest and most convenient payments system in the world.

ETA would like to thank the Committee for this opportunity to provide this statement for the record on this important topic. 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