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

March 6, 2019

Chairman Dereck Davis
House Economic Matters Committee
House Office Building #231
Annapolis, MD 21401

RE: ETA Comments – Privacy – H 901

Dear Chairman Davis:

On behalf of the Electronic Transactions Association ("ETA"), we appreciate the opportunity to comment on H 901. The payments industry makes dedicated efforts to use innovation to fight fraud and ensure that consumers have access to safe, convenient, and affordable payment services. ETA and its members strongly support a privacy framework that allow companies to implement innovative tools to protect consumer privacy and data while fighting fraud. While ETA prefers a uniform national approach to privacy rather than a patchwork of disparate state requirements, if policymakers would like to institute a state law in Maryland, ETA requests that any law allow for an explicit exemption for permissible use of data for purposes of fraud prevention and data used under the federal Gramm-Leach-Bliley Act and implementing regulations.

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

Executive Summary

ETA and its members support U.S. and international efforts to strengthen privacy laws to not only help industry combat fraud and but also disclose to consumers 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 so that companies can continue to combat fraud and cybercrime and ensure consumers have access to safe, convenient, and affordable payment options and other financial services.

There are numerous existing consumer protection laws in the U.S. and around the globe that address data security and privacy, and which align with the payments industry's fraud fighting efforts. In the U.S., for example, financial information data is governed by federal laws, including the Gramm-Leach-Bliley Act and related Federal Trade Commission's Safeguards Rule and Consumer Financial Protection Bureau's Privacy Rule, as well as robust self-regulatory programs like the Payment Card Industry Data Security Standard, 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 critical role played by industry in combatting fraud, and they include provisions that allow for the targeted use

and sharing of information by financial institutions and payments companies to protect consumers and to prevent fraud from occurring in the first instance.

Moving forward, ETA encourages policymakers to consider ways that law enforcement and industry stakeholders can continue to work together to develop new ways to combat rapidly evolving and increasingly sophisticated fraud and cybercrime. Working together, lawmakers, regulators, and the payments industry have kept the rate of fraud on payment systems at remarkably low levels. By continuing to collaborate, government and industry can provide consumers with access to safe and reliable payment services. As different states and the federal government consider this important issue, it is important for policymakers to work together across state-lines to provide a consistent privacy framework without creating a patchwork of conflicting regulations.

The Role of the Payments Industry in Fighting Fraud

The payments industry is committed to providing consumers and merchants with a safe, reliable, and modern payments system. Indeed, consumers continue to choose electronic payments over cash and checks because of the protections afforded by electronic payments. These protections include, for example, zero liability for fraudulent charges, making electronic payments the safest and most reliable way to pay.

When it comes to credit cards, for example, a consumer can submit a chargeback request to his or her card issuing bank disputing a particular transaction. This process protects consumers and ensures that the financial institution bears ultimate responsibility for fraudulent transactions, demonstrating the industry's strong interest in making sure fraudulent actors do not gain access to payment systems.

In addition, the payments industry has a long history of fighting fraud through robust underwriting and monitoring policies and procedures, and the use of advanced authentication technologies. With the benefit of decades of expertise, ETA members have developed effective due diligence programs to prevent fraudulent actors from accessing payment systems, monitor the use of those systems, and terminate access for network participants that engage in fraud. 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," which provide information on anti-fraud tools, security, and related issues. When it comes to card data protection, the payments industry took the lead in developing the Payment Card Industry Data Security Standard ("PCI-DSS") to ensure the safety of cardholder data. The PCI-DSS sets forth requirements designed to ensure companies that process, store, or transmit credit card information maintain a secure environment for such data. In addition, the PCI-DSS establishes a framework for implementation of those data security standards, such as assessment and scanning qualifications for covered entities, self-assessment questionnaires, training and education, and product certification programs.

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

ETA 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, the payments industry gains 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 stores.

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.

ETA Supports a Uniform Regulatory Framework that Recognizes the Efforts of Industry to Fight Fraud and Protect Privacy

ETA and its members support U.S and international regulatory efforts that encourage and respect industry efforts to combat fraud and disclose to consumers how their personal information is being used. Working together, lawmakers, regulators, and the payments industry have had remarkable success in protecting consumers and providing them with access to safe and convenient payment systems. This is achievable because the existing legal framework for protecting consumer privacy recognizes the important role of industry efforts in preventing and fighting fraud.

In the U.S., for example, laws have been passed to protect health information (HIPAA) and financial information (Gramm-Leach-Bliley Act 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. These laws recognize the important role that industry plays in combatting fraud and provide provisions that allow for the targeted use and sharing of data to protect consumers and to prevent actual or potential fraud from occurring in the first instance.

Just a few of these U.S. laws include:

Consumer Protection Laws and Provisions Related to Industry Fighting Fraud
Gramm Leach Bliley Act ("GLBA"): The GLBA requires financial institutions to explain their information-sharing practices to customers and safeguard sensitive data. The GLBA has an exception to its information-sharing restrictions for information disclosed to "protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability."[1]
Bank Secrecy Act ("BSA"): The BSA establishes various requirements for covered financial institutions to assist the government in identifying and combatting money laundering and terrorist finance. The BSA includes numerous provisions governing the sharing of information between covered financial institutions and law enforcement, as well as sharing of information between financial institutions in order to identify and report activities that may involve terrorist activity or money laundering.
Health Insurance Portability and Accountability Act of 1996 ("HIPAA"): This law provides data privacy and security provisions for safeguarding medical information. Under the HIPAA Privacy Rule, a covered entity can disclose protected health information to detect fraud, abuse, or compliance violations.
California Financial Information Privacy Act ("CFIPA"): The CFIPA governs financial institutions in California handling nonpublic personal information of the State's residents, including provisions related to consumer notice and the sharing of this personal information. The CFIPA creates an exception to its restrictions to allow sharing of consumer information with nonaffiliated third parties "to protect against or prevent actual or potential fraud, identity theft, unauthorized transactions, claims, or other liability."[2]
Federal Trade Commission ("FTC") Act: Section 5 of the FTC Act prohibits unfair or deceptive business acts or practices, including those relating to privacy and data security. The FTC has recognized the need for industry to share information in order to fight fraud. In a 2012 privacy report, the FTC identified "fraud prevention" as a category "of data practices that companies can engage in without offering consumer choice" because they are "sufficiently accepted or necessary for public policy reasons."[3]

[1] 12 C.F.R. § 1016.15(a).

[2] Cal. Fin. Code § 4056. While the CCPA does not contain an express fraud prevention exception from the substantive rights and protections in the law, for purposes of the opt-out requirement for the sale of a consumer's personal information, there is an argument that a business's disclosure of personal information to prevent fraud affecting the consumer would not amount to the "sale" of such information because the information is not being disclosed "for monetary or other valuable consideration." As discussed further in this letter, such language should indeed be clarified in the CCPA to preserve this vital consumer protection.

[3] FTC, Protecting Consumer Privacy in an Era of Rapid Change, available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change recommendations/120326privacyreport.pdf at 36 (2012); see also id. at 39 (reaffirming this preliminary conclusion following review of public comments).

Consumer Protection Laws and Provisions Related to Industry Fighting Fraud
The Fair Credit Reporting Act ("FCRA"): The FCRA establishes a framework for the use and sharing of consumer reports and requires covered entities to develop and implement an identity theft prevention program. While not an explicit exemption, it has traditionally been understood that consumer information disclosed for the purposes of fraud prevention is not "consumer report information" subject to the restrictions of the FCRA.[4]
Telephone Consumer Protection Act ("TCPA"): The TCPA was designed to safeguard consumer privacy by regulating telemarketing using voice calls, text messaging, and faxes. In 2015, the Federal Communications Commission exempted from the TCPA calls from financial institutions intended to prevent fraudulent transactions, identity theft, or data breaches.[5]

Likewise, the legal frameworks in Europe and Canada respect the need for industry to share personal 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) "processing of personal data strictly necessary for the purposes of preventing fraud,"[6] and (b) decision-making based on profiling that is used for fraud monitoring and prevention 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. . . ."[7]

As lawmakers and regulators continue to explore new ways to protect consumers, ETA and its members encourage them to collaborate with industry to ensure that new laws and regulations are appropriately tailored to address specific needs – this ensures a balance between protecting consumers and allowing industry room to innovate and develop new and beneficial security practices and fraud detection and mitigation tools.

Conclusion

The payments industry never rests. We work tirelessly to fight fraud and protect consumers, including by developing new tools and solutions to prevent, identify and fight fraud by analyzing data. Privacy laws, such as H 901, should 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.

---

[4] This view was supported by the court's decision in Kidd v. Thomson Reuters Corp., 299 F. Supp. 3d 400 (S.D.N.Y. 2017), which concluded that Thomson Reuters was not a "consumer reporting agency" by virtue of a service that disclosed information to customers for fraud prevention purposes.

[5] See In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 et al<https://www.fcc.gov/document/tcpa-omnibus-declaratory-ruling-and-order>., CG Docket No. 02-278, July 10, 2015 at ¶ 129.

[6] European Union, GDPR, Recital 47.

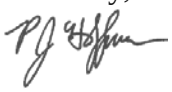
[7] PIPEDA, Available at https://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/118084/sc-2000-c-5.html.

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

* * *

Thank you for the opportunity to participate in the discussion on this important issue. If you have any additional questions, you can contact me or ETA Senior Vice President, Scott Talbott at stalbott@electran.org.

Sincerely,



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

Cc: Members of the House Economic Matters Committee
Delegate Ned Carey
Delegate Benjamin Brooks
Delegate Terri Hill