ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

# Statement of the Electronic Transactions Association

United States House of Representatives
Energy & Commerce Committee
Subcommittee on Commerce, Manufacturing, and Trade Hearing:
*"Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?"*
Thursday, July 18, 2013

In anticipation of the Commerce, Manufacturing, and Trade Subcommittee's July 18 hearing, the Electronic Transactions Association ("ETA") -- an international trade association representing companies that offer electronic transaction processing products and services – submits the following statement for the hearing record.[1] ETA's comments are intended to assist in the Subcommittee's examination of the necessity of federal data breach legislation.

The ETA believes that a uniform national standard for data breach notification will best address the rights of consumers to be notified of a breach when the security of their Personally Identifiable Information ("PII") is truly at risk. Any such national standard should attempt to minimize the compliance risk to businesses. Today, payment processors are forced to comply with an ever-changing array of 47 different state laws on breach notification, a significant challenge to the industry's goal of protecting all consumers against data breaches with uniform national practices.

ETA recommends that any federal breach notification legislation incorporate the following:

A Clear Notification Triggering Mechanism

A clear notification triggering mechanism is essential to facilitating compliance. Legislation should establish a standard for data breach notification that requires notice only when it is determined that there is an actual risk of fraudulent use of compromised PII.

Unambiguous Preemption of State Law

In order to provide consumers with a consistent level of protection, any federal data breach legislation must establish a uniform national standard for data breach notification. Ambiguous state preemption provisions will place businesses in the unenviable position of having to navigate a variety of state laws (at present, 47 different state laws). This is precisely the predicament any legislative proposal should aim to prevent.

[1] ETA represents more than 500 companies that provide payment processing services, including card networks, financial institutions, processors, manufacturers, independent sales organizations, and technology companies.

A Succinct Definition of Personally Identifiable Information

Any definition of PII should be limited to an individual's full name, biometric data, email address, street address, telephone number, full Social Security number and/or personal financial information. The inclusion of various combinations of data elements, especially marginal identifiers (*e.g.*, mother's maiden name, passport number, etc.), will create a compliance standard that is nearly impossible for businesses to adhere to.

Reasonable Notification Requirements

A number of parties in the payment chain will not have access to the contact information necessary to directly notify persons whose PII has been compromised. Federal data breach legislation should allow reasonable time for the party that suffered the data compromise to fulfill any notification obligations by identifying and notifying the industry member in possession of the essential contact information to deliver any required notices.

Recognition of the Existing Legal Framework

Federal data breach legislation should provide a compliance "safe harbor" for entities subject to the Gramm-Leach-Bliley Act or the Fair Credit Reporting Act without making additional parties subject to such banking laws and regulations. This will prevent duplication with existing law that will result in additional, unnecessary, and unproductive regulation.

Acknowledgement of Industry Self-Regulatory Efforts

Federal data breach legislation must provide a "safety net" for effective industry governance related to protection of transactor data. For example, efforts by payment networks (*e.g.*, American Express, Discover, MasterCard, Visa) to establish the Payment Card Industry-Data Security Standards ("PCI-DSS") represent effective security controls by the parties in the best position to ensure that the standards evolve as technology and risk profiles develop and change over time. Any additional regulation should build upon and reflect existing efforts.

* * * * * * *

The payments professionals comprising the ETA's membership take seriously their obligation to protect the confidentiality and security of their customers' credit, debit, and other non-public financial account information. The current patchwork of state laws provides inconsistent protection for consumers and the varying standards established by these laws have created serious compliance challenges for businesses of all types.

As the Subcommittee's examination of federal data breach legislation proceeds, the ETA looks forward to sharing additional information regarding the impact of federal data breach legislation on the payments industry.