



Electronic Transactions Association

2009 Government Relations Policy Position

ISSUE: Data Security and Breach Notification

The payments professionals comprising the Electronic Transactions Association's (ETA) membership take seriously their affirmative and continuing obligation to protect the confidentiality and security of their customers' credit, debit, and other non-public financial account information ("Personal Financial Information"). This protection ensures the free flow of information vital to helping consumers access and use electronic payments, ensures the free flow of commerce, promotes price competition, and maintains public confidence. The current patchwork of state laws provides inconsistent protection for consumers in a national marketplace and the varying standards established by these laws have created serious compliance challenges for businesses of all types.

ETA POSITION:

ETA strongly supports industry self-regulatory efforts for the protection of cardholder data, foremost of which is the Payment Card Industry Data Security Standards (PCIDSS). In the area of government regulation, ETA believes that a uniform national standard for data security and breach notification with respect to Personal Financial Information would best balance the rights of consumers to be notified of a breach when the security of their Personal Financial Information is truly at risk, while minimizing the compliance and legal risk to businesses. ETA believes that any such law should address the following goals:

- ***Establish a clear notification triggering mechanism*** - This is essential to facilitating understanding and compliance. Legislation should establish an unambiguous standard for breach notification that requires notice only when it is determined that there is an actual risk of fraudulent use of compromised Personal Financial Information.
- ***Provide reasonable and effective notification requirements*** - Notice obligations should acknowledge that many parties in the industry will not have access to the contact information necessary to directly notify those persons whose Personal Financial Information was compromised. Legislation should provide that in such cases, the party that suffered the data compromise may fulfill its obligations by notifying the industry-member in possession of the contact information to deliver such notices, or by notifying the affected payment networks. Notice obligations should recognize that parties in the industry may need to research which other industry party or parties possess the contact information to directly notify those persons whose Personal Financial Information was compromised. Legislation should allow reasonable time for the party that suffered the data compromise to fulfill its obligations by identifying and notifying the industry-member in possession of the essential contact information to deliver such notices.
- ***Unambiguously pre-empt state law*** – In order to provide consumers with a consistent level of protection and businesses with commercially reasonable compliance requirements, legislation must establish a uniform national standard for data security and breach notification.

- **Acknowledge responsive industry self-regulatory efforts** – Legislation must provide a “safety-net” for effective industry governance related to protection of cardholder data. For example, efforts by the payment networks (e.g., American Express, Discover, MasterCard, VISA, etc.) to establish the PCIDSS 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 those efforts.
- **Recognize the existing legal framework** – 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.

Formatted: No bullets or numbering

