



**Electronic Transactions Association**

January 19, 2007

Identity Theft Task Force, P065410  
Federal Trade Commission  
Office of the Secretary, Room H-135 (Annex N)  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
Via Email: [regs.Taskforcecomments@idtheft.gov](mailto:regs.Taskforcecomments@idtheft.gov)

Re: President's Identity Theft Task Force Request for Public Comment

Dear Task Force Representative:

The Electronic Transaction Association<sup>1</sup> ("ETA") is pleased to submit comments to the President's Identity Theft Task Force<sup>2</sup> (the "Task Force") on ways to improve the effectiveness and efficiency of federal government efforts to reduce identity theft. ETA applauds the President for bringing together 17 different federal agencies and departments to develop a consolidated approach in directing the federal government's efforts to combat identity theft under the leadership of Attorney General Alberto R. Gonzales and Federal Trade Commission Chairman Deborah Platt Majoras.

The Task Force request for comment covers a wide range of issues including: government use of social security numbers; prosecution of identity thieves who reside in foreign countries; creation of a national identification document; and many other important measures that the federal government may consider in its efforts to combat identity theft. While all of the items discussed in the request for comment are meritorious, national standards for data security and breach notification are strongly supported by the ETA Community.

The payments professionals comprising ETA's membership take seriously their affirmative and continuing obligation to protect the confidentiality and security of their customers' personal information. This protection ensures the free flow of information in our society which is vital to helping consumers daily with access to credit, price competition, and even with issues related to public safety. The ETA supports efforts to develop a national standard for data security and breach notification. Moreover, ETA recognizes that the current patchwork of state laws provides inadequate 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.

---

<sup>1</sup> ETA, founded in 1990, is the nation's oldest and largest organization of businesses representing the merchant acquiring industry that enables merchants to offer electronic payment services to consumers. ETA's diverse membership, including state/federal chartered financial institutions, merchant service providers (also known as independent sales organizations), and credit card companies, is an integral part of the backbone of the American economy that facilitates electronic payments.

<sup>2</sup> Presidential Executive Order (May 10, 2006), [www.whitehouse.gov/news/releases/2006/05/20060510-3.html](http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html)

ETA has consistently supported the legislative goals of balancing the rights of consumers to be notified of a breach when the security and confidentiality of their personal information is truly at risk, with the need to avoid “desensitizing” the public with too many unnecessary notices. ETA believes that any national standard for data security and breach notification should address the following goals:

- ***Establish a clear notification triggering mechanism*** - This is essential for immediate industry understanding and compliance. The legislation should establish an unambiguous standard for breach notification that requires notice only when it is determined that a real risk of identity theft exists (e.g., compromised information was unencrypted, evidence of misuse found, etc.).
- ***Unambiguously pre-empt state law*** – In order to provide consumers with consistent level of protection and businesses with workable compliance requirements, the legislation must establish a uniform national standard for data security and breach notification.
- ***Acknowledge responsive industry self-regulatory efforts*** – The legislation must provide a “safety-net” for effective industry governance. For example, efforts by the card companies (e.g., AMEX, Discover, MasterCard, VISA, etc.) to establish Payment Card Industry (PCI) data security standards that are both rigorous and enforceable, should represent effective security controls.
- ***Recognize the existing legal framework*** – The legislation should provide a compliance “safe harbor” for entities subject to the Gramm-Leach-Bliley Act. This will prevent duplication with existing law that will result in additional, unnecessary and unproductive regulation.

ETA urges the Task Force to recommend that the administration actively support passage of a national standard for data security and breach notification that satisfies the aforementioned criteria.

In conclusion, ETA applauds the efforts of the President’s Identity Theft Task Force to ensure that consumer information is protected and that an adequate legal framework exists to prosecute the perpetrators of identity theft. Should you have any questions or need any additional information, please contact Rob Drozdowski of my staff at (202) 828-2635 or [Rob.Drozdowski@electran.org](mailto:Rob.Drozdowski@electran.org).

Sincerely,

Carla Balakgie, CAE  
Executive Director  
Electronic Transactions Association