May 22, 2014

The Honorable Harry Reid
Majority Leader
U.S. Senate
Washington, D.C. 20510

The Honorable John Boehner
Speaker
U.S. House of Representatives
Washington, DC 20515

Dear Majority Leader Reid and Speaker Boehner,

As Congress continues to examine the issues surrounding data breach legislation, we the undersigned associations write to express our ongoing support for a uniform national standard for data breach notification. We represent thousands of the leading companies in the information economy. Our member companies use data in responsible and innovative ways that have revolutionized the delivery of products and services to their customers and fostered many additional consumer benefits, such as virtually limitless free Web content. In short, information and information-sharing has changed the everyday lives of most Americans and has significantly contributed to U. S. economic growth overall.

Businesses that provide products and services valued by consumers must be engaged in constantly building consumer trust. American businesses work tirelessly to implement security measures to safeguard data. Unfortunately, business systems are also under constant assault from criminals employing sophisticated techniques. In fact, according to the recently released ninth annual Ponemon Institute "*Cost of Data Breach Study: Global Analysis,"* the most expensive data breaches were those caused by malicious and criminal attacks. In the U.S. these costs are the highest in the world, reaching $246 per record compromised. Businesses have compelling incentives to protect sensitive information and maintain valuable customer relationships.

We agree that the delivery of proper notification to affected individuals when data is compromised is a vitally important issue for both businesses and consumers. To this end, we have worked collaboratively with Members of Congress in both chambers and on both sides of the aisle over the years to help identify a workable path toward passage of a federal data breach notification law. As discussions continue in the 113th Congress, we remain committed to supporting the enactment of legislation that will provide consumers with timely information and meaningful protections without unnecessarily hampering critical business operations.

We continue to believe that meaningful data breach notification legislation must establish a clear federal standard that preempts the patchwork of state laws in this area. Currently, disparate laws in 47 states plus the District of Columbia, Guam, Puerto Rico and the Virgin Islands, frustrate efficient and uniform breach notification to consumers. This is particularly true when a data breach affects individuals nationwide who reside in a number of the jurisdictions covered by these various laws. Enforcement of a uniform federal standard should also be consolidated under the appropriate federal government agency or agencies.

Further, any federal notification regime should only be triggered a by a breach event that poses a *significant risk* of identity theft or other economic harm to the affected individuals. We remain concerned that an overly-inclusive trigger would cause consumers to be burdened with unnecessary notifications that could ultimately lead to consumer complacence when a truly actionable breach occurs. Similarly, a too broadly-drawn definition of sensitive personally identifiable information (sensitive PII) – one that captures non-sensitive data elements such as consumer information one might find in a printed or online telephone directory – could unnecessarily trigger notice when no real threat of identity theft or fraud exist.

A balanced bill would also exclude public records and information derived from public records from its scope.

As we have learned from several recent data breaches, businesses are best equipped to protect and notify consumers when they are provided sufficient time to gather the facts, secure their systems, and work with law enforcement before prematurely notifying the public. Initial breach detection, the restoration of system security, and a forensic analysis to determine which data may have been compromised and which customers may be affected are necessary but complicated tasks that often take months to complete. However, we do believe that businesses should always act to notify consumers *without unreasonable delay*, and, if additional time is required to complete what often becomes a criminal investigation, then law enforcement involved in helping companies track down criminals responsible for the breach should not have their investigation compromised by premature public notification.

Given the complexities of both data breach response and notification – often layered with the added complication of an ongoing criminal investigation -- we believe that a federal notification standard should not allow for a private right of action. Similarly, we do not believe that the Federal Trade Commission should be granted additional civil penalty authority in this area.

We need Congress to act now to enact legislation to help businesses effectively inform and ultimately protect the customers they serve when data compromises do occur.

We look forward to working with you on these important issues.

Sincerely,

American Association of Advertising Agencies
American Advertising Federation
Association of National Advertisers
Consumer Data Industry Association
Direct Marketing Association
Electronic Retailing Association
Electronic Transactions Association
Global Address Data Association
Interactive Advertising Bureau
MPA - The Association of Magazine Media
National Business Coalition
National Retail Federation
NetChoice
Online Publishers Association
Retail Industry Leaders Association
TechAmerica, powered by CompTIA

CC: Members of the Senate Committee on Commerce, Science, and Transportation; Committee on the Judiciary, and Committee on Banking, Housing and Urban Affairs; and members of the House Committee on Commerce and Energy; Committee on the Judiciary; and the Financial Services Committee