November 6, 2014

The Honorable Harry Reid
Senate Majority Leader
522 Hart Senate Office Building
Washington, DC 20510-2803

The Honorable Mitch McConnell
Senate Minority Leader
317 Russell Senate Office Building
Washington, DC 20510-1702

The Honorable John Boehner
Speaker of the House
1011 Longworth House Office Building
Washington, DC 20515-3508

The Honorable Nancy Pelosi
Minority Leader
235 Cannon House Office Building
Washington, DC 20515-0512

Dear Leaders Reid and McConnell, Speaker Boehner and Leader Pelosi:

The recent spate of news stories about data security incidents raises concerns for all American consumers and for the businesses with which they frequently interact. Organized groups of criminals, often based in Eastern Europe, have focused on U.S. businesses, including financial institutions, technology companies, manufacturing, retail, utilities and others. These criminals devote substantial resources and expertise to breaching data protection systems. Vigilance against these threats is necessary, but we need to focus on the underlying causes of breaches as much as we do on the effects.

Given the breadth of these invasions, if Americans are to be adequately protected and informed, any legislation to address these threats must cover all of the types of entities that handle sensitive personal information. Exemptions for particular industry sectors not only ignore the scope of the problem, but create risks criminals can exploit. Equally important, a single federal law applying to all breached entities would ensure clear, concise and consistent notices to all affected consumers regardless of where they live or where the breach occurs.

If there is anything that the recently reported data breaches have taught us, it is that any security gaps left unaddressed will quickly be exploited by criminals. For example, the failure of the payment cards themselves to be secured by anything more sophisticated than an easily-forged signature makes the card numbers particularly attractive to criminals and the cards themselves vulnerable to fraudulent misuse. Better security at the source of the problem is needed. The protection of American's sensitive financial information is not an issue on which sacrificing comprehensiveness makes any sense at all.

The safety of Americans' data is only as secure as the weakest link in the chain of entities that share that data. For instance, when information moves across communications lines – for transmission or processing – or is stored "in the cloud," it would be senseless for legislation to exempt these service providers, if breached, from data security and notification obligations that the law would place upon any other entity that suffers a breach. Likewise, data breach legislation should not subject businesses handling the same sensitive customer data to different

rules with different penalty regimes, as such a regulatory scheme will inevitably lead to inconsistent public notice and enforcement.

With respect to the breadth of the threat we face, some recent examples are instructive. This summer, it was reported that JPMorgan Chase had suffered a data security breach that we only recently learned is the largest reported breach on record, affecting 83 million accounts that had been accessed online or through mobile devices. The criminals involved reportedly took over computers around the world to cover their tracks. Given the sophistication of the attack, even months after initial disclosure, it is not clear whether the bank's system is free of the hackers involved. It has also been reported that nine other banks suffered similar data breaches and there is evidence that there is a focused effort to breach financial institutions by these criminals. At least four companies, for example, have determined that an IP address used to attack JPMorgan is the same as one used to attack their own systems. Despite all that reporters have uncovered to date, however, financial regulators have not required financial institutions to provide the same detailed notice to their customers as is required of other businesses under law.

Following the coordinated attack on banks this summer, it was revealed in September that over 100 account subscribers to Apple's widely-used iCloud service had suffered a series of targeted attacks that ultimately led to the unlawful acquisition of sensitive photographs stored on the iCloud servers. Merchants have also been attacked by criminals employing sophisticated and previously unseen tools to steal payment card numbers. Payment card data has been targeted by criminals in data breaches at every type of entity that handles such data – from financial institutions to retailers, card processors, and telecommunications providers. While the media typically reports breaches occurring at large, well-known companies, these breaches affect organizations large and small alike, even such local entities as Georgia's Own Credit Union.

The recent breach at a Department of Homeland Security contractor that exposed sensitive information of tens of thousands of DHS employees heightens awareness of the significant risks of breaches outside the commercial sector. The Government Accountability Office (GAO) warned on April 2, 2014, that there were 25,566 "reported information security incidents involving personally identifiable information (PII)" at federal agencies in 2013 alone.[1] The GAO report observed that "the federal government collects large amounts of PII from the public, including taxpayer data, Social Security information, and patient health information" and concluded that it is "critical that federal agencies ensure that this information is adequately protected from data breaches."

The Verizon Data Breach Investigations Report is the most comprehensive summary of these types of threats. The 2014 report (examining 2013 data) determined that there were 63,437 data security incidents reported by industry, educational institutions and governmental entities last year and that 1,367 of those had confirmed data losses. Of those, the financial industry suffered 34%, public institutions (including governmental entities) had 12.8%, the retail industry had 10.8%, and hotels and restaurants combined had 10%.

Data security intrusions are a threat faced by every sector of our nation. Consumers deserve to know when they are placed at risk, regardless of where the risk arises. The public

[1] See http://www.gao.gov/products/GAO-14-487T.

expects no less. Congress should act to standardize reasonable, timely notification of sensitive data breaches whenever and wherever they occur. However, legislation that would demand notice of some sectors, while leaving others largely exempt, will unfairly burden the former and unnecessarily betray the public's trust.

We look forward to working with you to address criminal data thefts in a way that covers everyone who is at risk, and that promotes solutions that will protect American consumers now.

Alabama Grocers Association
American Hotel and Lodging Association
California Retailers Association
Conexxus
Florida Petroleum Marketers and Convenience Store Association
Food Marketing Institute
Georgia Association of Convenience Stores
Illinois Retail Merchants Association
Independent Oil Marketers Association of New England
Indiana Retail Council
Louisiana Retailers Association
Minnesota Grocers Association
Minnesota Retailers Association
National Association of Chain Drug Stores
National Association of College Stores
National Association of Convenience Stores
National Association of Truck Stop Owners
National Grocers Association
National Restaurant Association
National Retail Federation
Nebraska Retail Federation
New Hampshire Retail Association
New Jersey Food Council
New Jersey Retail Merchants Association
New York Association of Convenience Stores
North Dakota Petroleum Marketers Association
North Dakota Retail Association
Ohio Grocers Association
Pennsylvania Food Merchants Association
Pennsylvania Retailers' Association
Petroleum Marketers Association of America
Petroleum Marketers & Convenience Stores of Iowa
PMCI Trust
Retail Association of Maine
Retailers Association of Massachusetts
Retail Solutions Providers Association
RINAlliance, Inc.

Society of Independent Gasoline Marketers of America
Utah Food Industry Association
Utah Retail Merchants Association
Vermont Retail & Grocers Association
Virginia Petroleum Convenience and Grocery Association
Washington Food Industry Association Education Foundation
West Virginia Oil Marketers and Grocers Association