CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

R. BRUCE JOSTEN
EXECUTIVE VICE PRESIDENT
GOVERNMENT AFFAIRS

1615 H STREET, N.W.
WASHINGTON, D.C. 20062-2000
202/463-5310

September 14, 2011

The Honorable Patrick J. Leahy
Chairman
Committee on Judiciary
United States Senate
Washington, DC 20510

The Honorable Charles E. Grassley
Ranking Member
Committee on Judiciary
United States Senate
Washington, DC 20510

Dear Chairman Leahy and Ranking Member Grassley:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses and organizations of every size, sector, and region, writes to express concerns with S. 1151, the "Personal Data Privacy and Security Act of 2011" and S. 1408, "the Data Breach Notification Act of 2011."

The Chamber appreciates the goal of both S. 1151 and S. 1408. Protecting individuals' sensitive personal information from theft or illegal uses has been and will continue to be a top priority for the business community. Enacting a uniform federal standard for data security and breach notifications could ease compliance and foster job creation.

However, the Chamber believes that certain aspects of such legislation would impede the ability of businesses to expand and innovate. The Chamber urges the Committee to address these shortcomings before either bill reaches the full Senate.

I. S. 1151, the "Personal Data Privacy and Security Act of 2011"

a. Definition of Sensitive Personally Identifiable Information (PII)

Beyond the question of whether mother's maiden name and date of birth should be classified as sensitive information, it is highly unlikely that those data elements could be used, as envisioned in Section(3)(a)(12), to commit identity theft unless other information was also present. The Chamber suggests a construct that ties name and address back to truly sensitive information, such as full Social Security number, a driver's license number or a financial account number, including any PIN which is required to access the account. This would be consistent with most of the laws already enacted by states—laws with which our members are already complying.

b. Federal Trade Commission (FTC) Rulemaking Authority to Modify the Definition of PII

Providing the FTC with Administrative Procedure Act (APA) rulemaking under Section 3(b) of this Act would create regulatory uncertainty and harm business' ability to innovate.

Moreover, as the definition is a key feature in determining who is and who is not covered by the bill, this language represents an inappropriate delegation of congressional power to an unelected regulatory body. Therefore, the Chamber urges the Committee to delete this provision because the FTC's current rulemaking authority is sufficient.

c. Breach Notification Trigger

Section 212(b)(1)(A) says breach notification is not required if the risk assessment finds that there is "no significant risk that a security breach has resulted in, or will result in, identity theft, economic loss or harm, or physical harm to the individual…." To avoid over-notification, the presumption should be reversed and require notice only when there is a security breach that creates a significant risk of identity theft, fraud, or other financial harm. The element of physical harm should be eliminated because it is overly broad and could bring in claims (e.g., embarrassment, loss of dignity, time spent filing a complaint, etc.) not related to identity theft, fraud, or other financial harm.

d. Enforcement of the Act by State Attorneys General

The Chamber has concerns with the undefined nature and number of the entities that can be granted enforcement power under Section 203(c)(1) of the Act. Under the provision, "any State or local law enforcement agency" as authorized by statute or by the State Attorney General (AG) is an eligible entity. Accordingly, a State Attorney General could hire an outside plaintiffs' attorney firm on a contingency fee basis—a practice that often creates a conflict of interest and threatens the rule of law. Worse, the infinite number of potential plaintiffs would virtually guarantee that otherwise innocent defendants would have to settle the cases lodged against them rather than exercise their right to receiving a judgment on the merits.

e. National Standard for Breach Notification

Under Section 214(b), states can add additional breach notification content requirements. This lack of full and effective preemption could frustrate the purpose of the legislation and create a confusing patchwork of requirements and enforcement regimes that could undermine the effectiveness of this legislation.

f. Liability

The Chamber has serious concerns that the civil penalty language in Section 203(c)(4) would permit State AGs (possibly all 50 of them) and a potentially unlimited number of state or local law enforcement agencies to prosecute the same defendants on the same facts in the same federal court. As noted previously, this would encourage settlements rather than judgments on the merits.

g. Requirements for a Personal Data Privacy and Security Program

The detailed security program requirements in section 202 would result in an expensive and excessive compliance burden, and the Chamber reiterates its objection to the inclusion of privacy components in the legislation. Additionally, the Chamber questions the enforceability of such requirements and would rather have the legislation tout these programs as a goal rather than mandate their implementation. The chamber also is concerned about the regulatory

unpredictability that would be created, in an uncertain economy, by giving the FTC rulemaking authority to implement this section of the act.

h. Breach Notification and Criminal Penalties

Criminal penalties for failure to notify are inappropriate because the determination as to whether a security breach has taken place is complicated and too often subjective. A person could make a good faith determination that a breach has not occurred and therefore not reportable, and still be subject to criminal penalties. Criminal penalties, which involve the loss of personal liberty, should always be reserved for those that actually use PII for unlawful purposes.

Although Section 102 now requires an economic harm of at least $1,000 and that an individual must have knowledge about the obligation to notify, the revisions do not eliminate the inappropriate risks to companies that criminal penalties may impose.

i. Safe Harbor

The Chamber is concerned that Section 201(d) directs the FTC to identify and define the "industry standards" that determine which entities are eligible for the Safe Harbor. The Chamber urges the Committee to give precise guidance to the FTC, especially with criminal penalties at stake.

II. S. 1408, "the Data Breach Notification Act of 2011"

The Chamber is also concerned about similar provisions contained in S. 1408, the "Data Breach Notification Act of 2011." For example, S. 1408 contains an overly broad notification trigger where there is a "significant risk that a security breach has resulted in, or will result in, harm to the individual. …" In addition to over notification, the term "harm" could allow for claims not related to the underlying purpose of the bill.

Additionally, the bill classifies things like mother's maiden name and date of birth as "sensitive personally identifiable information" which could lead to identity theft. While securing sensitive data is a laudable goal, without other information present, it is highly unlikely that those data elements could be used to commit such a crime. These are just a few of the concerns which the Chamber urges the Committee to address these before S. 1408 is considered by the full Senate.

Thank you for taking our concerns into consideration. The Chamber looks forward to continued discussions with you, your committee colleagues, and your staff on this very important topic.

Sincerely,

R. Bruce Josten

cc: Members of the Senate Committee on the Judiciary