



Statement of the U.S. Chamber of Commerce

ON: H.R. ___, A DISCUSSION DRAFT TO REQUIRE GREATER PROTECTION FOR SENSITIVE CONSUMER DATA AND TIMELY NOTIFICATION IN CASE OF BREACH

TO: UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE

BY: JASON D. GOLDMAN
COUNSEL, TELECOMMUNICATIONS & E-COMMERCE
U.S. CHAMBER OF COMMERCE

DATE: JUNE 15, 2011

The Chamber's mission is to advance human progress through an economic, political and social system based on individual freedom, incentive, initiative, opportunity and responsibility.

The U.S. Chamber of Commerce is the world's largest business federation, representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

More than 96 percent of the Chamber's members are small businesses with 100 or fewer employees, 70 percent of which have 10 or fewer employees. Yet, virtually all of the nation's largest companies are also active members. We are particularly cognizant of the problems of smaller businesses, as well as issues facing the business community at large.

Besides representing a cross-section of the American business community in terms of number of employees, the Chamber represents a wide management spectrum by type of business and location. Each major classification of American business – manufacturing, retailing, services, construction, wholesaling, and finance – is represented. Also, the Chamber has substantial membership in all 50 states.

The Chamber's international reach is substantial as well. It believes that global interdependence provides an opportunity, not a threat. In addition to the U.S. Chamber of Commerce's 113 American Chambers of Commerce abroad, an increasing number of members are engaged in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Positions on national issues are developed by a cross-section of Chamber members serving on committees, subcommittees, and task forces. More than 1,000 business people participate in this process.

Hearing on H.R. ____, A Discussion Draft to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach

**Testimony of Jason D. Goldman
Counsel, Telecommunications & E-Commerce
U.S. Chamber of Commerce**

June 15, 2011

Good morning, Chairwoman Bono Mack, Vice Chairwoman Blackburn, Ranking Member Butterfield, and other distinguished members of the Subcommittee on Commerce, Manufacturing and Trade. I am Jason Goldman, Telecommunications & E-Commerce Counsel at 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. On behalf of the Chamber and its members, I thank you for the opportunity to testify here today regarding the discussion draft of the "Secure and Fortify Electronic Data Act" (the "SAFE Data Act").

I. Information Economy

We live in an information economy. Today, Chamber members of all shapes and sizes communicate with employees, existing customers, potential customers, and business partners around the world. They use data to spur sales and job growth, enhance productivity, enable cost-savings, and improve efficiency. For example, the beneficial use of U.S. health care data could result in \$300 billion in value to health care consumers each year, including reducing national expenditures in this area by \$200 billion or 8 percent.¹ The power of data also could help retailers boost their profit margins by as much as 60 percent.²

Global and U.S. data usage will continue to skyrocket. The "gigabyte equivalent of all movies ever made will cross global IP networks every five minutes" by 2015, according to Cisco.³ U.S. mobile data traffic is expected to increase by 21 times from 2010 to 2015.⁴ As consumers embrace tablets, smart appliances, and other wireless broadband-enabled devices,

¹ McKinsey Global Institute, *Big Data – The Next Frontier for Innovation, Competition, and Productivity*, p. 2, May 2011, available at: http://www.mckinsey.com/mgi/publications/big_data/pdfs/MGI_big_data_full_report.pdf.

² *Id.*

³ White Paper, *Cisco Visual Networking Index: Forecast and Methodology, 2010–2015*, Cisco Systems, Inc., June 1, 2011, available at: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html

⁴ Press Release, *Cisco Visual Networking Index Forecast Projects 26-Fold Growth in Global Mobile Data Traffic From 2010 to 2015*, Cisco Systems, Inc., Feb. 1, 2011, available at: http://newsroom.cisco.com/mobile/dlls/2011/prod_013111.html. ("Cisco Visual Networking Index Forecast Global Mobile Data Forecast").

mobile network traffic will soar. Mobile-connected tablets will generate as much traffic in 2015 as the entire global mobile network in 2010, growing over 205-fold over that same time period.⁵

In today's tough economy, businesses depend more than ever on having beneficial and trusted relationships with their customers. Therefore, there is no question that protecting sensitive consumer information should be a priority for all businesses that collect and store this data, and that consumers deserve to be promptly notified if a security breach has put them at risk of identity theft, fraud, or other harm.

II. *SAFE Data Act*

The Chamber supports the enactment of meaningful federal data security legislation that would implement national data security standards to protect against the unauthorized access to sensitive personal information about businesses' customers and breach notification requirements to notify customers when a significant risk to them may result from a data security breach. At the same time, the Chamber urges policymakers to ensure that any legislation in this area does not hinder innovation or the beneficial uses of data.

The Chamber appreciates the willingness of the Subcommittee to work with us on legislation aimed at accomplishing this goal and believes that this bill contains improvements in several areas that raised concern in similar legislation that was considered by the full Committee and the full House in the 111th Congress.

The Chamber only recently received the text of the SAFE Data Act, so the comments below are based on our initial read of the bill and may change as we further analyze the language and vet the bill through our membership.

a. Federal Preemption

The United States has a national economy, and almost every state has enacted various data security and breach notification provisions, many of which differ from one another in material ways.⁶ This patchwork of state laws not only makes compliance difficult for businesses, but can also create confusion for consumers who receive notices from many sources. The Chamber supports the preemption of state information security and related liability laws to create a national uniform standard that would create regulatory certainty and minimize compliance costs for businesses that operate in multiple states.

⁵ *Cisco Visual Networking Index Forecast.*

⁶ *State Security Breach Notification Laws*, National Conference of State Legislatures, Oct. 12, 2010, available at: <http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx>. ("Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.")

b. Breach Notice Trigger

The Chamber has long advocated for a notice requirement that avoids the dangers of over-notification. If needlessly alarmed, consumers may take actions that are not warranted and waste their time. Alternatively and more worrisome, consumers that are flooded by notices may be falsely lulled into inactivity and not take proper action when a true risk is identified. Therefore, the Chamber is pleased that the draft bill recognizes that notification should be based on risk of harm, not just on the mere fact a data breach has occurred. There is a tremendous difference between a breach that creates the possibility of identity theft and a breach where no or little risk is created. Additionally, the Chamber recommends changing the standard from “reasonable risk” to “significant risk.”

Moreover, Congress should place restrictions on the Federal Trade Commission’s (Commission) ability to define “harm” when examining risk. It is of course incredibly important for the government to fulfill its traditional role of protecting consumers from financial theft, physical injury, and other tangible forms of harm. However, any move to broaden the definition of “harm” should be carefully considered.

The Chamber agrees that notification of a breach is not necessary where the data has been rendered unusable, unreadable, or indecipherable by a commonly-accepted, effective industry standard or industry practice, such as encryption, redaction, or access controls. The Chamber encourages a technology-neutral approach to this provision that keeps the Commission, which may not have the requisite expertise, from having the responsibility of determining the adequacies of these technologies.

The Chamber recommends the inclusion of a threshold number of individuals requiring notification that would also trigger notification to the Commission. One option is 5000, which is the draft bill’s threshold for notification to credit agencies. Another option is 500, the threshold for notice to the Department of Health and Human Services under the Health Information Technology for Economic and Clinical Health (“HITECH”) Act. If neither of these provisions is adopted, then the draft bill should direct the Commission to issue guidance about what criteria the agency will use to determine which breaches are listed on the agency’s Web site. Without such guidance, the Commission could potentially post all breaches, no matter the severity.

c. Breach Notification Timing

The Chamber agrees that consumers should be notified in a timely manner after the occurrence of a reportable data breach. However, given the complexities of dealing with a data breach, the Chamber recommends that the draft bill be modified to allow companies a “reasonable” amount of time to notify consumers, rather than a specific timeframe (i.e., 48 hours).

Adopting a “reasonable” timeframe would help to ensure that consumers are notified when there is a true risk and avoids over-notification that may lead to consumer overreaction and inconvenience (e.g., needlessly cancelling a credit card). Also, it is important to note that each layer of requirements that must be completed, included, or offered (e.g., arranging for credit

report monitoring or issuing replacement credit cards) as part of the breach notification potentially adds to the time that it takes to prepare and issue the notification.

To help catch cybercrooks and other criminals as well as to ensure the safety of our nation, the Chamber supports the provisions in the draft bill permitting delay of notification for law enforcement or national security purposes. It is proper to delay notification to avoid impeding civil or criminal investigations. Additionally, if it is determined that notification would harm national or homeland security, delay is certainly appropriate. Additionally, the Chamber recommends the inclusion of language to clarify which state or federal agencies (such as the Department of Homeland Security) that a company can reasonably rely upon for this exemption.

d. *Liability*

The Chamber is concerned about the application of a daily fine as it relates to the draft bill's security requirements. For example, if an entity is found liable for violating the data minimization requirement, is every day that the entity maintains records that should have been destroyed throughout all of their databases a multiplier penalty? Companies could potentially be in permanent violation.

e. *Data Minimization*

The determination of what information to collect is different for each company and business plan. The Chamber is concerned that a data minimization requirement could lead to regulatory uncertainty. Rather than risk liability, companies may self-censor themselves. By taking such action, these companies may fail to realize the full, legitimate benefits of their data. Innovation and economic activity could suffer. Thus, the Chamber recommends that the draft bill should encourage data minimization as a goal, not a requirement.

f. *Information Brokers*

Information brokers provide information that is used in many beneficial ways in our economy and by our society, including: fair and efficient consumer credit allocation; local and national background employment screenings and national security clearances; fraud prevention in the private-sector and in government; the collection of child support payments; and assistance to law enforcement, private agencies, public and private-sector investigators on matters ranging from locating missing and exploited children to preventing money laundering and terrorist financing.

The Chamber is pleased that the draft does not include provisions contained in last year's bill (H.R. 2221) that could unintentionally reduce consumer protection by endangering the establishment and use of databases that are designed to protect consumers, such as those intended to stop fraud and identity theft.

g. Enforcement

The Chamber is concerned that enabling state attorneys general to impose 50 different enforcement regimes will undermine the uniformity of this Act, and will make compliance exceedingly difficult. Alternatively, this provision should be transparent and consistent with existing law (i.e., the Fair Credit Reporting Act). At the very least, the draft bill should curtail the ability of state attorneys general to utilize private outside contingency fee lawyers to enforce this Act or to litigate claims on behalf of their constituents.

h. Technology Neutral

The Chamber urges policymakers to ensure that federal laws and regulations are technology-neutral. The government should not be in the position of picking technology winners and losers. The marketplace, not government fiat, is the best way to ensure technological innovation and consumer choice.

Therefore, the Chamber is pleased that the draft bill directs the Commission to promulgate rules under this Act in a technology-neutral manner. Specifically, the draft bill prohibits the Commission from requiring the deployment or use of any specific products or technologies, including any specific computer software or hardware.

i. No Private Right of Action

Though the Chamber would prefer the inclusion of explicit language prohibiting private rights of action, the Chamber supports Section 6(b)(1) of the draft bill. Allowing private lawsuits would only serve to increase the likelihood that elements of the plaintiffs' class action trial bar will use this legislation as a way to increase class action litigation with little benefit being given to the general public. Additionally, a perverse incentive not to notify consumers of a data breach could be created if entities covered under the draft bill become worried about opening themselves to potential law suits.

j. Definitions

For the definition of "service provider," the Chamber recommends adopting language that more closely tracks the definition of telecommunications in the Telecommunications Act.⁷ One option may be to use the language in H.R. 1707, the "Data Accountability and Trust Act," which defines "service provider" as:

[A]n entity that provides to a user transmission, routing, intermediate and transient storage, or connections to its system or network, for electronic communications, between or among points specified by such user of material of the user's choosing, without modification to the content of the material as sent or received. Any such entity shall be treated as a service provider under this Act only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage or connections.

⁷ 47 U.S.C. § 153(50).

III. Conclusion

Once again, the Chamber greatly appreciates the opportunity to testify today. The Chamber stands ready to work with you on these and other issues. Thank you very much.