



STATEMENT OF  
STUART K. PRATT  
CONSUMER DATA INDUSTRY ASSOCIATION  
BEFORE THE  
Energy and Commerce Committee  
Subcommittee on Commerce, Manufacturing and Trade  
House of Representatives  
ON  
Discussion Draft of H.R. \_\_\_\_, a bill to require greater protection for sensitive  
consumer data and timely notification in case of breach

Wednesday, June 15, 2011

1090 Vermont Avenue, NW, Washington, D.C. 20005

202-371-0910 Phone 202-371-0134 FAX

Chairman Bono-Mack, Ranking Member Butterfield, and members of the Subcommittee, my name is Stuart Pratt, and I am president and CEO of the Consumer Data Industry Association (CDIA). Thank you for this opportunity to testify.

CDIA is an international trade association with more than 190 member companies, providing our nation's businesses with the data tools necessary to manage risk in a wide range of consumer transactions. These products include credit and mortgage reports, identity verification tools, law enforcement investigative products, fraudulent check transaction identification systems, employment screening, tenant screening, depository account opening tools, decision sciences technologies, locator services and collections. Our members' data and the products and services based on it, ensure that consumers benefit from fair and safe transactions, broader competition and access to a market which is innovative and focused on their needs. We estimate that the industry's products are used in more than nine billion transactions per year.

We applaud the focus of this hearing. For more than a decade CDIA has been on record as supporting the enactment of a uniform Federal standard for both the security of sensitive personal information and the notification of consumers where there is a significant risk of identity theft.

You have asked us to comment on the discussion draft H.R. – entitled the “Secure and Fortify Electronic Data Act” (SAFE Data Act). While CDIA will continue to analyze this proposal, below are selected thoughts which we hope will be helpful to you and the

Committee as you continue to refine the bill. We look forward to continuing this dialogue beyond today's legislative hearing.

**Alignment of H.R. – with existing state and Federal laws:**

Section 2 of the draft bill proposes to require any person engaged in interstate commerce that owns or possesses data in electronic form containing personal information to establish policies and procedures for information security based on rules which would be promulgated by the Federal Trade Commission. Section 3 of H.R. - requires these same persons to comply with specific requirements of the Act where they discover a breach of security relating to personal information.

First, it is essential that these two duties (securing information and notification in the case of a data breach) are fully and completely preemptive of any current or future state laws that address in any way the same subject matter. With this in mind, we generally applaud the inclusion of Section 6 dealing with preemption. In terms of details, we will look over the provision in greater detail and likely provide some additional suggestions to ensure that the intent of this section is accomplished.

Regarding the data security component of the bill, section 2(b) is an excellent start in terms of ensuring that H.R. – does not impose duplicative standards on U.S. businesses that are already subject to duties in other Federal laws. CDIA fully supports the clear and complete exemption for persons who are subject to the Gramm-Leach-Bliley Act with

regard to duties to secure sensitive personal information. This clear exemption is the right statutory construction. We would suggest expanding this exemption to include consumer reporting agencies that are subject to the Fair Credit Reporting Act (15 U.S. C. 1681 *et seq.*).

Regarding the breach notice component of the bill, we suggest that the same statutory construction of the data security exemption be used with regard to Section 3(j). Section 3(j) appears designed to avoid duplicative duties for persons who must provide a notification to consumers under other Federal laws where there has been a breach of sensitive personal information. We believe the bill's "in compliance with" standard, however, does create a problem of double-jeopardy for companies subject to other laws or Federal regulations. We look forward to continuing a dialogue on this provision and appreciate the inclusion of language on this subject.

#### **Align duties and enforcement -**

Section 4 of H.R. – applies the requirements of Sections (2) and (3) to any person in possession personal information as defined by the bill. We will continue to analyze this question, but our first-impression is that the broad application of these requirements appears to create tension between the application and the exemptions to these requirements established in sections 2(b) and 3(j), discussed above. We would like to work with your staff to clarify that these questions are addressed.

We would also want to further examine the references to the term “information broker,” and how that definition may be duplicative of the general application of the draft legislation.

Let me now discuss some of the ways in which duties under H.R. - interplay with existing duties found in other laws.

### **Data Breach Notification Requirements**

Section 3 of H.R. - establishes requirements for notifying consumers where there is a breach of personal information. A notice is not required where “there is no reasonable risk of identity theft, fraud, or other unlawful conduct.” There are also exceptions to the notification requirement if the data was encrypted or otherwise rendered unreadable or indecipherable.

CDIA agrees that an effective risk-based trigger for the disclosure of notices is necessary and believes that the phrase “significant risk of identity theft” sets the right standard. We also agree that there should be specific exceptions for data which is encrypted or otherwise rendered unreadable, indecipherable or unusable.

### **Timing of breach notification**

We agree that law should set clear parameters with regard to the timing of when notices should be sent to consumers. Currently H.R. – proposes that notices should be sent within 48 hours. CDIA will continue to consult with its members to provide additional input on this requirement and whether or not there are consequences to this approach. We would urge the committee to also consider consultation with law enforcement agencies which sometimes need additional investigative time to fully understand the nature of the breach and the risks to consumers.

### **Content of Breach Notifications**

Section (3)(d)(B) describes the content of notices which will be sent to consumers. With regard to the consumer's right to one free credit report on a quarterly basis, we appreciate inclusion of the language in Section 3(e) which makes it clear that the person who experienced the breach and who is notifying consumers is the one who pays for the credit reports to which the consumer is entitled.

3(d)(B)(iv) requires that the toll-free numbers for major credit reporting agencies be included in the notice. We request that the bill be amended to require those who are sending out breach notifications to more than 5,000 individuals to notify the consumer reporting agencies in advance, so that our members can appropriately prepare to handle the spike in volume. Further, all persons issuing notices must verify the

accuracy of the contact information included. Our members have at times discovered that breach notices issued by others had incorrect toll free numbers listed, which is a disservice to consumers.

### **Definition of Personal Information**

Section 5(7)(A) establishes a definition of the term “personal information.” Having a definition is clearly necessary to ensure that all persons affected by the scope of the bill understand the type of data which must be protected. Our members are concerned with the inclusion of Section 5(7)(B) which allows the FTC to alter this definition. We believe the definition as proposed is adequate and should be set by Congress. The FTC could make a determination that a new element of data is now included under the definition and in doing so unintentionally cause extraordinary expense for affected persons. As written the FTC is not required to validate their reasons for changing the definition, nor are they required to determine the financial or product impact such a change would have.

### **Enforcement**

CDIA continues to believe that enforcement of the statute by state attorneys general should be comparable to the FCRA provision which allows them to sue for actual or statutory damages of \$1,000 for each negligent or willful violation (see FCRA Section 621(c)(1)(B)). We believe a cap on damages is also appropriate and that compliance with the provisions of this Act should be tied to a “reasonable procedures” standard.

## **Uniform National Standard**

As discussed above, CDIA applauds the inclusion of language in Section 6 which proposes to preempt additional state actions. Our members believe that absolute uniform standards are critical if this bill is to become law and we are happy to provide additional input on the current provision, which appears to be construed too narrowly.

## **Conclusion**

Again, thank you very much for the opportunity to testify. I am happy to address any questions that you may have.