STATEMENT OF

STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION

BEFORE THE

Energy and Commerce Committee

Subcommittee on Commerce, Trade and Consumer Protection

House of Representatives

ON

Legislative Hearing on H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P Act

Tuesday, May 5, 2009

Chairman Rush, Ranking Member Radanovich, and members of the Subcommittee, thank you for this opportunity to appear before you today. My name is Stuart Pratt, 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 250 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.

My comments will focus exclusively on H.R. 2221. H.R. 1319 focuses on issues relating to the practice of making "files from a protected computer available to another computer through a peer-to-peer file sharing program" and CDIA's members are not involved in these types of activities.

Scope of H.R. 2221

We applaud the introduction of H.R. 2221. Section 2 of H.R. 2221 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. 2221 requires these same persons to comply with specific requirements of the Act where they discover a breach of security relating to personal information. Section 2(c) of H.R. 2221 proposes to impose certain unique duties regarding "information brokers" as that term is defined in Section 5(6).

CDIA's members agree that sensitive personal information should be protected. They also agree that consumers should receive breach notices when there is a significant risk of them becoming victims of identity theft. Our members agree with the Federal Trade Commission recommendation offered in multiple testimonies on the Hill and via their joint Task Force report issued along with the Department of Justice that if a federal statute is to be enacted, it should be a true national standard and that it should focus on safeguarding sensitive personal information and notifying consumers when a breach has occurred which exposes the consumer to a significant risk of becoming a victim of identity theft. In the absence of a national standard, our members have worked constructively with state legislatures to create security breach notification laws, data security laws and laws which define the crime of identity theft.

We believe that in general the data security and breach notification provisions of H.R. 2221 would be most effective if they were better aligned with requirements found in other current federal laws. From our experience, statutory alignment is a key to ensuring that all who are affected by the Act are successful in complying with new duties under DATA and also with their current duties found in other laws such as the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act. We also believe it is important to ensure that requirements do not harm the operation of products, which is a policy result none of us would wish to see.

Let me now discuss some of the ways in which duties under H.R. 2221 interplay with existing duties found in other laws.

Information Brokers & Consumer Reporting Agencies

In Section 5(6) of H.R. 2221, the term "information broker" is defined. It is a broad definition, and information brokers have specific, unique duties under the Act. Absent aligning this bill with other current laws, our members' products will be affected.

This bill would require information brokers to: have reasonable procedures to verify the accuracy of personal information; provide consumers with access to these data; and ensure a system by which a consumer can dispute information and to correct disputed information where it is found to be inaccurate.

All of our members operate consumer reporting agencies as this term is defined by the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*) and produce data products defined as "consumer reports." Consumer reports are used to make determinations of a consumer's eligibility for a service or product. The FCRA establishes duties of accuracy, access and correction as it relates to consumer reports produced by consumer reporting agencies. Our members agree that where data is used to make a decision regarding a consumer's eligibility for a product or service, the consumer should have these rights, which have been available to all of us as consumers since 1970.

Since there are similar duties under the FCRA (consumer reporting agencies) and the DATA (information brokers), we propose that the definition of "information broker" should be amended to exclude a "consumer reporting agency" as that term is defined in the FCRA. We appreciate the inclusion of Section (c) (3) (C) which attempts to address our concern, but we believe that since the FCRA's duties are well understood and well established and the FTC already has direct enforcement powers under the FCRA with regard to the practices of consumer reporting agencies, that a clear exemption for consumer reporting agencies from the definition of information broker is the most effective approach.

Fraud Prevention Tools – Access and Correction Duties

Our members produce best-in-class fraud prevention tools and, due to the breadth of the definitions of "personal information" and "information broker," these products are

affected by the duty to provide access and correction. We appreciate the inclusion of Section 2(c)(3)(B)(iii)(I) & (II), which allows an information broker to limit access to information which otherwise must be disclosed. It is important to ensure that the "recipe" for fraud prevention tools is not disclosed. Unlike consumer reports regulated under the FCRA, fraud prevention tools are not used to stop a transaction or to make a decision about a consumer, but only to ensure that a consumer is properly identified in a transaction. We believe that Section (c)(3)(B)(iii)(II) would be less ambiguous if the decision to not disclose was not tied to an information broker having to decide whether or not disclosure would compromise the fraud prevention tool. We suggest that the phrase "that would be compromised by such access." be struck to ensure that fraud prevention tools are protected. Similarly, we believe that FTC Rulemaking in Section (c)(3)(B)(iv) could inhibit the development of these tools, as well.

Fraud Prevention/Investigative/Location Tools – Verification of Accuracy

While Section (c)(3)(B)(iii) allows an information broker, under certain circumstances, to not disclose personal information to a consumer, the section does exempt an information broker's fraud prevention tool from the duty to verify accuracy found in Section (c)(3)(A). Consumer reports are used to make decisions about a consumer's eligibility for a product or service. Because of this a consumer reporting agency must use "reasonable procedure to ensure maximum possible accuracy" standard when producing consumer reports. In contrast, a fraud prevention tool is not used to stop a transaction and in fact it is built based on the premise that fraud is not easily identified. Fraud tools are

designed to identify the possibility of fraud. To apply an accuracy standard to fraud prevention tools is unworkable since these tools are designed to warn a lender or utility for example, of the possibility of fraud. Fraud prevention tools consider how data has been used in previously identified cases of fraud and employ many other relational strategies. We urge Section (c)(3)(B)(iii) to be expanded to apply to Section (c)(3)(A) as well as to (B). We are also concerned about many investigative tools used by law enforcement and location tools used, for example, in the enforcement of child support. These investigative and location tools are build to help identify possible connections that will lead to the right person. As is the case with fraud prevention tools, imposing an accuracy standard is unworkable.

Data Security Requirements

Section 2 of H.R. 2111 establishes a requirement that all persons of a certain type which possess personal information must secure the data. Our members agree that data security is essential.

Our members operate consumer reporting agencies regulated by the FCRA and also operate financial institutions as defined by the Gramm-Leach-Bliley Act (Pub. L. 106-102). In addition to these specific statutes which impose data security requirements, every business in this country has to consider the implications of the Federal Trade Commission's enforcement efforts regarding data security where they have been successful in asserting that lax practices are likely unfair, or deceptive or both. Further,

data breaches have resulted in a range of private actions against companies that had inadequate security practices and thus this case law also informs the thinking of all companies which possess sensitive personal information.

Due to the extensive data security requirements already imposed on our members via both of these laws (and regulations therein) and the context of legal actions taken, we believe that consumer reporting agencies and financial institutions should be excluded from the requirements of Section 2 of H.R. 2111. We agree that because of the breadth of the application of H.R. 2111 that there is the need for the inclusion of Section 2(a)(3). This provision is important and helps to account for unanticipated results of the bill, but where we can identify specific instances where protections already exist as is the case for GLB and FCRA we do not believe an FTC determination is necessary and thus financial institutions and consumer reporting agencies should be specifically excluded from the requirements of Section 2.

Data Breach Notification Requirements

Section 3 of H.R. 2111 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 there should be an effective risk-based trigger for the disclosure of notices is necessary and believes that the phrase “significant risk if identity theft” sets the right standard. We also agree that there should be specific exceptions for data which is encrypted or otherwise rendered unreadable or indecipherable.

Since CDIA members operate consumer reporting agencies defined by the FCRA and also often as financial institutions as defined by the Gramm-Leach-Bliley Act we proposed that these two entities be excluded from the data breach requirements of this bill since they are already required to comply with the breach notification requirements of other laws.

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. 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.

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, etc. 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. 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

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.