STATEMENT OF STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION

WASHINGTON, D.C.

Legislative Hearing on S. 3742, the Data Security and Breach Notification Act of 2010

Committee on Commerce, Science and Transportation
United States Senate

Wednesday, September 22, 2010

Chairman Rockefeller, Ranking member Hutchison and members of the committee, thank you for this opportunity to appear before you today to discuss S. 3742, the Data Security and Breach Notification Act of 2010. For the record, my name is Stuart K. Pratt and I am president and CEO of the Consumer Data Industry Association.[1] My testimony will focus on:

- The value and importance of the data systems and analytical tools our members produce.
- The sufficiency of current laws which regulate our members' products.
- Comments on S. 3742.

CDIA MEMBERS' DATA AND TECHNOLOGIES HELP BOTH THE PUBLIC AND PRIVATE SECTORS TO MANAGE RISK AND PROTECT CONSUMERS

Whether it is counter terrorism efforts, locating a child who has been kidnapped, preventing a violent criminal from taking a job with access to children or the elderly or ensuring the safety and soundness of lending decisions our members' innovative data bases, software and analytical tools are critical to how we manage risk in this country, ensure fair treatment and most importantly, how we protect consumers from becoming victims of both violent and white-collar crimes of all types.

[1] CDIA, as we are commonly known, is the international trade association representing over 300 consumer data companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services, systems for insurance underwriting, skip-tracing tools, law enforcement investigative systems and also collection services.

Following are examples of how our members' products, software and databases bring material value to consumers and our country:

- Helping public and private sector investigators to prevent money laundering and terrorist financing.
- Ensuring lenders have best-in-class credit reports, credit scoring technologies, income verification tools and data on assets for purposes of making safe and sound underwriting decisions so that consumers are treated fairly and products make sense for them.
- Bringing transparency to the underlying value of collateralized debt obligations and in doing so ensuring our nation's money supply is adequate which militates against the possibility and severity of economic crises.
- Enforcing child support orders through the use of sophisticated location tools so children of single parents have the resources they need.
- Assisting law enforcement and private agencies which locate missing and exploited children through location tools.
- Researching fugitives, assets held by individuals of interest through the use of investigative tools which allow law enforcement agencies tie together disparate data on given individuals and thus to most effectively target limited manpower resources.
- Witness location through use of location tools for all types of court proceedings.
- Reducing government expense through entitlement fraud prevention, eligibility determinations, and identity verification.
- Making available both local and nationwide background screening tools to ensure,

for example, that pedophiles don't gain access to daycare centers or those convicted of driving while under the influence do not drive school buses or vans for elder care centers.

- Helping a local charity hospital to find individuals who have chosen to avoid paying bills when they have the ability to do so.
- Producing sophisticated background screening tools for security clearances, including those with national security implications.
- Improving disaster assistance responses through the use of cross-matched databases that help first-responders to quickly aid those in need and prevent fraudsters from gaming these efforts for personal gain.

Not only do our members' technologies and innovation protect us and ensure that we are managing risk in this country, but they reduce costs and labor intensity. Risk management is not merely the domain of the largest government agencies or corporations in America, it is available to companies of all sizes thanks to our members' investments. Consider the following scenarios:

Scenario 1 – Effective Use of Limited Resources

The following example was given during a Department of Homeland Security meeting on use of data by the department:

"One extremely well-known law enforcement intelligence example from immediately post 9/11 was when there was a now well-publicized threat…that there might be cells of

terrorists training for scuba diving underwater bombing, similar to those that trained for 9/11 to fly – but not land – planes. How does the government best acquire that? The FBI applied the standard shoe- leather approach – spent millions of dollars sending out every agent in every office in the country to identify certified scuba training schools. The alternative could and should have been for the Federal government to be able to buy that data for a couple of hundred dollars from a commercial provider, and to use that baseline and law enforcement resources, starting with the commercial baseline."

Scenario 2 – Lowering Costs/Expanding Access to Best-in-Class Tools

One commercial database provider charges just $25 for an instant comprehensive search of multiple criminal record sources, including fugitive files, state and county criminal record repositories, proprietary criminal record information, and prison, parole and release files, representing more than 100 million criminal records across the United States. In contrast, an in-person, local search of one local courthouse for felony and misdemeanor records takes 3 business days and costs $16 plus courthouse fees. An in-person search of every county courthouse would cost $48,544 (3,034 county governments times $16). Similarly, a state sexual offender search costs just $9 and includes states that do not provide online registries of sexual offenders. An in-person search of sexual offender records in all 50 states would cost $800.

Scenario 3 – Preventing Identity Theft & Limiting Indebtedness

A national credit card issuer reports that they approve more than 19 million applications for credit every year. In fact they process more than 90,000 applications every day, with an approval rate of approximately sixty percent. This creditor reports that they identify one fraudulent account for every 1,613 applications approved. This means that the tools our members provided were preventing fraud in more than 99.9 percent of the transactions processed. These data also tell us that the lender is doing an effective job of approving consumers who truly qualify for credit and denying consumers who are overextended and should not increase their debt burdens.

CURRENT LAWS REGULATING OUR MEMBERS ARE ROBUST

The United States is on the forefront of establishing sector-specific and enforceable laws regulating uses of personal information of many types. The list of laws is extensive and includes but is not limited to the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*), The Gramm-Leach-Bliley Act (Pub. L. 106-102, Title V), the Health Insurance Portability and Accountability Act (Pub. L. 104-191), and the Drivers Privacy Protection Act (18 U.S.C. 2721 *et seq.*).

Following are more probative descriptions of some of these laws, the rights of consumers and also the types of products that fall within the scope of the law.

Fair Credit Reporting Act

Key to understanding the role of the FCRA is the fact that it regulates any use of personal information (whether obtained from a public or private source) defined as a consumer report. A consumer report is defined as data which is gathered and shared with a third party for a determination of a consumer's eligibility for enumerated permissible purposes. This concept of an eligibility test is a key to understanding how FCRA regulates an extraordinarily broad range of personal information uses. The United States has a law which makes clear that any third-party-supplied data that is used to accept or deny, for example, my application for a government entitlement, employment, credit (e.g., student loans), insurance, and any other transaction initiated by the consumer where there is a legitimate business need. Again, this law applies equally to governmental uses and not merely to the private sector and provides us as consumers with a full complement of rights to protect and empower us. Consider the following:

• The right of access – consumers may request at any time a disclosure of all information in their file at the time of the request. This right is enhanced by requirements that the cost of such disclosure must be free under a variety of circumstances including once per year upon request, where there is suspected fraud, where a consumer is unemployed and seeking employment, when a consumer places a fraud alert on his or her file, or where a consumer is receiving public assistance and thus would not have the means to pay. Note that the right of access is absolute since the term file is defined in the FCRA and it includes the base information from which a consumer report is produced.

• The right of correction – a consumer may dispute any information in the file. The right of dispute is absolute and no fee may be charged.

• The right to know who has seen or reviewed information in the consumer's file – as part of the right of access, a consumer must see all "inquiries" made to the file and these inquiries include the trade name of the consumer and upon request, a disclosure of contact information, if available, for any inquirer to the consumer's file.

• The right to deny use of the file except for transactions initiated by the consumer – consumers have the right to opt out of non- initiated transactions, such as a mailed offer for a new credit card.

• The right to be notified when a consumer report has been used to take an adverse action. This right ensures that I can act on all of the other rights enumerated above.

• Beyond the rights discussed above, with every disclosure of a file, consumers receive a notice providing a complete listing all consumer rights.

• Finally, all such products are regulated for accuracy with a "reasonable procedures to ensure maximum possible accuracy" standard. Further all sources which provide data to consumer reporting agencies must also adhere to a standard of accuracy which, as a result of the FACT Act, now includes new rulemaking powers for federal agencies.

Gramm-Leach-Bliley Act

Not all consumer data products are used for eligibility determinations regulated by the FCRA. Congress has applied different standards of protection that are appropriate to the use and the sensitivity of the data. We refer to these tools as Reference, Verification and Information services or RVI services. RVI services are used not only to identify fraud, but also to locate and verify information for the public and private sectors.

Fraud prevention systems, for example, aren't regulated under FCRA because no decision to approve or deny is made using these data. Annually businesses conduct an average more than 2.6 billion searches to check for fraudulent transactions. As the fraud problem has grown, industry has been forced to increase the complexity and sophistication of the fraud detection tools they use. While fraud detection tools may differ, there are four key models used.

- **Fraud databases** – check for possible suspicious elements of customer information. These databases include past identities and records that have been used in known frauds, suspect phone numbers or addresses, and records of inconsistent issue dates of SSNs and the given birth years.
- **Identity verification products** – crosscheck for consistency in identifying information supplied by the consumer by utilizing other sources of known data about the consumer.

Identity thieves must change pieces of information in their victim's files to avoid alerting others of their presence. Inconsistencies in name, address, or SSN associated with a name raise suspicions of possible fraud.

- **Quantitative fraud prediction models** – calculate fraud scores that predict the likelihood an application or proposed transaction is fraudulent. The power of these models is their ability to assess the cumulative significance of small inconsistencies or problems that may appear insignificant in isolation.
- **Identity element approaches** – use the analysis of pooled applications and other data to detect anomalies in typical business activity to identify potential fraudulent activity. These tools generally use anonymous consumer information to create macro-models of applications or credit card usage that deviates from normal information or spending patterns, as well as a series of applications with a common work number or address but under different names, or even the identification and further attention to geographical areas where there are spikes in what may be fraudulent activity.

The largest users of fraud detection tools are financial businesses, accounting for approximately 78 percent of all users. However, there are many non- financial business uses for fraud detection tools. Users include:

- **Governmental agencies** – Fraud detection tools are used by the IRS to locate assets of tax evaders, state agencies to find individuals who owe child support, law enforcement to assist in investigations, and by various federal and state agencies for employment background checks.

• **Private use** – Journalists use fraud detection services to locate sources, attorneys to find witnesses, and individuals use them to do background checks on childcare providers.

CDIA's members are also the leading location services providers in the United States. These products are also not regulated under FCRA since no decision is based on the data used. These services, which help users locate individuals, are a key business-to-business tool that creates great value for consumers and business alike. Locator services depend on a variety of matching elements. Consider the following examples of location service uses of a year's time:

- There were 5.5 million location searches conducted by child support enforcement agencies to enforce court orders. For example, the Financial Institution Data Match program required by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PL 104-193) led to the location of 700,000 delinquent individuals being linked to accounts worth nearly $2.5 billion.

- There were 378 million location searches used to enforce contractual obligations to pay debts.

- Tens of millions of searches were conducted by pension funds (location of beneficiaries), lawyers (witness location), blood donors organizations (blood

supply safety), as well as by organizations focused on missing and exploited children.

- There were 378 million location searches used to enforce contractual obligations to pay debts.

- Tens of millions of searches were conducted by pension funds (location of beneficiaries), lawyers (witness location), blood donors organizations, as well as by organizations focused on missing and exploited children.

Clearly RVI services bring great benefit to consumers, governmental agencies and to businesses of all sizes. Laws such as the Gramm-Leach-Bliley Act and Fair Credit Reporting Act are robust, protective of consumer rights, but also drafted to ensure that products used to protect consumers, prevent fraud and to locate individuals are allowed to operate for the good of consumers and business.

S. 3742 – THE DATA SECURITY AND BREACH NOTIFICATION ACT OF 2010

Now let me turn to S. 3742. CDIA is pleased to provide our comments on the bill as a whole and in particular on provisions which propose to regulate and entity called an "information broker."

Let me start by stating unequivocally that CDIA's members agree that sensitive personal information should be protected. CDIA agrees 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. Though our members support these goals, we believe provisions of S. 3742 need improvement and it is also our view that the provisions which propose to regulate an entity defined as an "information broker" should be struck. Following are more detailed comments regarding the bill.

Information Broker

This section of the bill imposes accuracy, access and correction standards to a certain type of entity defined as an information broker. It is still unclear to us on what industry the information broker provisions are intended to focus. We believe the provision should be struck from the bill and encourage the focus of this bill to be on data security and breach notification. Following are concerns we have with this provision:

Double Jeopardy with FCRA: As discussed above, consumer reporting agencies which compile and maintain data for purposes of producing consumer reports which are used

for eligibility determinations are regulated under the FCRA. These products are subject to accuracy, access and correction standards. The definition of "information broker" does not expressly exclude consumer reporting agencies (FCRA). Rather than fully exempt consumer reporting agencies, the bill proposes an exception which establishes an "in compliance with" test. In essence a consumer reporting agency is regulated as a consumer reporting agency under FCRA and also as an "information broker" under this proposal where the consumer reporting agency is not in compliance with FCRA. CDIA appreciates the effort to exclude consumer reporting agencies via Section 2(b)(3)(C) but we oppose this approach to an exception. By contrast in Section 2(c) the bill unequivocally exempts certain service providers. Consumer reporting agencies as defined under FCRA should not be considered information brokers in any context.

Interference with Fraud Prevention, Identity Protection and Location Services -
RVI products such as those designed for fraud prevention and location are produced under laws such as the Gramm-Leach-Bliley Act and Section 5 of the Federal Trade Commission Act. financial institutions (GLB). The definition of information broker does not exclude financial institutions regulated under GLB. Therefore products developed under the data-use limitations found in GLB Title V, Section 502(e) are adversely affected by the information broker provision.

Neither a product developed for fraud prevention nor location should be subject to accuracy, access and correction standards since neither product is used to deny or

approve an application, etc. If they were designed for the purpose of making decisions about a consumer's eligibility, then they would already be regulated under the FCRA.

Consider the effect of the information broker duties on fraud tools. While Section 2(b)(3)(A)(ii) provides a limited exception for fraud databases consisting of inaccurate information, the exception is not sufficient, though we do applaud the effort to try and address the problem of imposing an accuracy standard on fraud tools. Fraud prevention tools are built based on data about consumers, data about confirmed fraud attempts, data about combinations of accurate and in accurate data used for fraud attempts and more. Fraud tools are designed to identify transactions or applications that are likely to be fraudulent in order to allow the user to take additional steps to prevent the crime and still process legitimate transactions. The current exception does not appear to address all types of fraud prevention tools used today and further the limitations of the exception impose statutory rigidity that will prevent the design of new tools as the strategies of the criminals change. It is our view that applying an accuracy standard to any aspect of a fraud prevention system that is not used to stop a transaction or used to make a yes-or-no decision does not make sense.

Similarly it is wrong to subject fraud prevention tools to be subject to an access and correction regime. While Section 2(b)(3)(iv) attempts to exclude fraud prevention tools from the duty to disclose (and therefore any right to dispute data), the exception is tied to a variety of tests such as where the use of the tool would be "compromised by such access." It is our view that fraud tools, because they are not used to make decisions,

should be absolutely excluded from duties to disclose. If details of a fraud tool are disclosed it is akin to disclosing the recipe for fraud prevention. The fact that the exception to disclosure is not absolute leaves open the risk that a tool will have to be disclosed which simply reduces the value of fraud prevention tools which are protecting consumers. This result works against the premise of the bill which is to protect consumer's from crime, particularly identity theft.

As discussed in this testimony, location services are materially important to how risk is managed. These tools are not designed to be used for decision making and thus are not regulated under the FCRA, which already regulates all data used for eligibility decisions (including the imposition of accuracy, access and correction rights). Location services cannot have an accuracy standard applied to them as this bill would propose. The tools are about helping local law enforcement investigate crimes, attorneys to locate witnesses, and federal agencies to cross match data in the pursuit of kidnappers, etc., nonprofit hospitals to collect debts from patients who have the ability to pay but refuse to do so and in the enforcement of child support orders. These systems are designed to, for example, help a user identify possible connections between disparate records and ultimately possible locations for the subject of the search. Measuring the quality of the possible connections is not akin to an accuracy standard, nor should an accuracy standard be applied to "possible matches." Further, providing access to a database for purposes of error correction could affect the quality of the systems since matches are sometimes based on combinations of accurate and inaccurate data. Ultimately, the data is not used

to deny a consumer access to goods or services and thus CDIA opposes the application of accuracy, access and correction duties to these fraud prevention systems or RVI services.

Information Brokers and Audit Logs

Section 2(b)(4) establishes a duty for information brokers to maintain an audit logs for accessed or transmitted information. Such a duty is appropriate to a database used for eligibility and thus is appropriate under the FCRA. CDIA urges the committee to reject the application of such a concept to data systems which are not used to determine eligibility. Audit systems impose costs on business both small and large. Based on even the current limited exceptions to information broker duties to ensure accuracy and provide access and correction, it appears that an audit log must be maintained.

Harmonizing Data Security Standards

While CDIA's members support the creation of a national standard for data security, we believe that it is also critical that such a standard not interfere with the operation of other federal laws which already exist. To accomplish this, additional work must be done to fine-tune the exception in the current bill. Allowing a company to be exempt from a data security standard only when it is "in compliance with" a similar standard found in another law imposes two sets of duties, two sets of costs and two sets of liability on that company. For CDIA's largest and smallest businesses this is an unnecessary burden. For our smallest businesses this duty likely increases the costs of the Errors and Omissions insurance policies which have to cover this dual liability risk. We urge the committee to

adjust the exception so that is not an "in compliance with" test and to instead use a "subject to" test.

FTC Website for Publishing Breaches

The bill requires covered entities to report any breach to the Federal Trade Commission and further it requires the FTC to publish the fact of these breaches on a website. The fact that the bill has a breach notification standard ensures that all affected consumers are notified when there's a risk of being harmed by the breach. CDIA agrees that notices to consumers who are at significant risk of becoming a victim of identity theft makes sense. However, publishing the names of companies does not. A company could have deployed best-in-class technologies and procedures and still have been affected by the criminal actions of rogue employees or new technologies used by an organized gang. The business or governmental agency which suffered the breach due to criminal actions is a victim of a crime. The publication of the names of those who have suffered a breach would imply that the business did not work hard, did not care about their customers and by these implications, the publication of names imposes a guilty verdict on their good names, no matter how hard the business had worked to protect the data and no matter how responsible they were in working to protect their customers following a breach. We urge the committee to strike this provision.

Preemption

CDIA applauds the intent of this bill to set uniform national standards for data security and breach notification. However, the exception to this preemptive standard, which attempts to preserve state laws, swallows the rule. Congress should not enact a fifty-first law. A true national standard will benefit consumers because they will enjoy the benefits of this standard no matter where they live.

Enforcement

CDIA believes that the preservation of uniform national standards for data security and breach notification are best achieved by limiting the enforcement of the law to a single federal agency, in this case the Federal Trade Commission. By extending the enforcement powers to state attorneys general, which in turn can designate any other "official or agency of the state" to bring enforcement actions, as well will not increase a company's desire to comply but will lead to experimental litigation that may simply diminish the true national standard the bill sets out to establish. Further, the same issues and same facts of a given incident should not be open for multiple lawsuits. CDIA operates an errors and omissions insurance program for its small-business members and it is our experience that policy costs will rise where there is additional exposure. Even larger members who self-insure simply have to set aside more money for litigation rather than investing it in research and development. We urge the committee to limit enforcement to the FTC.

CONCLUSION

We thank you again for giving us this opportunity to testify. It is only through such dialogue that good laws are enacted. We welcome continued dialogue on S. 3742 and I'm happy to answer any questions.