STATEMENT OF STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION

WASHINGTON, D.C.

ON

"Privacy and Data Security: Protecting Consumers in a Modern World

Committee on Commerce, Science and Transportation

United States Senate

Wednesday, June 29, 2011

Chairman Rockefeller, Ranking member Hutchison and members of the committee, thank you for this opportunity to appear before you today. For the record, my name is Stuart K. Pratt and I am president and CEO of the Consumer Data Industry Association. My testimony will focus on:

- The importance to consumers of the data systems and analytical tools our members produce.
- How current laws which regulate our members' products already protect consumers.
- Separating privacy issues from the important work of establishing a national standard for securing sensitive personal information and data breach notification.
- Aligning new law with existing laws.
- Creating a truly national standard.

CDIA MEMBERS' DATA AND TECHNOLOGIES PROTECT CONSUMERS AND HELP US BUSINESSES MANAGE RISK

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.

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 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' PRODUCTS PROTECT CONSUMERS AND 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.

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.

A NATIONAL DATA SECURITY AND DATA BREACH NOTIFICATION STANDARD IS A SEPARATE MATTER FROM PRIVACY

Let me start by stating unequivocally that CDIA's supports the creation of a national standard for both securing sensitive personal information and notification of consumers when there has been a breach of that data. Our position is in agreement 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. This committee can play a leading role in ensuring that such a standard is set. This committee can also ensure that privacy issues are not confused with the core consumer protections found in a proposal that focuses on data security and breach notification.

Provisions found in some bills that create national standards for security and notification also impose accuracy, access and correction standards on a certain type of entity defined as an information broker. We believe that provisions such as these should be struck because they do not advance the cause of protecting data, and they interfere with how other current laws regulate the development of products which do protect consumers. Consider the following:

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. The definition of information broker often 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 information broker provisions.

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. Further accuracy, access and correction standards are not relevant to the important work of this Committee to establish a national standard for securing sensitive personal information and notifying consumers when there is a breach of such data.

Consider the effect of applying an accuracy standard to fraud tools. Ironically doing so would lead to interference with the very tools that help protect consumers against the risks posed by failures to protect sensitive personal information. Fraud prevention tools are built based on data about consumers, data about confirmed fraud attempts, data about combinations of accurate and inaccurate 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.

Similarly it is wrong to subject fraud prevention tools to an access and correction regime. If details of a fraud tool are disclosed it is akin to disclosing the recipe for fraud prevention. This result works against a bill which is focused on protecting consumers from crime, particularly identity theft.

As discussed in this testimony, location and investigative research services are materially important to how risk is managed. They 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). Such services are, for example, designed to 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.

Accuracy, access and correction duties are best left to future debates about privacy, but they have no relevance to data security and breach notification.

ALIGNING THE OPERATION OF NEW AND CURRENT LAW

As discussed above, by not including privacy issues (information brokers/accuracy/access/correction) in a data security and notification bill, the committee avoids many problems with the operation of effective federal laws that are on the books today (e.g. FCRA, GLB, HIPAA, DPPA, etc.). Further the committee's bill should not create overlapping burdens where U.S. companies are already in compliance with a security breach notification or security standard for sensitive personal information. For example, financial institutions which are subject to the data security standards of the Gramm-Leach-Bliley Act and also federal agency guidance regarding data breach

notification should be fully exempted from the bill.

THE IMPORTANCE OF A NATIONAL STANDARD

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. Such a standard also benefits U.S. businesses of all sizes because they can then be successful in the goal they all share and that is to protect consumers' sensitive personal information by building data security into their entire enterprise and to notify consumers where there is a significant risk of identity theft.

CONCLUSION

This committee has a number of important opportunities:

- To fill an important gap in current law by ensuring that all U.S. businesses which are not already subject to a data security duty for sensitive personal information are in the future.
- To harmonize the 48 state data breach notification duties and in doing so create much needed uniformity.
- To exclude privacy issues which are not relevant to data security and breach notification.
- To avoid creating law which interferes with the operation of current laws already on the books.
- To create an effective national standard for securing sensitive personal information and data breach notification.

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