STATEMENT OF

STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION

BEFORE THE

Senate Banking Committee

ON

Cybersecurity and Data Protection in the Financial Services Sector

Tuesday, June 21, 2011

Chairman Johnson, Ranking Member Shelby, and members of the Committee, 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 on cybersecurity and data protection in the financial sector.

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.

You have asked us to address a number of topics in our testimony. Let me start with an overview of some of the most relevant laws and regulations which apply to our members' products and services.

DATA SECURITY

The Senate Banking Committee has a clear record across many Congresses of oversight of the financial services sector's efforts to secure sensitive personal information. Let me describe just a few of these efforts.

One of the most notable and prescient actions of the Committee was the 1999 passage of Title V of the Gramm-Leach-Bliley Act, signed into law by President Clinton. While Title V established a number of new duties relative to how data transfers occur in the financial services sector, most notable for today's hearing was the direction given to bank regulatory agencies and the Federal Trade Commission in section 501 to develop regulations regarding the security of nonpublic personal information.

The FTC's explanation of the Safeguards Rule, which implements the security requirements of the GLB Act, speaks to the breadth of the rule's application and what is required of any person who must comply:

"[It] requires financial institutions to have reasonable policies and procedures to ensure the security and confidentiality of customer information. The "financial institutions" covered by the Rule include not only lenders and other traditional financial institutions, but also companies providing many other types of financial products and services to consumers. These institutions include, for example, payday lenders, check-cashing businesses, professional tax preparers, auto dealers engaged in financing or leasing, electronic funds transfer networks, mortgage brokers, credit counselors, real estate settlement companies, and retailers that issue credit cards to consumers.

The Rule is intended to be flexible to accommodate the wide range of entities covered by GLB, as well as the wide range of circumstances companies face in securing customer information. Accordingly, the Rule requires financial institutions to implement a written information security program that is appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it

handles. As part of its program, each financial institution must also: (1) assign one or more employees to oversee the program; (2) conduct a risk assessment; (3) put safeguards in place to control the risks identified in the assessment and regularly test and monitor them; (4) require service providers, by written contract, to protect customers' personal information; and (5) periodically update its security program."

It is hard to overstate the effects that this action has had on the security of the flows of sensitive personal information in the United States. CDIA's members operate as financial institutions under GLB and thus comply with the Safeguards Rule. The model that this Committee established more than a decade ago has withstood the test of time. It should operate as a framework for other committees as they consider establishing a similar data security duty.

Of particular importance to the CDIA is that the Senate Banking Committee had the foresight to ensure that data security was not a hard-coded statutory prescription. Risks change over time and so too must the strategies used to mitigate these risks. The Committee also recognized that those who have a duty to comply will vary in terms of size, complexity and even the types of data retained. Because of this, the Committee built into the statute direction for regulators to take into consideration these factors when designing the rule and measuring how each person implements its requirements. This "regulatory flexibility act like" approach has been critical to ensuring strong security, by not dictating a single solution or approach to security threats, thus leaving our members' security experts the creative room to secure data assets against threats. At the same time, its flexibility is not a statutory and regulatory regime which drives small- and medium-sized businesses out of the marketplace.

The GLB Safeguards Rules are also designed to be administratively enforced, which we believe has ensured that national uniformity has not been impaired by private actions that could create a circuit-by-circuit compliance nightmare for U.S. businesses operating on a super-regional or nationwide basis. This is not to say, however, that such laws are not enforceable. For financial institutions subject to regulatory examination by bank agencies, compliance with the GLB Safeguards Rule is an annual event measured with prudence and care. For persons not subject to bank agency examinations, the Federal Trade Commission has proven itself to be an able agency in many ways. First, it has sought to encourage successful compliance through education. CDIA applauds this education-first approach which compliments the Association's own training programs on this subject. FTC enforcement actions have focused on both smaller and larger institutions, and consent orders have informed the broader community regarding approaches to compliance and FTC expectations. Overall, the GLB Safeguards Rules have operated just as expected, and have ensured that literally trillions of data transmissions and transactions are secure in the context of a healthy and competitive private-sector marketplace.

DISPOSAL OF RECORDS

The Senate Banking Committee's accomplishments are not limited to the enactment of Title V of GLB. In 2003, as part of its extensive oversight of the Fair Credit Reporting Act, the Committee recognized that disposing of sensitive data, whether stored electronically or otherwise, should be addressed. As part of the Fair and Accurate Credit Transactions Act of 2003, Congress amended the Fair Credit Reporting Act by

adding Section 628 [15 USC 1681w] entitled "Disposal of Records." This enactment required the Federal Trade Commission (as well as the Federal banking agencies, NCUA and SEC) to promulgate rules regarding the proper disposal of "consumer information, or any compilation of consumer information, derived from consumer reports…". This duty expanded the concept of proper disposal of records beyond the borders of users of consumer reports who were already subject to duties under the GLB Safeguards rule. This simple, straight-forward duty, it brought tens of thousands of users of data under the new law and specific rules. In doing so, the Committee ensured that sensitive personal data about consumers wasn't simply left in a dumpster, or on the hard drive of a laptop or a hand-held device which was sold without concern for its contents.

CREDENTIALING CUSTOMERS

As a result of this Committee's actions to enact the FCRA (1970) and Title V of GLB (1999), our members have a number of duties to ensure that they know their customers, which is yet another important part of ensuring that a full and complete data security program is in place. Section 607(a) of the FCRA requires our members when operating as consumer reporting agencies to have each customer certify the uses for which they will order consumer reports. Today, this certification process often involves onsite inspections of the customer's offices, reviewing and confirming other credentials such as business licenses, and cross-referencing a prospective customer with the SDN list and other lists administered by the U.S. Treasury's Office of Foreign Assets Control. Further, the GLB Safe Guards Rules issued by bank agencies and the FTC require that proper access controls be in place to protect against unlawful access to nonpublic

personal information. Access control strategies may include details of how passwords are administered, the frequency with which they are changed, how many factors are used to authenticate a legitimate user or the use of technologies to detect possible fraudulent access.

ALIGNING CURRENT LAW WITH CYBERSECURITY PROPOSALS

You have asked us to comment on how proposals, such as the Administration's cybersecurity bill, would affect financial institutions that come under the Committee's jurisdiction.

Clearly because of the leadership of the Senate Banking Committee in establishing data security requirements found in laws such as the FCRA and Title V of GLB, as well as extensive regulations and guidance issued by bank agencies which resulted from these enactments, cybersecurity risks for financial institutions and their customers are far less than would otherwise be the case. Our members already invest heavily in defending against attacks by deploying external resources, leading-edge technologies and internal data security teams with unique core competencies. Some of our largest members also participate in existing information sharing systems such as the Financial Services Information Sharing and Analysis Center.[1]

With the existing legal and regulatory framework in mind, CDIA's members recognize that risks remain, and we do believe it is appropriate for the Administration and the Congress to focus on the ever-changing mix of risks posed by cybersecurity threats. We believe, however, that it is important for new laws not to impinge on frameworks of

[1] ISACs were created as a result of Presidential Decision Directive 63 (PDD-63) in 1998. The directive created a public/private-sector partnership to share information about physical and cyber threats.

law which already establish the necessary focus on data security. Such conflicts are not inevitable and do not have to impede the passage of new national cybersecurity protections.

As an example of how conflicts can be avoided, in place of 47 existing state laws the Administration's bill proposes to protect the American people by creating a single, national standard for how and when a notification should be sent to a consumer if there has been a breach of sensitive personal information that could pose a risk. CDIA is on record testifying as recently as this past week in support of establishing an appropriate national standard for breach notification. We look forward to contributing our experience and expertise to any effort to structure a standard that is uniform and effective for consumers. Part of ensuring that such a standard is effective is to avoid arbitrarily overwriting existing national standards that are effective today -- such as data breach guidance already issued by bank agencies.

The "financial sector" is considered part of the "Nation's critical infrastructure" according to the Administration's May 12, 2011 release. As described above, the financial services industry (including CDIA's members) is heavily regulated in general and specifically with regard to securing sensitive personal information. It is not clear, however, how a "critical infrastructure" designation as determined by the Department of Homeland Security would operate in the context of new agencies such as the Consumer Financial Protection Bureau created by the Dodd Frank Act, and the existing bank agencies that have a leading mission when it comes to data security or even the Federal Trade Commission. Avoiding conflicts is necessary and will require the Senate Banking Committee to proactively engage on the broad topic of cybersecurity to ensure that

current, effective laws, regulations and guidelines for the financial services industry continue to operate coterminous with new data security or data breach notification duties that may be established for other critical infrastructure identified by DHS.

DATA SECURITY AND PRIVACY ARE NOT THE SAME ISSUE

The Senate Banking Committee can also play a vital role in ensuring that the important work of reducing the risks of cybersecurity attacks are not distracted by privacy issues, such as data collection and use practices. Several Congressional committees have delved into this privacy arena in an effort to address the data collection and use practices of so-called "information brokers." It is important to understand that information brokers provide the data services and products necessary for commercial entities.

Our members' products and services are particularly essential to the financial services sector. Financial institutions offering credit need to detect and prevent fraud, including identity theft, and to verify the identities of individuals seeking products and services through increasingly common remote transactions such as through the Internet, over mobile services, through the telephone and even by direct mail. CDIA members also help financial institutions enforce contracts with customers who have the ability to pay, but don't choose to do so. Lenders who must comply with bankruptcy code requirements to cease dunning a consumer who has filed for protection use our members' data tools to comply. USA Patriot Act Section 326 duties demand that financial institutions properly identify their customers and again it is our members' products and

services which help them accomplish this goal and reduce the downstream effects of stolen data and other criminal efforts.

CONCLUSION

Let me conclude with just a few summative points:

1. As stated above, CDIA has been on record for more than a decade in support of establishing uniform, national standards for data security and data breach notification. Action on cybersecurity law could advance this cause.
2. Eliminating possible conflicts between the laudable and important goal of ensuring that the nation is secure from cybersecurity risks and the operation of effective current data security and breach notification laws/regulations/guidance which govern the financial services sector can be accomplished with the involvement of this Committee.
3. Keeping the privacy and data security debates separate is vital to ensuring the continuance of data products and services which contribute to preventing the crimes which arise from data/cybersecurity risks and ensuring that the important work of mitigating cybersecurity risks is not encumbered by policy issues that are not relevant.

Our members again thank you for the opportunity to testify. I am happy to answer any questions.