STATEMENT OF

STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION
WASHINGTON, D.C.

BEFORE THE

Committee on Banking, Housing and Urban Affairs

United States Senate

ON

The financial services industry's responsibilities and role in preventing identity theft and protecting the sensitive financial information of their customers.

September 22, 2005

Chairman Shelby, Senator Sarbanes and members of the Committee, thank you for this opportunity to appear before the Committee on Banking, Housing and Urban Affairs. For the record, I am Stuart Pratt, president and CEO for the Consumer Data Industry Association.

CDIA, as we are commonly known, is an international trade association representing approximately 250 consumer information companies that are the nation's leading institutions in credit and mortgage reporting services, fraud prevention and risk management technologies, tenant and employment screening services, check fraud prevention and verification products, and collection services.

We commend you for holding this hearing on the financial services industry's responsibilities and role in preventing identity theft and protecting the sensitive financial information of their customers. You have asked the CDIA to provide input on a number of issues that have been raised in hearings and legislation this year and in doing so, let me begin with some comments on how the Fair Credit Reporting Act[1] as amended by the Fair and Accurate Credit Transactions Act (PL 108-159) has already contributed materially to the protection of consumers by establishing new duties for the industry and empowering consumers with important new rights. It bears noting that these new duties and rights are all the more effective and easy for consumers to use because they are uniform. We again thank you, Mr. Chairman, Senator Sarbanes and the committee for the successful effort to set these national standards which are necessary to ensure that all consumers continue to enjoy the benefits of a nationwide credit reporting system and

[1] 15 U.S.C. 1681 *et seq.*

ultimately a low-cost, competitive and creative credit market place which helps fuel our nation's continued economic expansion.

FACT Act –

By December 1, 2004 all FACT Act amendments made to the Fair Credit Reporting Act were effective. As of this date our members had brought online a series of nationwide practices which inure particular benefits to consumers who may have concerns about identity theft. These national standards include:

Fraud Alerts – These alerts were voluntarily established by our members in the mid-nineteen nineties. Our members have long believed that fraud alerts strike the right balance for consumers who wish to ensure that a lender is notified of their concerns about identity verification where they have already been or may become victims of the crime of identity theft. Consumers recognize that while these alerts can slow down credit approval processes, alerts do not stop a transaction and, thus, consumers can continue to actively seek out better financial products and services whenever they wish.

The FACT Act created two specific types of fraud alerts. Initial alerts stay on the consumer's report for a minimum of 90 days and will be placed on the report even when there is just a concern that a person might become a victim of identity theft. Creditors which receive this alert must take steps to form a reasonable basis that they have properly identified the consumer. Extended alerts are placed on the consumer's file when he/she presents an identity theft report. This alert remains on the consumer's file for a full seven years and it may include contact

information for a consumer which can be used as part of the identity verification process. Most important to the codification of our members' voluntary fraud-alert practice was that the FACT Act tied the presence of the alerts to specific duties for the recipients. This tying of the consumer reporting agency's duty to place such alerts with a corresponding duty for recipients to form a reasonable basis for identity verification had never previously been established and our members believe that this materially improves upon the fraud alert systems that previously existed.

Active Duty Alerts – Though similar to fraud alerts, active duty alerts may only be used by individuals who are serving in an active duty capacity for our armed services. These alerts remain on the service member's credit report for twelve months and, like fraud alerts, are tied to duties for recipients to take steps necessary to reasonably identify the identity of the applicant before approving the application.

Address Discrepancy Indicators – The FACT Act also established additional protections for consumers in transactions even where a fraud alert might not be involved. Specifically, the FCRA now requires that where a nationwide consumer reporting agency receives a request from a creditor for a credit report and finds that the address submitted by the creditor differs materially from the address on the consumer's credit report, it must indicate to the creditor that this difference exists. Thus, lenders have an additional red flag to consider in attempting to properly validate the identity of an applicant. It is important to note that changes in addresses are not necessarily a strong indication of fraud when one considers that approximately 40 million addresses change each year in this country. Nonetheless, the FACT Act ensured an appropriate focus on address discrepancies by all financial institutions and this adds additional protection for

consumers. While final regulations specifying what a recipient of an address discrepancy indicator must do with them are not completed, no doubt these indicators are being used by lenders today.

Identity Theft Reports – The FACT Act also defined the term "identity theft report." This definition was a key to ensuring that victims of identity theft could avail themselves of a number of rights under the law even if they were having trouble obtaining a traditional police report. The ultimate success of this new definition is in the balance struck by the rules which ensure that such reports can be readily accessed and used by all victims without creating a situation where the reports are hard to verify, misused or easily forged.

Identity Theft Reports and Blocking Fraudulent Data – In year 2000, CDIA's national credit reporting agency members established a nationwide voluntary initiative for victims of identity theft which allowed them to submit a police report and request that fraudulent data be blocked in victims' reports. The FACT Act codified this initiative and expanded it by use of the new "identity theft report" definition. In enacting this national standard, Congress ensured that all victims received the same treatment and that fraudulent data would be removed from victims' reports.

Red Flag Guidelines - Beyond the specific provisions of law discussed above, Congress recognized the need to empower regulators to develop guidance for financial institutions which is intended to encourage the use and accelerate the adoption of a robust combination of

technologies and business rules to further reduce the incidence of identity theft. These guidelines are still under development.

The fact that the provisions just discussed all operate as national standards bears repeating. The Congress was prescient in recognizing that fraud prevention and, in fact, regulation of a nationwide system of credit reporting and credit markets is best handled through uniform national standards. A series of state laws which impede the free flow of information across this country cannot possibly achieve the same benefit for all citizens wherever they may live. We applaud the Congress and the principal sponsors of the FACT Act for the necessary focus on the needs of consumers and identity theft victims through the establishment of national standards of practice.

In closing our discussion of national standards under FCRA, I am reminded of the fact that the FCRA itself remains the only law which directly regulates our members operating as consumer reporting agencies. The national standards reauthorized and established by the FACT Act were critical to our nationwide members and it remains vitally important that our members operating as consumer reporting agencies are regulated under this single set of national standards, law and regulation.

Information Security and Consumer Notification –

Beyond the FACT Act's many new protections and rights for consumers, the security of sensitive personal information held by non-financial institutions has been the focus of debate in a number of House and Senate committees. In fact, this committee was the first to hold hearings

on breaches of sensitive personal information and ultimately there are two key themes on which to focus:

- Ensuring the security of sensitive personal information; and
- Sending consumers meaningful notices of a breach of sensitive personal information when there is a significant risk of identity theft.

Information security and requiring consumer notification if the loss of information poses a significant risk are not new areas of focus for this committee, which has traditionally taken a leadership role on information policy. Most recently enactment of the Gramm-Leach-Bliley Act[2] (GLB), Title V included a requirement[3] that federal agencies write regulations[4] for securing and protecting nonpublic personal information, including taking into consideration when a loss of such information should lead to consumer notification. The FTC published its final rule on May 23, 2002 and they became effective on May 23, 2003.[5]

The discussion of safeguarding sensitive personal information and notifying consumers when there is a substantial risk of identity theft has expanded beyond the boundaries of financial institutions. It is our view that rational and effective national standards should be enacted both for information security and consumer notification as it applies to sensitive personal information, regardless of whether the person is a "financial institution."

[2] 15 U.S.C. 6801-6809 (Financial Privacy).
[3] See Section 501(b) of Title V, PL 106-102.
[4] See 15 U.S.C. 6801(b), 6805(b)(2).
[5] 16 CFR Part 314, Standards for Safeguarding Customer Information; Final Rule.

Safeguarding sensitive personal information – GLB's statutory framework for safeguarding sensitive personal information is equally well-suited to information safeguards for sensitive personal information held by any person not otherwise defined as a financial institution. Under this approach, the FTC would promulgate rules for any non-financial persons just as they did under GLB. To ensure that there is absolute regulatory continuity between the applicable provisions of GLB and rules therein and new information security standards and rules, financial institutions which are compliant with their obligations under GLB should be deemed in compliance with any new requirements. Any new standards for non-financial entities should be substantially similar to those required by the GLB safeguard rule.

Consumer Notification – Consumers should receive notices when their sensitive personal information is breached and there is a significant risk of identity theft. While there are many details which go into creating an effective notification requirement, a fundamental element is making sure that it does not result in either over-notification, or too few notices sent where there is a significant risk to the consumer.

We believe that the general guidance provided this year by FTC Chairman Majoras in her testimony before a number of congressional committees regarding the appropriate "trigger" for a notice is on point. That is that notices should be sent when there is a significant risk of harm. In our view, harm is best defined as significant risk of identity theft. A poorly structured trigger leads to over-notification, which erodes the effectiveness of each subsequent notice sent to a given consumer. If notices are not tied to events that truly pose significant risks they will be ignored by many consumers who may become anesthetized to the importance of them.

Further, consumer reporting agencies as defined under FCRA Section 603(p)[6], are affected by the volume of even legitimate breach notices (in addition to those that result from over-notification). The national systems' contact information is consistently listed in notices going to consumers. If you add up even just a few of the high-profile breaches which have taken place over the course of this year, it is easy to come up with tens of millions notices containing our members' contact information. Thus, we believe that when a breach results in more than 1000 notices to consumers, the company that breached the sensitive personal information should:

- Notify each nationwide consumer reporting agency of this fact and provide the estimated number of notices to be sent;
- Notify each other consumer reporting agency whose contact information will be listed in the notice; and
- Confirm the contact information that should be used for each listed consumer reporting agency. Our members report that there have been times when incorrect telephone numbers have been listed on notices.

A well-reasoned national standard for information security for sensitive personal information, coupled with effective notices where such information is breached by a party can contribute materially to the reduction in risk for all consumers.

Credit Report/File Freeze

You have also asked us to provide background on and discuss our views of the trend in state laws often termed "credit report freeze", "file freeze" or "security freeze". First, it is important to clarify that a freeze is not a fraud alert as enacted by the FACT Act. It is also important to understand how a file freeze operates based on our experience with current state laws.

A fraud alert accompanies a credit report sent to a lender and as such, a lender is notified of the consumer's concern. With a fraud alert, the lender can still process the application, though it will take additional measures to ensure that a consumer is properly identified before doing so. In contrast a file freeze empowers a consumer to request that a consumer reporting agency not provide the credit report for a "new business" transaction such as an application for credit and, thus, the transaction cannot be completed.

File freezes are not absolute and consumers can request that a freeze be lifted temporarily for a period of time (e.g. for thirty days). Depending on when and in what manner the request is received, this temporary lift does not happen instantaneously and consumers have to remember to make their request for a temporary lifting of the freeze to the consumer reporting agency prior to making an application for credit.

All state laws and proposals allow consumer reporting agencies to charge a fee for placing or lifting a freeze (how and where fees are charged varies by state). Our members have viewed the right to charge a fee for the placement of a freeze and for each temporary lifting of a freeze as a

[6] The Fair Credit Reporting Act: 15 U.S.C. 1681 *et seq.*

matter of equity where such laws are enacted. California agreed with this principal when it enacted the first law in the country. Throughout the FACT Act hearings, time and time again this committee heard testimony regarding the value that the credit reporting system brings to individual consumers. Simply put, credit reports lower credit costs, by lowering risk. Credit reports empower consumers and lead to the robust credit economy that benefits all consumers.

In the past several months, federal legislation has been introduced which would codify the right of consumers to freeze the release of their credit reports and /or certain additional sensitive information under certain circumstances. These measures are, S.1408, introduced by Sen. Gordon Smith on July 14, 2005 which was marked up and reported out of the Senate Commerce Committee on July 28, 2005, and S.1336 introduced by Senator Mark Pryor on June 29, 2005 and referred to the Senate Commerce Committee.[7] On July 21, 2005 Senate Banking Committee Chairman Richard Shelby introduced a virtually identical measure as S. 1336.[8] That bill was referred to the Senate Banking Committee.

The federal measures follow significant state activity over the past several years in this area. Currently, twelve states have enacted file freeze laws (California, Colorado, Connecticut, Illinois, Louisiana, Maine, Nevada, New Jersey, North Carolina, Texas, Vermont and

[7] Note that file freezing is only one of a range of issues addressed in this bill.

[8] The following quote by Senator Shelby drawn from the congressional record explains the senator's motivations for the introduction of this bill:

"Mr. President, I rise today to introduce the Consumer Identity Protection and Security Act. This legislation provides consumers the ability to place credit freezes on their credit reports. Mr. President, my sole intent in introducing this legislation is to address a jurisdictional question that has recently arisen with respect to the Fair Credit Reporting Act. I want to make sure that the referral precedent with respect to legislation that amends the Fair Credit Reporting Act, or touches upon the substance covered by that Act, is entirely clear. I believe the Parliamentarian's decision to refer this bill to the Senate Banking Committee establishes that there is no question in this regard and that this subject matter is definitively and singularly in the jurisdiction of the Senate Banking Committee."

Washington). Since 2003, all but approximately ten states have had file freeze measures introduced and though some have rejected the concept, this past year seven states enacted new law. It is expected that there will be significant state activity in this area in 2006.

The state laws vary in terms of substantive scope and operational elements. The measures contain different standards in the following key areas: 1) the circumstances under which consumers may request a freeze ; 2) the extent to which consumer reporting agencies are required to notify other CRA's or entities which report affected information ; 3) the extent to which certain information is exempt from a freeze ; 4) the timetables within which freezes must be imposed or removed ; 5) whether there are limits on amounts that can be charged to freeze or unfreeze reports ; 6) and , the scope of liability for violations of the freeze laws.

Though some file freeze provisions of state laws have been effective for years, our experience with them remains very limited. For example, we estimate that just a little over 9,000 California consumers have made use of the file freeze. With a population of more than 25 million credit-active Americans, this population of frozen credit reports yields no useful information regarding the individual consumer experience. Most state laws are very recent enactments and, thus, we also have no experience with consumers moving in and out of states where the file can and cannot be frozen.

The merits of file freezing have been heatedly debated in many state legislative forums and in media. Some states have in fact rejected file freezes. The consumer reporting industry has often been quoted as expressing concerns that the rigidity of freezes, which operate in stark contrast to

fraud alerts where transactions can continue under a "caution flag." However, it is our view that as the number of state law enactment climbs, disparate state law file freeze provisions will increasingly affect the seamless operation of our nation's credit reporting system which the FACT Act sought to preserve through the reauthorization of existing and establishment of additional national standards. Thus, in the context of significant state legislative activity, an increasing numbers of state file freeze laws, and also a country where 40 million consumers' addresses change each year, with many consumers moving across state lines, we must continue to monitor the risks to our nationwide credit reporting system and engage in an ongoing federal dialogue about how best to preserve the efficiency and economic benefits that were protected first by the enactment of the FACT Act.