COMMENTS OF

THE CONSUMER DATA INDUSTRY ASSOCIATION

September 5, 2007

TO:

The Federal Trade Commission

Regarding:

"SSNs In The Private Sector - Comment, Project No. P075414"

1090 Vermont Avenue, NW, Washington, D.C. 20005
202-371-0910 Phone 202-371-0134 FAX

September 5, 2007

Federal Trade Commission/Office of the Secretary
Room H-135 (Annex K)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: "SSNs In The Private Sector - Comment, Project No. P075414"

To Whom It May Concern:

The Consumer Data Industry Association (CDIA)[1] welcomes the opportunity to comment on "Private Sector Use of Social Security Numbers." CDIA appreciates the efforts of the Task Force to find ways to protect consumers from the pernicious crime of identity theft.

FRAMEWORK CONSIDERATIONS:

CDIA believes it is key to ensure that the framework of thought for a discussion of the private sector's use of the SSN is correct, and we believe that the FTC's own testimony about the importance of Social Security Numbers helps to establish the correct perspective:

> "SSNs play an important role in our economy. With 300 million American consumers, many of whom share the same name, the unique 9-digit SSN is a key identification tool for businesses, government, and others. For example, consumer reporting agencies use SSNs to ensure that the data furnished to them is placed in the correct file and that they are providing a credit report on the correct consumer.[8] Businesses and other entities use these reports in making eligibility and pricing decisions for a variety of products and services, including credit, insurance, home rentals, or employment. Additionally, SSNs are used in locator databases to find lost beneficiaries, potential witnesses, and law violators, and to collect child support and other judgments. SSN databases also are used to fight identity fraud – for example, to confirm that an SSN provided by a loan applicant does not, in fact, belong to someone who is deceased. Federal, state, and local governments rely

[1] CDIA is an international trade association that represents 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, and collection services. As we will discuss below, the legal, secure and protected use of the Social Security Number (SSN) is an important key to the effectiveness of these systems and services.

> extensively on SSNs in administering programs that provide services to consumers, and businesses in many circumstances are required to collect SSNs."[2]

We offer the following additional key points for the FTC's consideration.

I) Consumer Expectations

A) Consumers Expect Data about Themselves to be Accurate

It is no surprise that consumers expect a record which is used for a consequential decision about them to be accurate. This is a generally accepted premise in any fair information practices framework, it is a key duty under the Fair Credit Reporting Act[3] and a point which is driven home by the FTC itself. The social security number is a significant contributor to meeting consumer expectations for accuracy and precision.

Specifically, as will be discussed more fully below, the SSN contributes to database accuracy by helping with the "data matching" process, to help ensure the accuracy of CDIA-member databases. The process of "matching data" applies to three separate and distinct processes, all of which play a major role in accuracy: 1) loading data into a database, to ensure that the incoming data is accurately matched to the right file; 2) extracting data from a database to ensure that the correct file is returned when requested; and 3) matching and integrating data across databases.

As discussed in the FTC's Data Matching study, data matching is not always exact, but utilizes sophisticated software, complex algorithms and years of experience to determine the best way to properly match files. These algorithms can recognize, for example, that slight differences in name (such as the use of a full name in one account vs. the use of a nickname on another account), SSN (such as transposed numbers) and other discrepancies that may be present in the file are still the same person, or are different people.

The Social Security Number plays a vital part in correctly matching data in all of these instances, because, as discussed below, all other potential identifiers fall short: in the U.S., there are 42 million address changes each year, 3 million marriages and divorces with attendant name changes, and there are six million vacation and second homes. Additionally there are 4.5 million Americans who have one of two last names (Smith or Johnson) and 14 million who have one of ten last names. 26.6 million females have one of ten first names and 57.7 million males have one of ten first and last names. The SSN is at present the only practicable way to identify individuals across multiple systems and databases and does not change over time.

B) Consumers Expect Security

i) Businesses will secure data

[2] *Hearing on Protecting the Privacy of the Social Security Number from Identity Theft*: Before the Subcomm. on Social Security of the House Ways and Means, June 21, 2007 (110th Cong.) (Statement of Joel Winston, Associate Director of the Division of Privacy and Identity Protection.)

[3] 15 U.S.C. 1681 *et seq.*

Consumers expect that businesses will take steps to ensure that sensitive data about them is not compromised. The SSN is one of a number of identifying elements which are considered sensitive when taken in total. As CDIA President and CEO Stuart K. Pratt testified before the Senate Banking Committee in 2005, CDIA believes that all companies who hold sensitive personal information, including SSNs and other data, should be required to secure that information, regardless of whether they are financial institutions or not:

"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."

Therefore, a discussion of the uses of the SSN in the private or public sector should be set into the context of a need to for sensitive information to be secure. Securing data is an effective approach to protect consumers and caution needs to be taken not to limit legitimate uses of the SSN by the private sector under the mistaken belief that limiting uses of the SSN will reduce fraud or force business to use "better" systems for identification.

ii) They will be protected from fraud and unauthorized transactions

A second part of the security expectation is the consumer expectation that they will be protected from fraudulent and unauthorized transactions, and, as discussed more fully below, the SSN plays a key role in meeting those expectations.

For instance, SSNs are used by lenders to help determine that a loan applicant is who they say they are, and not some imposter, and they are used by credit card companies to contact consumers to verify possible fraudulent transactions. Without the SSN, the incidence of fraud and identity theft would likely increase, making consumers far less secure.

II) <u>Limitations on the use of other data have amplified the importance of the SSN</u>

The private sector should not rely exclusively on the use of SSN as a single-factor identity authentication tool or data matching point. In fact, CDIA believes that the more data points a company can use, the more accurate their merging and authentication decisions will be. However, rather than removing the SSN or limiting its use, it is our view that utilizing more information, rather than less, would help to diminish the importance of the SSN in any given transaction. For instance:

- Cell Phone Numbers – Cellular telephone numbers are tied to a particular individual, and could potentially serve as an additional check point in identifying or authenticating an individual. However, due to many impediments, including regulatory limitations, this information is not widely available for use as an authenticator.
- Drivers License Numbers – Similarly, an individual's Driver's License number could be used as part of the identification/authentication test, as well, to supplement the use of the SSN. However, the Driver's Privacy Protection Act (DPPA) prohibits the use of the number for purposes such as data matching or authentication.

- NCOA Addresses – Another potential identifier and authentication tool is also precluded: Licensing agreements prohibit the use of the National Change of Address process, established by the U.S. Postal Service, for any purposes except delivery of mail. The real irony here is that Congress, in the FACT Act, recognized that attempts to change the billing address for consumers made them more vulnerable to fraud, and yet one tool that could be used to help in that area cannot be utilized for those purposes.[4]

III) Authentication

The key to an identity thief successfully opening a fraudulent account in someone else's name lies in the success or failure of the lender to properly authenticate the applicant. If the lender is not able to authenticate the applicant, the application is blocked, but if the authentication process itself fails, the fraudulent application is processed.

A) The SSN Is Not Used As a Single Identity Authenticator

SSNs are not, and should not be, "the key" to unlock credit.

CDIA strongly believes that meaningful authentication should be applied to all consequential transactions to determine if that the consumer with whom an organization is dealing is who he/she claims to be. Further, we believe that, in most situations, a name and SSN is not, and should not be, sufficient to accomplish that.

In fact, part of the reason that so much progress is being made in efforts to stop identity theft[5] is because of tools that utilize more data and more information, including SSNs.

---

[4] We hope that the final versions of the FTC and FRB's Red Flag guidelines and rule will facilitate the use of the NCOA process.

[5] As the Federal Trade Commission's annual report on consumer complaints shows, complaints about identity theft dropped in 2006 and, in particular, complaints about credit card fraud have plummeted 22 percent since 2003. Further, this result is mirrored by other measures, as well, such as the FTC Synovate and Javelin survey data show a downward trend in total victims from 10.1 million in 2002 to 8.9 million in 2005, an 11.9% reduction, and a Javelin Survey & Research announcement that identity theft has dropped 21 percent nationwide from 2003 to 2006.

Second, there is no demonstrable link between data breaches and identity theft**.**

Not only have ID theft rates been declining, but studies, such as that prepared by the GAO in 2007 and by Javelin Research in 2006, suggest that breaches may only account for a tiny portion of the known causes of identity theft.

Further, some data shows that while the number of publicly announced data breaches has increased, the levels of identity theft and total number of victims appear to be leveling off, or even falling. Perhaps this is the strongest proxy data which indicates that breaches are not driving identity theft.

Or, as the Task Force Report indicates, "The link between a data breach and identity theft often is unclear," and "Little empirical evidence exists on the extent to which, and under what circumstances, data breaches lead to identity theft, and some studies indicate that data breaches and identity theft may not be strongly linked."

The New York Times published a comprehensive review of security breaches and noted while from September 2005 through September 2006 "the personal records of nearly 73 million people [one in four Americans]…have been lost or stolen…there is no evidence of a surge in identity theft or financial fraud as a result. In fact, there is scant

The private sector is well ahead of its duties under law when it comes to using identity verification tools to authenticate applications. For instance, CDIA's members are the leading providers of identity verification and fraud prevention technologies, and are leaders in key discussions about the future of identity management, including participation in the ANSI-facilitated discussions and those held under the aegis of the Center for Identity Management and Information Protection (Utica College, Utica, NY).

B) The use of authentication tools should be expanded

While financial institutions have certain authentication requirements, such as Section 326 of the USA Patriot Act and the anti-money laundering requirements of the Bank Secrecy Act, there are many other consequential transactions for which no similar customer identification duty exists. For example while the FTC's 2006 identity theft complaint data shows that utilities fraud of all types makes up 16 percent of all complaints, it isn't clear that utilities have any clear duty to properly authenticate consumers. In fact over 60 percent of all identity theft complaints were about transactions outside of the financial services industry.

Therefore, it is CDIA's view that customer identification standards like those applied to the financial services industry should be applied to other consequential transactions involving consumers.

IV) A "Necessity Test" for SSN Use is Not the Right Question

The question of determining the "necessity" of an SSN has been raised any number of times in public policy discussions. However, because of the nature of how SSNs are used, that is not the right questions to ask.

As discussed above, an SSN serves as a linchpin, tying together oftentimes disparate information. However, decisions utilizing an SSN are risk and rule based, utilizing multiple data points to attempt to determine "truth" –SSNs are extremely useful in helping to reach a better decision, but they are not the final arbiter of any decision. In other words, CDIA is concerned that a "necessity" test will miss that important nuance.

However, to the extent that the Task Force is already headed down this path, CDIA agrees with the President's ID Theft Task Force Report characterization of the necessity of the SSN: "There are many necessary or beneficial uses of the SSN. SSNs often are used to match consumers with their records and databases, including their credit files, to provide benefits and detect fraud. Federal, state, and local governments rely extensively on SSNs when administering programs that deliver services and benefits to the public." *President's ID Theft Task Force Report, P. 22*

---

evidence that identity theft and financial fraud have increased at all. Even when computer networks are cracked into, and troves of personal information intentionally stolen, fraudsters can typically exploit only a tiny fraction of it." In fact, the author of the study of breaches and ID theft, Mike Cook of ID Analytics, notes that backstabbing relatives do more damage than hackers. Source: Steve Lohr, *Surging Losses, but Few Victims in Data Breaches*, New York Times, Sept. 27, 2006.

Tools that utilize SSNs have developed in different ways, and different companies or products use SSNs in different, but no more or less "necessary" ways than similar products that seek the same results. For instance, some fraud detection and authentication tools may require companies such as financial institutions and contractors to share Social Security Numbers, while other products may utilize a slightly different model, and not share that data. While the "uses" are perhaps similar, proposals to restrict sharing would have significantly different impacts on these products, and could cripple some tools that are effective, but are no more a factor in causing identity theft than any others.

V) Public Records

While CDIA believes that disclosure of the SSN to the general public must be prohibited, we also believe that public records must be made available, including SSNs, to those with an appropriate need.

Public records play a vital role in our society, and bring value to consumers. Bankruptcy records, tax liens and judgments are part of consumer "credit" reports used by lenders to make decisions. Records of eviction are critical to landlords who must themselves pay the bills and attempt to lease properties to consumers who will do the same. Validating professional licenses for employment screening agencies is yet another use of public records, as is accessing criminal histories.

Through the development of nationwide databases of public record information, CDIA's members have addressed the problems inherent in having to search through tens of thousands of federal and state court houses and agency databases. In this way, the SSN is as important an identifier in a public document as it is in a private-sector database. It is a critical identifier for all of the data management reasons discussed above. Without an SSN, a consumer can simply alter a few items of information, such as moving to a new address, or even changing a name, and thus separate himself/herself from a bankruptcy record, a tax lien, a record of eviction and even a criminal history, in some cases. Clearly this is not a positive outcome for consumers or for American businesses which are on the front lines of making, for example, fair and accurate risk based lending and employment decisions, while at the same time fighting identity theft and fraud.

While CDIA supports restricting the availability of SSNs to the general public, the availability of the SSN is vital to data matching and other purposes explained more fully below. The concern of the CDIA's members is that a requirement that state and local governments truncate SSNs on public documents may be perceived as an unfunded mandate, which will drive under-funded state agencies to either stop requesting the SSN when processing vital records, or to simply deny all access to public records containing SSNs.

It is important that public records, including those records containing SSNs, continue to be made available.

The debate about the presence of the SSN in public records has suggested a possible binary solution, where SSNs could be made available electronically for certain entities, but could possibly be redacted for publicly available electronic documents, though costs will have to be

addressed. It is encouraging to hear state court organizations discussing strategies for protecting SSNs, and CDIA will continue to engage in these dialogues.

SPECIFIC QUESTIONS

We turn now to the specific questions raised in the FTC's Notice:

1. ***Current Private Sector Collection and Uses of the SSN***

    - *What businesses and organizations collect and use the SSN? For what specific purposes are they used?*

As discussed in CDIA's attached testimony, a wide range of businesses, non-profit organizations, government agencies and public institutions collect SSNs for a wide range of legal, beneficial reasons, from customer identification and identifying potentially fraudulent transactions to hiring and managing employees.

CDIA members collect and provide SSNs in conjunction with consumer reports or other products to qualified business entities that have been carefully screened to ensure that they have either a valid permissible purpose under the Fair Credit Reporting Act or an allowable use under Section 502(e) of the Gramm-Leach-Bliley Act (GLBA).

Specifically, Social Security Numbers are used for a variety of purposes by CDIA members, ranging from facilitating the accuracy of information contained in a consumer's credit report to authentication and order processing. Social Security Numbers are also used for verifying or obtaining credit scores and for internal matching purposes.

Other uses for SSNs include: pre-employment screening for volunteer employees, locating former employees, beneficiaries and heirs, collection of overdue payments, account tracking, audit and quality control.

CDIA's members use SSNs for the following purposes:

I) **Match Data**

The SSN is an important match key for CDIA members and across a range of products and databases. The SSN isn't the sole match key, but it is unique to a consumer, making it different than virtually any other match key available, and it helps make the match decision more accurate. We discussed previously some other match keys that would be helpful, and would further increase CDIA –members ability to accurately match data, but which are not available due to legal and regulatory restrictions.

As discussed above the SSN contributes in a number of ways relative to data matching.

The SSN is a match key to how new information is merged into, for example, an existing credit report[6] in spite of changes of address, changes of surname due to marriage or divorce, and

[6] "Social Security numbers are used to match consumers to their credit and other financial information. Without them, information may be attributed to the wrong consumer, and the accuracy of credit reports may be degraded."

variations in name.[7] It is a match key in cross-matching data across data bases in the context of fraud prevention, so that data can be assembled and used to evaluate the authenticity of consumer-supplied data. It is used as a match key for data extraction where the SSN is included in inquiring data.

A study of data matching conducted by the FTC points out that "The lack of a fully reliable identifier means that the CRAs inevitably face situations where records match with a high probability, but not with certainty. In such cases, a CRA must make a difficult choice. Accepting the match risks assigning a credit history to the wrong consumer, while rejecting the match risks excluding information that is legitimately part of the consumer's credit history. Either outcome [when the wrong decision is made] can hurt consumers."[8]

To further illustrate the importance of the SSN, consider the following example. Without the SSN to assist CDIA members in data matching purposes, it has been estimated that the major credit bureaus could suffer as much as a 15-20% decrease in average credit file content, due to an expansion of the number of isolated or fragmented files caused by to the absence of SSN in the data they receive from information furnishers (predominantly financial institutions)[9]. It is likely that such a decrease in file content will correspondingly erode the performance of most models which attempt to score those files. Specifically, the omission of good credit

---

Hearing on Enhancing Social Security Number Privacy: Before the Subcomm. on Social Security of the House Ways and Means Comm. Subcom. on Social Security, June 15, 2004 (107th Cong.) (Statement of J. Howard Beales, III, Director of the Bureau of Consumer Protection, Federal Trade Commission).

"[Consumer reporting agencies] use SSNs as the primary identifier of individuals, which enables them to match the information they receive from their business clients, with the information stored in their databases on individuals. Because these companies have various commercial, financial, and government agencies furnishing data to them, the SSN is the primary factor that ensures that incoming data is matched correctly…" *Hearing on Enhancing Social Security Number Privacy: Before the Subcomm. on Social Security of the House Ways and Means Comm. Subcom. on Social Security*, June 15, 2004 (107th Cong.) (statement of Barbara D. Bovbjerg, Director of Education, Workforce, and Income Security Issues, U.S. General Accounting Office).

[7] "The credit reporting companies compile and reconfigure the newly received data to create or update the record of an individual's credit experiences. This reconfiguration can require a high level of technical sophistication. For example, credit reporting companies have had to develop rules for deciding when to ignore slight variations in personal identifying information and techniques for recognizing that data items with the same identifying information, such as name, may actually be associated with different individuals. *An Overview of Consumer Data and Consumer Reporting, Federal Reserve Bulletin, Feb. 2003, 50.*

[8] FTC "Report to Congress, Under Sections 318 and 319 of the Fair and Accurate Credit Transactions Act of 2003", December 2004.

[9] "One of the challenges that credit reporting companies face is constructing a unified credit record for a consumer. This challenge arises for a number of reasons. An individual's social security number, for example, may be recorded incorrectly on a loan application, or it may be transmitted incorrectly to the credit reporting companies. Problems also arise because the identifying information may not be current or because a consumer may have accounts under different names or addresses. For instance, a consumer may be inconsistent in using a full name in all applications for credit or may change names, perhaps after a marriage or divorce. Furthermore, accounts may be difficult to link to a given consumer if the consumer's address has changed. Credit reporting companies have established a series of protocols to address each of these challenges." *An Overview of Consumer Data and Consumer Reporting, Federal Reserve Bulletin, Feb. 2003, 53.*

information for good borrowers and/or the inclusion of bad credit information that does not belong to that good borrower may occur more frequently without an SSN.

II) Fraud Prevention

There are a number of different ways that CDIA members use and supply products to others that utilize SSNs to prevent fraud:

1) The SSN itself provides information regarding year and state of issuance, for instance, and if applicant data does not match, a further investigation may be triggered.

2) CDIA members may also provide financial institutions and others with access to various "fraud databases" that may have records relating to known fraudulent activity. The SSN is often used to match data in these cases to help detect potential fraud.

3) CDIA members may also provide tools to lenders and others to search across multiple databases for inconsistent information, such as an address that does not match the one on file. The SSN is used to help search across multiple databases to determine if name/SSN/address/date of birth and other data match consistently.

III) Identity Verification

SSNs may be used to help determine if the documentation provided by a consumer is legitimate; determining for example that an SSN is in fact valid, at least, for example, to the extent that it is part of a range of SSNs that the SSA has issued and not otherwise on the SSA's death master file. This validation process can also extend to trying to determine whether or not a combination of seemingly valid identifying elements is valid as well.

IV) Identity Authentication

As discussed, authentication is a separate test which seeks to determine if the person who is submitting a set of validated identifying elements is in fact the person to whom those elements belong.

As discussed below, SSNs are used to help verify that a particular individual is who they say they are. SSN are used for various identity verification products derived from Social Security Administration (SSA) records and other sources. For instance, the SSN is used to verify the identity of an individual whose name and date of birth match those associated with the SSN, and so that other information is accurate.

A number of CIDA members produce products that are used by financial institutions, insurance companies and others to verify the identity of an individual and determine that the person they are interacting with is who they say they are. These products are very effective in detecting and preventing identity theft and financial fraud before it happens.

The SSN helps businesses prevent fraud by cross-checking applicant data against various other data sources in order to authenticate the consumers' identity. Absent the use of an SSN, these systems will be far less likely to trigger security protocols, which prevent identity theft.

In 2004, the GAO conducted a study on Social Security Numbers, and concluded that "information resellers, credit reporting agencies and health care organizations use social security numbers to build tools that verify an individual's identity or match existing records since there is no widely accepted alternative." The report further states that "restricting business access to social security numbers would hurt customers and possibly aide identify thieves since it would be more difficult for business to verify an individual's identity."

V) **Background Screening**

The information that is most often received on an individual is based on demographic identifiers, such as date of birth, first name, last name, gender, race, address and SSN. The SSN may be used in conjunction with other data to associate information to the specific individual.

Additionally, many CDIA members rely on the SSN to perform critical employment, residential, and volunteer background screening functions for business, government, and non-profit organizations. The SSN is a critical data element to not only verify the identity of the individual, but also accurately match vital data associated with that individual. The SSN provides significant matching capability to the background screening process and helps ensure that employers, residential managers and volunteer organizations are able to accurately and timely navigate the labyrinth of similar and common names and addresses to make critical business and public safety decisions.

Specific Examples: Given this general discussion, the following specific examples describe some of the legal and legitimate ways in which CDIA members utilize SSNs every day for legitimate purposes to help people, protect consumers, and assist law enforcement efforts. We hope they shed some more light on how critical SSNs are in everyday transactions:

- **Access to home ownership:** Every homeowner benefits from a credit reporting system that reduces the costs of all mortgage loans by a full two percentage points, thus putting literally thousands of dollars in disposable income into their pockets. Homeownership is no longer a luxury of the well-to-do, but is a truly democratized American dream enjoyed by nearly seventy percent of the population. The SSN helps to facilitate the efficient operation of this system, as described above.

- **Locating sex offenders**—SSNs are used to locate registered, and unregistered, sex offenders. There are over 560,000 sex offenders in the U.S., and approximately twenty-four percent of these individuals fail to comply with address registration requirements mandated by law. Access to SSNs allows law enforcement to locate sex offenders even when the registration address has not been kept current.
- **Law enforcement**—SSNs are used routinely by law enforcement officials to locate fugitives and witnesses to crimes. The ability to conduct an information search using an SSN is essential. Restrictions on access to SSNs in government records would hamper the ability of CDIA members to provide this critical information to law enforcement.
- **Locating and recovering missing children**—Locating a missing child within the first 48 hours is critical; after that time, the chance of recovering the child drops dramatically. In many of these cases, it is the non-custodial parent who has taken the child. The use of SSNs

is critical in locating the non-custodial parent and recovering the missing child. This effort will be seriously hampered if SSNs in public records are no longer available.

- **Recovery of child support and other debts**—Public and private agencies rely on social security numbers and other information to locate persons who are delinquent in child support payments, other lawful debts, and to locate and attach assets in satisfying court-ordered judgments. The Association for Children for Enforcement of Support (ACES), a private child support recovery organization, has stated that social security numbers are the most important tool for locating parents who have failed to pay child support. ACES has had tremendous success using SSNs to locate nonpaying parents using products produced by CDIA members.
- **Credit card fraud prevention**—Public record information compiled using SSNs is routinely used to detect fraudulent credit card applications and to authenticate consumers when fraud is suspected. This identifying information is used to prevent identity theft and fraud by allowing companies to prescreen applications to determine that the address, phone number and other information of the applicant matches the applicant's name.
- **Insurance fraud prevention**—Insurance companies use public record information compiled using social SSNs to detect fraudulent insurance claims. According to the National Fraud Center, the average American household pays $200 to $400 a year in additional insurance premiums to offset the cost of fraud. This cost would likely increase if companies did not have the information they needed to detect and prevent fraud.
- **Preventing and investigating financial crime**—The Financial Crimes Enforcement Network (FinCEN) under the U.S. Treasury Department supports federal, state and local law enforcement agencies in financial investigations, and is heavily reliant on SSNs in these investigations. The use of SSNs by financial institutions to verify and validate information on prospective customers is critical to the success of these programs.
- **Location of missing heirs—**SSNs are an important tool used in locating pension fund beneficiaries and missing heirs so they can receive the money owed them. Pension Benefit Information (PBI), a private company that locates former employees that are due pension benefits, has indicated that in many cases the SSN becomes the only link between an employer and their former employees with vested benefits. Employees move, marry and change their name, but the one thing that remains constant is their SSN.
- **Employment/security screening:** As discussed above, SSNs serve as vital links among disparate records that help businesses verify prospective employees' identities and conduct thorough, accurate background checks to ensure workplace safety and business security.
- **Small business B-to-B transactions:** An SSN is the key business entity identifier to virtually all sole proprietorships or partnerships; as a result, SSNs are necessary to facilitate business-to-business transactions between small businesses.
- **Securitized credit markets:** Confidence in the U.S. securities market is made possible by accurate financial histories compiled using the SSN as a key identifier. Restricting use of the SSN could undermine confidence in these securitized credit portfolios, resulting in substantially higher consumer costs for credit, including mortgages and auto loans.

Additionally, without the use of the SSN, consumers would suffer harm:

- **Incomplete data harms consumers:** As discussed, there would likely be a decrease in the ability of consumer reporting agencies to properly match incoming information to the correct consumer about whom the information relates. For instance, there are

consequences for consumers of having a consumer credit report that does not contain all of the accounts that they pay on time and which makes them eligible for the lowest cost loans.

- **Incomplete data harms our banking system:** The absence of the SSN would also put at risk the safety and soundness of lending decisions due to less information being included in consumer credit reports due to data matching issues.

- **Incomplete data prevents consumer access to goods and services:** Think about the consequence for consumers when a consumer reporting agency cannot locate the proper file on a consumer and thus a lender, insurer or other service provider wanting to do business with the consumer has to deny the application, or the consumer has to pay higher rates.

Below are some more specific examples of how SSNs are used every day for legitimate purposes that CDIA believes that it is important to highlight. We hope they shed some more light on how SSNs may be utilized in everyday transactions:

Example A: Accessing a Sensitive Facility

Accessing a sensitive facility, such as a nuclear power plant, would most likely involve a two-step credentialing and identity verification process. First, a background check is performed to verify the person's identity, among other things. This is typically done by hiring a consumer information company such as a CDIA member to take the information the person has provided about himself, and ensure that it matches other available information about that individual. Once that step is complete, the person receives their credentials - perhaps an identification card or badge.

Second, when the person seeking access arrives at the facility, their credentials (the ID or badge) would be checked to verify that the person attempting to access the facility is the same person who received the credentials (i.e., to make sure that the credentials were not stolen by a person now attempting to access the facility). The facility may also collect some additional identifying information from the individual and may send it to a company that provides identity verification services, who will then give back an indication of the likelihood that the person is who he or she claims to be.

Example B: Opening a Bank Account

All banks (national and state banks, credit unions, and state and national thrifts) must have a Customer Identification Program ("CIP") as mandated by Section 326 of the USA PATRIOT Act. The CIP is intended to enable a bank to "form a reasonable belief that it knows the true identity of each customer." Banks do not independently have information enabling them to meet identity verification obligations, but they rely on consumer information providers such as CDIA members. When a consumer attempts to open a depository account, the bank submits the consumer's identifying information to the service provider, who replies either by indicating that the information matches the information it has associated with a living person of the same name,

or whether (and in which respects) the information is inconsistent. Because there are many people with the same name and similar address histories, the SSN is an important ingredient which gives the verification process a higher degree of confidence in the person's identity before the bank provides them with an account.

Further, the SSN may be utilized by the financial institution to check for a bad check history – does this person have any outstanding bounced checks at another lending institution that may make them a risk to pass bad checks again.

- *What is the life cycle (collection, use, transfer, storage and disposal) of the SSN within the businesses and organizations that use it?*

Because these records are generally linked to specific individuals, the use of the SSN continues until the file is destroyed. However, that does not necessarily mean that the information contained in the file is maintained indefinitely. Specifically, under the Fair Credit Reporting Act, certain data may only be reported for specific periods of time. Information retention and disposal of data are done in accordance with all legal and regulatory requirements.

- *Are governmental mandates driving the private sector's use of the SSN?*

There are more than 34 federally mandated programs requiring SSN collection. In addition, however, the federal government often relies upon private-sector verification of its own information[10].

For example, certain governmental mandates like the US Patriot Act have "know your customer" provisions that require financial institutions to obtain SSNs as part of verifying and identifying their customers. Other regulations, such as anti-money laundering (AML) laws, requirements to locate beneficiaries, and state laws regarding parents in arrears of child support payments (i.e. "Deadbeat Dad" laws) require the use of SSNs.

Other provisions of the Patriot Act, such as the Real ID Act, have yet to be fully enacted by the Department of Homeland Security, but the final regulations will likely call for verification of SSNs, as well.

Many state laws consider SSNs an acceptable form of identification for use in opening or accessing financial accounts. At the state level, SSNs are also used for purposes such as subpoena compliance, as well as compliance with child support and elder abuse laws.

However, apart from government mandates, businesses generally need to know their customers and to make prudent provisions for the potential need to recover from losses or fraud on some of

---

[10] "Cross-verification [of SSNs by the Social Security Administration through both public and private sector systems] can combat and limit the spread of false…identification and misuse [and] the rewards of cross-verification can be impressive…" *Hearing on the Homeland Security Threat from Document Fraud, Identity Theft, and Social Security Number Misuse, before the Senate Committee on Finance, Sept. 9, 2003 (statement of Patrick P. O'Carroll, Assistant Inspector General for Investigations, Social Security Administration).*

their accounts. The SSN is an important element of information for all of those purposes. Thus, although government mandates such as Patriot Act know-your-customer rules are drivers of the need for SSN, the need would exist without these drivers.

- *Are there alternatives to these uses of the SSN?*

Generally there are no viable alternatives for the SSN. For instance, name and address can't be relied on by themselves because they are too common, change due to marriage and divorce, and, according to the U.S. Census Bureau, 42 million consumers move every year. Even for consumers who's address and name are constant, they do not always use their identifiers inconsistently (i.e. in some instances they will use a nickname, and may inconsistently use their generational designations (e.g., III, or Sr.)) There are also times where consumers themselves make mistakes when completing applications. Thus, a consumer's identifiers may be presented in different ways in different databases and, in some cases, the data may be partially incorrect. Further, personal identifiers such as name and date of birth, are generally not as unique as they may first appear to be.

Additionally, for many uses, even a truncated SSN will not suffice[11]:

In September 2003, a nation-wide CDIA member performed a test using 9,906 bankruptcy records. This company ran a test with and without the SSN. With an SSN, name and full or partial address (some court records were missing city, state or zip information) the company was able to accurately match 99.82% of the records. Without the SSN, 25.71% failed an identification/authentication match (6.11% were due to an incomplete address/no SSN, and an additional 19.60% failed due to the lack of an SSN).

The company also conducted an analysis using the last four digits of the SSN in identifying the correct consumer. According to the company "searching our database on only the last 4 digits identifies too many possible false-positive candidate consumers to be evaluated. Therefore we had to omit this search option and consequently miss any consumer matches that the 9 digit SSN would provide."

Using the 4 digit SSN in the company's match evaluation was also analyzed. The following is an anonymous example of an actual search:

> Record: Chapter 7 bankruptcy for Juan Gonzales, 100 Main St., Orange CA, SSN XXX-XX-4587.
>
> On file data:
> Juan B. Gonzales, 100 Main St, Orange, CA, SS XXX-XX-4587
> Juan R. Gonzales, 100 Main St, **Apt 22**, Orange, CA SS XXX-XX-458**9**
> Juan Gonzales, **2**01 Main St, Orange, CA SS XXX-XX-4587
> Juan B. Gonzales, 100 Main St, Orange, CA SS XXX-XX-4**8**87

[11] "...the use of partial Social Security numbers may not provide sufficient accuracy when an agency is working with a large database." 69 Fed. Reg. 63922, 63931 (Nov. 3, 2004) (concerning the information needed to place security alerts on credit reports).

All 4 of the above listed consumers may or may not be the consumer who filed the bankruptcy at issue. All have slight variations in their data on file, which may be due to common input errors, typos, handwriting anomalies, etc. However, due to the limited data provided in the public record, the company was unable to ascertain, to its required stringent degree of certainty, if any of the consumers are a match. Having all nine digits of an SSN in the evaluation process allows room for a calculated degree of variation in digits and letters. The company involved in the test, and possibly other CDIA members, may therefore not consider the 4 digit SSN a reliable identification factor.

Further, the use of other alternatives that could possibly serve as a substitute for an SSN, such as a cell phone number or driver's license number, is often restricted by law, as discussed above.

For instance, the use of Drivers' license numbers as an alternative to the SSN in commerce is restricted by provisions of the Drivers Privacy Protection Act. In addition, a person who moves from state to state will have multiple drivers' licenses numbers.

Finally, while credit reporting agencies in some countries have attempted to develop a type of aggregated match key based on a combination of name and address data or a unique identifier such as a national ID number, this has resulted in a more ambiguous match with lower and less accurate match rates. For example, in the UK matching is less accurate. There is no national identifier or equivalent to the SSN. The credit reporting companies rely more heavily on address match and the national government provides them with address updates each year from mandatory voter rolls.

- *What has been the impact of state laws restricting the use of the SSN on the private sector's use of the SSN?*

Many states have passed laws regulating the use and disclosure of SSNs. California was the first state to take on the issue of prohibiting the sale of SSNs to the general public and other restrictions on the display of SSNs, though it took the California Legislature four years to strike a careful balance that still preserves the ability of businesses to use and share SSNs in a responsible fashion, such as is permitted by the Fair Credit Reporting Act (FCRA) and Gramm-Leach-Bliley Act (GLB). More than 16 other states have also enacted similar legislation, and they have done so in a deliberate and careful manner that does not restrict legitimate uses.

Another type of state legislation restricting the disclosure of full SSNs on public records has had an impact on the ability of CDIA members to match public record information. SSNs are a key identifier used to match public records with the consumer; without this information, it is significantly more difficult to match a public record with the correct consumer file in a manner that meets the FCRA's standard of "reasonable procedures to assure maximum possible accuracy." Authentication and credit verification using only a name, address and birth date is less precise than a SSN match.

State laws restricting access to SSNs on public records has resulted in considerable difficulty in the ability of consumer reporting agencies to match the public record with the consumer file. Absent this matching ability, lenders might have no way to know a potential borrower's past history, including bankruptcies, liens, and judgments.

Some states, such as Minnesota, have passed legislation calling for the truncation of SSNs. However, a truncated SSN is often an ineffective as a tool for matching data, as the use of partial SSNs is often not enough to provide sufficient accuracy for matching purposes. These types of restrictions on SSN use results in decreased information, requiring lenders to make less informed decisions that could lead to bad loans, or ever greater identity theft.

Finally, ensuring that the Social Security number issue is addressed in a uniform fashion, so that all consumers are protected, is a vital component of this debate. Any legislation that would restrict the sale or display of SSNs must contain federal preemption so that businesses are subject to a single, national law rather than having to comply with various state laws all with differing and potentially conflicting requirements.

2. ***The Role of the SSN as an Authenticator***

    - *The use of the SSN as an authenticator – as proof that consumers are who they say they are – is widely viewed as exacerbating the risk of identity theft. What are the circumstances in which the SSN is used as an authenticator?*

We know of no instance in which the SSN is used in isolation as an authenticator. It is used in conjunction with other identifying information to attempt to authenticate identity.

The process of identification – where a consumer professes to be who they say they are - should be considered distinct from the process of authentication, which essentially requires that the first step of self-identification take place, plus the additional step of querying an independent third-party database to verify that the customer is in fact who he says he is. Pragmatically-speaking, a self-reported identifying SSN from a consumer is relatively meaningless until it has been independently verified by a third party as being linked to that consumer by some degree of certainty.

Once a consumer has identified themselves by providing a SSN, third-party databases (including databases that include public records information, address histories, etc.) can then be used to authenticate that the consumer is who he says he is. The SSN and other data is also used to "authenticate" the identity of the individual – that is, to make sure that the person is who they say they are. In that case, the lender may use the SSN and other data to look for anomalies (for example, do the name and address and SSN all match), to look for indicia of fraud (does the SSN match a number from the Death Master File, which keeps track of SSNs of deceased individuals), and to look for other potential problems.

At the authentication stage, a SSN can be used to compare data elements associated to the number, to those data elements associated with the individual. For example, all SSNs have a date issue range associated to them. If a consumer provides a date of birth that is after the issue date, it is highly likely that the SSN was not assigned to the consumer as the consumer was born after the number was issued.

The value of a SSN in the authentication process lies in its ability to be paired with information that only the consumer would know, i.e. "out -of- wallet" questions. Multi-factor authentication provides the best defense against fraud and identity theft. For instance, multi-factor authentication could be composed of three distinct processes: 1). Something the consumer possesses, like an ATM card 2). Something only the consumer would know, like a

PIN or "challenge" question (i.e. favorite color, city of birth, etc.) and 3). Something the consumer is, i.e. "biometric" information (for example, fingerprints, etc.). Authentication could be made up of two or even three of these steps to ensure reliability.

Identity Authentication with Current Customers is Different than with New Applicants

It is important to note the difference between authenticating a current customer vs. validating identifying elements and then authenticating a consumer who is making application to become a new customer of an institution.

It is our experience that some policy makers are in fact confusing the two processes and thus think that authenticating a consumer's identity is as simple as requiring a password. While this might be true for a current customer relationship, it is not true at the point of a new application with a consumer who is not yet a customer. As the FTC itself knows, an example of knowing a "current" customer can be found in the new multi-factor online authentication guidance issued by the FFIEC. Much of the CDIA discussion is focused on the new customer application process.

To the extent that the FTC's report can bifurcate its discussion to account for authentication differently in each context, this will help to inform the dialogue as a whole regarding the role of SSNs in the private sector.

- *Are SSNs so widely available that they should never be used as an authenticator?*

The question implies that SSNs are or can be utilized by themselves as authenticators – an assumption CDIA disagrees with. As we have stated elsewhere, SSNs are never and should be used on their own as an authenticator, regardless of its availability.

However, the SSN serves a role in authentication in a variety of ways: It can be tied back to combinations of identification elements to determine whether or not it is a common combination; It can be used to determine whether the SSN is used commonly with other combinations of identifying elements including completely different names; It can be used as a matching element to identify whether or not it has been used as part of verified fraudulent transactions via "fraud exchange database" where participants report on identified fraud and the application data therein; It can be used as a cross match against other data elements provided on an application including a date of birth or a state of birth; and It can be used to cross match against the SSA's Death Master File and also against ranges of SSNs which have been issued by the SSA to verify that the number given is in an active range. Therefore, even if it were broadly available, the SSN should nonetheless be used as PART of an authentication undertaking.

In other words, more data and more robust authentication, rather than fewer data points, should be utilized for authentication purposes – the more matching data points there are, the more confidence that the person is who they say they are. Reducing the amount of data available to authenticate an individual will exacerbate the problems, not make them better.

For example, most names, addresses and phone numbers are available in the phone book; however, because they are widely available does not make them any less important.

- *What are the costs or other challenges associated with eliminating the use of the SSN as an authenticator?*

Because of its ubiquitous use, there is no way to calculate the costs of eliminating the SSN in the authentication process. The SSN is a key identifying piece of information that links together various pieces of information to establish as reliable an assurance as possible that this consumer is in fact who he says he is; without a SSN, it is extremely difficult to reliably link together disparate information to prove a consumer is who he says he is.

Moreover, identification is a necessary condition for authentication. Eliminating the use of a SSN in the authentication process would essentially weaken fraud protection processes already built into the authentication process. The costs would be borne in a higher incidence of identity theft and other forms of financial fraud; in greater costs associated with borrowing reflected in either higher interest rates or higher fees; and in less availability of credit to consumers.

Eliminating the use of SSNs as an authenticator would also lead to increased costs for businesses in the form of increased incidences of fraud and costs associated with having to manually review files to determine an accurate match.

The costs to private industry would be significant if SSNs could not be used in the authentication process – not only would the rate of fraud rise due to less accurate authentication processes, companies that provide this authentication services would have to implement entirely new, less reliable matching models – increased costs would include updating data collection methods, updating matching logic, developing new fraud modeling algorithms as well as updating storage policies and parameters.

3. ***The SSN as an Internal Identifier***

- *Some members of the private sector use the SSN as an internal identifier (e.g. employee or customer number), but others no longer use the SSN for that purpose. What have been the costs for private sector entities that have moved away from using the SSN as an internal identifier? What challenges have these entities faced in substituting another identifier for the SSN? How long have such transitions taken? Do those entities still use the SSN to communicate with other private sector entities and government about their customers or members?*

- *For entities that have not moved away from using the SSN as an internal identifier, what are the barriers to doing so?*

CDIA believes that these questions miss the mark – the questions should be whether or not the SSN is accessible to the public or other employees. Specifically, companies almost always will need to link their employees' identification number with their SSN for tax collection purposes with the IRS, for the utilization of employee benefits, and for other purposes. The question, however, should be whether companies are displaying the SSN publicly – that is, are they displaying it on ID badges and writing it in places where others can access it.

CDIA believes that that type of public display of the SSN is unnecessary, though we caution the FTC that requiring businesses to develop an alternative system to using an employee's SSN number in any context but reporting to the government would likely result in more errors in reporting, as each business' HR department would essentially be required to manually verify every employee SSN number before submitting information for government reporting purposes.

4. ***The Role of the SSN in Fraud Prevention***

    - *Many segments of the private sector use the SSN for fraud prevention, or, in other words, to prevent identity theft. How is the SSN used in fraud prevention?*

Businesses rely on SSNs to validate and verify consumer information and to identify potentially fraudulent applications. Examples include: a submitted SSN is often compared against a death master list to see if an applicant is deceased; a SSN provided by a consumer is compared with name and address for a match; the first five digits of a SSN (which indicate state and year of issuance) can be used in conjunction with other documents, including a birth certificate, to verify identity.

Additionally, in the mortgage industry, SSNs are used to validate such things as employment status, as well as income and existing assets, all important factors a lender needs to know in processing a mortgage. Lenders often check a potential borrower's SSN against a third-party database to see if the borrower has been involved in any previous fraudulent transactions.

    - *Are alternatives to the SSN available for this purpose? Are those alternatives as effective as using the SSN?*

Generally there is no alternative to the SSN. There is no other identifier that is unique, follows a person for his or her whole life, and is utilized by such a wide range of entities that it can be used to combine records regarding an individual across data bases.

    - *If the use of the SSN by other sectors of the economy were limited or restricted, what would the ramifications be for fraud prevention?*

Limiting the use of SSNs for fraud prevention purposes would significantly undermine the ability of fraud protection tools and services to prevent fraud. Restricting access to SSNs would weaken the ability of fraud protection services in several ways: it would restrict data collection methods used to compile information to protect against fraud; it would impact the efficiency of fraud modeling algorithms; and it would undermine the strength and accuracy of search logic programs that link together information via a SSN. The result would be a higher incidence of identity theft and other forms of financial fraud; greater costs associated with borrowing reflected in either higher interest rates or higher fees; and less availability of credit to consumers.

5. ***The Role of the SSN in Identity Theft***

- *How do identity thieves obtain SSNs?*

Identity thieves obtain SSNs as part of a process of collecting enough information to fraudulently open an account by impersonating the other person. While the SSN may be a necessary piece of information, it is not enough. The thief needs more information about a person than a name and SSN. Thieves obtain this additional information in a variety of ways, though the largest single category appears to involve theft of the SSN by persons in positions of trust stealing information from friends and family members. Other ways include rogue employees of financial institutions that collect application data, keylogging, or even "boxing", the practice of stealing mail from mail boxes, which could include SSA notices, bills, insurance statements, or anything that might have information on an individual including the SSN number. Other ways in which identity thieves have obtained SSNs has included phishing by fraud rings, often as a means to fund other criminal activities.

- *Which private sector uses of the SSN do thieves exploit to obtain SSNs, i.e., SSN as identifier or SSN as an authenticator? Which of those uses are most vulnerable to identity thieves?*

As stated above, because it appears as though most identity theft is committed by someone close to the victim, we would postulate that an identity thief might not have trouble obtaining additional information about a consumer, such as "out of the wallet" answers, that might likely be used to authenticate the individual.

However, for other fraud, we believe that part of the solution to identity theft can be had by utilizing more robust authentication methods utilizing more data, rather than less.

Since both the identification stage and the authentication stage require a SSN, there is realistically-speaking no real difference between the vulnerability of the two. Industry already applies extensive security protections to safeguarding a SSN at both the identification and the authentication stages.

- *Once thieves obtain SSNs, how do they use them to commit identity theft? What types of identity theft are thieves able to commit with the SSN? Do thieves need other information in conjunction with the SSN to commit identity theft? If so, what other kinds of information must they have?*

In some instances, identity thieves create new identities using existing SSNs and sell them to individuals that cannot otherwise obtain a SSN legitimately for purposes such as financing, employment, or insurance. The legitimate holder of the SSN may not even become aware of the use of their SSN until it is time to collect social security or should their credit information ever be combined with the illegitimate holder's credit information. True person identity theft requires more than just a SSN. In many cases, identity thieves have methods of obtaining this information from a single source like a rogue employee or multiple sources in order to commit true person identity theft.

- *Where alternatives to the SSN are available, what kind of identity theft risks do they present, if any?*

We do not believe that there is any alternative that is currently viable. However, without the SSN, we believe that identity theft and fraud rates would rise dramatically.

Any alternative to the SSN is vulnerable to the same risks as a SSN, as whatever unique identifier is used as an alternative to the SSN will be subject to the same identity theft risk. However, the solution to identity theft is ***more*** information rather than ***less***. The recent progress on limiting identity theft – as seen in the declining number of identity theft complaints reported to the FTC and the declining trend in the annual surveys by Javelin Strategy and Research – is result of several factors that include the private sector using tools that rely upon ***more*** information and ask out-of-wallet questions. Ironically, eliminating the ability to use information actually makes it easier for fraudsters to operate.

CONCLUSION

In conclusion, the SSN is utilized for a variety of legal, beneficial uses. CDIA would argue that in establishing what uses of the SSN are "necessary," the FTC and the Task Force tread carefully – law that impedes legitimate business-to-business and business-to-government uses of the SSN could have profound effects on consumers, often in ways that are unanticipated.

Therefore, CDIA would strongly urge the Task Force to focus much of its effort on beneficial endeavors that could protect consumers. Specifically, CDIA would urge the Task Force to extend national uniform information security regulations to all who possesses the SSN in combination with a person's name and other sensitive data beyond just financial institutions.

To prevent fraud you must be able to crosscheck information, and to maintain accurate databases, you must be able to maintain a range of identifying elements. Absent the availability of the SSN, we will be less able to build accurate data bases, to accurately identify records and to help prevent identity theft through the development of fraud prevention and authentication tools.

Ultimately consumers expect us all to accomplish the goals of protecting and securing the SSN, and also ensuring the accuracy and effectiveness of databases which contain information about them.

Thank you for your time and consideration.

APPENDIX

Statement of Stuart Pratt, President, Consumer Data Industry Association

Testimony Before the Subcommittee on Social Security
of the House Committee on Ways and Means

June 21, 2007

Chairman McNulty, Ranking Member Johnson and members of the subcommittee, thank you for this opportunity to appear before you today to discuss the importance of Social Security Numbers. For the record, my name is Stuart Pratt and I am president and CEO of the Consumer Data Industry Association.[1]

Our members applaud this committee for the thoughtful and open dialogue that you have fostered regarding how Social Security Numbers are used, to identify risks associated with such use, and to address these risks in a reasonable, targeted fashion.

As a preliminary matter, CDIA supports efforts to limit the sale and public display of Social Security Numbers. CDIA's members do not publicly sell or display Social Security Numbers to the general public, and we oppose such activity. However, as will be discussed below, such restrictions have to be carefully considered, balanced and bounded so that restrictions on use do not interfere with legitimate business uses of SSNs to detect and prevent ID theft and financial fraud and for other beneficial purposes.

· The SSN is the only unique, individual identifier that follows a person throughout their lives, literally from the time they are born.

SSNs are important to the smooth operation of today's economy because there is no other single identifier that serves the same purpose as effectively as the SSN.

Although there are other identifiers that may serve similar purposes in some contexts, there are no other identifiers that serve this role across all individuals and circumstances.

For instance, name and address can't be used because they are too common, change due to marriage and divorce, and, according to the U.S. Census Bureau, 42 million consumers move every year. Even for consumers who's address and name are constant, they do not always use their identifiers inconsistently (i.e. in some instances they will use a nickname, and may inconsistently use their generational designations (e.g., III, or Sr.).) There are also times where consumers themselves make mistakes when completing applications. Thus, a consumer's identifiers may be presented in different ways in different databases and, in some cases, the data may be partially incorrect. Further, personal identifiers such as name and birthday, are generally not as unique as we may believe they are.

Further, the use of other alternatives that could possibly serve as a substitute for an SSN, such as a cell phone number or driver's license number, is often restricted by law.

Thus, the SSN is a truly unique identifier.

As the only unique identifier, the use of the SSN has migrated beyond simply keeping track of social security payments, even within the federal government itself. For example, it is used for tax purposes, Selective Service registration, employment verification, the provision of government benefits and a host of other uses. In addition, the use of the SSN is often mandated by the federal government. For instance, the Treasury Department regulations regarding PATRIOT Act compliance for financial institutions' in many instances requires financial institutions to use the consumers full SSN, as obtained from "trusted [private] sources," such as credit bureaus.

Additionally, many State laws require the use of the SSN for a wide range of important purposes dependent on accurate identification. For instance, to meet requirements of the law, government data often must be cross-checked or enhanced with data from private sector databases.

For the private sector, the role of the SSN is that it serves as a unique identifier that is permanent, so a consumer cannot voluntarily relinquish it in bad times, and it is consistent across various systems. For example, a financial institution, a wireless communications company and a hospital can all rely on the same identifier for widely divergent purposes, all to help ensure that the individual before them is the person they believe is before them. Said differently, after having verified that a consumer is legitimate, a bank, for example, can then create a unique identifier such as a customer or PIN number. But as long as the bank is dependent on third-party sources to cross check applicant data, unique identifiers must cut across external data sources.

- **CURRENT LAW PROTECTS THE PUBLIC FROM INAPPROPRIATE USE**

There are several federal and state laws and regulations that restrict the use or disclosure of SSNs, including: the Gramm-Leach-Bliley Act (15 U.S.C. 6826(b)) and its implementing regulations ("Privacy Rule"); the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); Section 5 of the FTC Act (15 U.S.C. 41-51); the Fair Debt Collection Practices Act (15 U.S.C. 1601 et seq.); the Health Insurance Portability and Accountability Act (Pub. L. 104-191); and the Drivers Privacy Protection Act (18 U.S.C. 2721 *et seq.*). Together, these laws restrict the use and display of SSNs, how they can be used, who they can (and can't) be shared with, and under what circumstances.

The use of the SSN by Credit Reporting Agencies, (CRAs), for instance, is governed by both the FCRA and, in most instances, GLB, as well. These statutes limit how and when CRAs can disclose SSNs, to whom, and under what circumstances.

For instance, many CDIA-member products are focused on helping consumers to gain access to the goods and services for which they apply –assisting a lender or other service provider in determining a consumer's eligibility. These products are regulated under the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*) as "consumer reports." Eligibility determinations include applications for any type of credit including unsecured credit, home purchases, auto financing, home equity loans, as well as for insurance of all types, employment, government benefits, apartment rentals, and for other business transactions initiated by the consumer.

The FCRA, enacted in 1970, has been the focus of careful oversight by the Congress resulting in significant changes in both 1996 and again in 2003. There is no other law that is so current in ensuring consumer rights and protections are adequate.

Similarly, some fraud detection tools are regulated under GLBA, and the use of data regarding those products is similarly circumscribed.

- **Beneficial Uses of the SSN**

Because the SSN allows for consistency across various systems and data bases, there are a number of ways that the SSN is used that benefits consumers. Further, without the availability of the SSN, many of the products and services that consumers take for granted today could become more scarce.

For instance, CDIA's members produce a range of critical consumer data products which bring great value to individual consumers, to society, and to the nation's economy. Our members design products used for determinations of a consumer's eligibility for a product or service, to prevent identity theft and fraud and to aid in the location of consumers for a variety of reasons.

1) Proper File matching: Ensuring that data goes to the right file, and is reported about the right individual

Lydia Parnes, Director of the Bureau of Consumer Protection at the Federal Trade Commission, recently testified about the importance of Social Security Numbers before the Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security:

"SSNs play a vital role in our economy, enabling businesses, government, and others to match information to the proper individual. For example, consumer reporting agencies use SSNs to ensure that the data furnished to them is placed in the correct file, and that they are providing the right credit report for the right consumer. SSNs also are used in locator databases to find lost beneficiaries, witnesses, and law violators and to collect child support and other judgments. Employers must collect SSNs for tax reporting purposes, and health care providers may need them to facilitate Medicare reimbursement." She went on to say that "the SSN is valuable in enabling entities to match information to consumers. With 300 million Americans, many of whom share the same name, the SSN presents significant advantages as a means of identification because of its uniqueness and permanence."

Financial institutions and others rely on full and complete information from credit bureaus. Complete information is necessary if the appropriate information is to be placed in the proper consumer account. As an example, a financial institution may obtain information from a credit bureau on its customer named Tom Jones. As you can imagine, there are thousands of Tom Joneses in the country. In fact, it is likely that many Tom Joneses share the same last four digits of their SSN. Therefore, a report with information pertaining to Tom Jones with the last four digits of 1234 may not provide the financial institution with sufficient information to determine to WHICH Tom Jones the report refers.

SSNs, therefore, help to ensure that our members are more likely to load data to the correct file with a high degree of precision. This is particularly true where a new account has been opened and is being added to the consumer's file for the first time. Consumer reporting agencies of all types have, under the Fair Credit Reporting Act, a duty to maintain reasonable procedures to ensure the maximum possible accuracy of the file; SSNs help them meet this requirement.

SSNs also help to ensure that the proper consumer's file is produced when a consumer applies for a benefit under the FCRA. If a consumer reporting agency cannot, with precision, identify the proper file of the consumer, it returns a message to the creditor indicating that no record was found. This result would likely lead to far higher credit denials for consumers due to the inability of the creditor to review the consumer's credit history. Said differently, the Fair Credit Reporting Act certainly does not contemplate the consumer reporting agency "taking a guess" as to which consumer's file must be accessed and thus this current liability coupled with the absence of the SSN would seriously impinge on the way in which credit is granted in this country today.

2) Identity Verification to Prevent Identity Theft and Fraud

A number of CIDA members produce products that are used by financial institutions, insurance companies and others to verify the identity of an individual and ensure that the person they are interacting with is who they say they are. These products are very effective in detecting and preventing identity theft and financial fraud before it happens.

The SSN helps businesses to prevent fraud by cross-checking applicant data against various other data sources in order to authenticate the consumers' identity. Absent the use of an SSN, these systems will be far less likely to trigger security protocols, which prevent the crime of identity theft.

In 2004, the GAO conducted a study on Social Security Numbers, and concluded that "information resellers, credit reporting agencies and health care organizations use social security numbers to build tools that verify an individual's identity or match existing records since there is no widely accepted alternative." The report further states that "restricting business access to social security numbers would hurt customers and possibly aide identify thieves since it would be more difficult for business to verify an individual's identity."

3) Other specific products and services are enabled and enhanced through the availability of the SSN:

Access to home ownership: Every homeowner benefits from a credit reporting system that reduces the costs of all mortgage loans by a full two percentage points, thus putting literally thousands of dollars in disposable income into their pockets. Homeownership is no longer a luxury of the well-to-do, but is a truly

democratized American dream enjoyed by nearly seventy percent of the population.[2] The SSN helps to facilitate the efficient operation of this system, as described above.

Child support payment enforcement: Access to SSNs dramatically increases the ability of child support enforcement agencies to locate non-custodial, delinquent parents (often reported in the news with the moniker "deadbeat dads"). 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. Child support enforcement agencies report that their efforts are far more effective when they have access to the parent's SSN. One agency reports that they are able to locate fully 80% more delinquent non-custodial parents when the SSN is available, and the Association for Children for Enforcement of Support (ACES), a private child support recovery organization, has stated that social security numbers are the most important tool for locating parents who have failed to pay child support.

Locator Services - SSNs are used routinely by law enforcement to locate missing children, fugitives and witnesses to crimes. The ability to conduct an information search using an SSN is essential. Restrictions on access to SSNs in government records would hamper the ability of law enforcement to obtain this vital information. Further a number of states report that use of SSNs to match across data bases has greatly reduced entitlement fraud. For example, Pension Benefit Information (PBI), a private company that locates former employees that are due pension benefits, has indicated that in many cases the SSN becomes the only link between an employer and their former employees with vested benefits. Employees move, marry and change their name, but the one thing that remains constant is their SSN.

Locating sex offenders—SSNs are used to locate registered and unregistered sex offenders. There are over 560,000 sex offenders in the U.S. Approximately twenty-four percent of these individuals fail to comply with address registration requirements mandated by law. Access to SSNs allows law enforcement to locate sex offenders even when the registration address has not been kept current.

Employment/security screening: As discussed above, SSNs serve as vital links among disparate records that help businesses verify prospective employees' identities and conduct thorough, accurate background checks to ensure workplace safety and business security.

Small business B-to-B transactions: An SSN is the key business entity identifier to virtually all sole proprietorships or partnerships; as a result, SSNs are necessary to facilitate business-to-business transactions between small businesses.

Securitized credit markets: Confidence in the U.S. securities market is made possible by accurate financial histories compiled using the SSN as a key identifier. Restricting use of the SSN could undermine confidence in these securities, resulting in substantially higher consumer costs for credit, including mortgages and auto loans.

Insurance fraud prevention—Insurance companies use public record information compiled using social SSNs to detect fraudulent insurance claims. According to the National Fraud Center, the average American household pays $200 to $400 a year in additional insurance premiums to offset the cost of fraud. This cost would likely increase if companies do not have the information they need to detect and prevent fraud.

4) Additionally, without the use of the SSN, consumers would suffer harm:

Incomplete data harms consumers: There would likely be an decrease in the ability of consumer reporting agencies to properly match incoming information to the correct consumer about whom the information relates. Think about the consequence to consumers of having a consumer credit report that does not contain all of the accounts that they pay on time and which makes them eligible for the lowest cost loans.

Incomplete data harms our banking system: The absence of the SSN would also put at risk the safety and soundness of lending decisions due to less information being included in consumer credit reports due to data matching problems.

Incomplete data prevents consumer access to goods and services: Think about the consequence for consumers when a consumer reporting agency cannot locate the proper file on a consumer and thus a lender, insurer or other service provider wanting to do business with the consumer has to deny the application, or the consumer has to pay higher rates.

- **INFORMATION SECURITY AND THE SSN**

As discussed above, the use of data like the SSN actually helps to prevent fraud and identity theft, by enabling better authentication of consumers, so that a lender knows that a loan applicant is you, and not an identity thief.

However, concerns have been raised that the SSN is a "key," and all a potential identity thief needs to "unlock" a consumer's credit – that simply is not true.

There are 2 basic types of financial fraud that may be perpetrated against an individual. The first is fraud against a person's existing accounts, such as credit card fraud, where a thief obtains your account number or credit card, and charges items to that card or drains your existing bank account. While those instances are problematic, and may cause a consumer some stress while getting those problems rectified, they do not cause any long-term harm to the consumer; they suffer no financial liability, and such fraud does not impact their credit in any way. More than 2/3rds of all "identity theft," as identified by the FTC, falls into this category.

The second, and more serious type of financial fraud is what we term "real name" fraud, where a fraudster obtains a person's sensitive personal information, such as their SSN and other information, and somehow fools a lender into thinking that they are that person. This may enable the thief to open new credit accounts in a victim's name without the knowledge of the victim. While the victim is ultimately not responsible for the financial harm, this type of fraud can have serious repercussions for the victim.

As discussed, while obtaining a person's SSN may potentially make them susceptible to identity theft, it takes a lot more information, and the ability to use it in a way that thwarts the fraud detection tools in place, to commit "real" identity theft. Further, the SSN plays a major role in helping to stop such fraud, as well.

The availability of MORE information, rather than less, is the key to reducing reliance on the SSN. Database matching is often like finger-print matching – the more unique data points there are, the more ability there is to identify and authenticate an individual. Further, each piece of data reduces the reliance on every other piece. However, Congress has limited the use of alternatives, increasing the reliance on SSNs.

For instance, there are other unique identifiers that could help reduce the reliance on SSNs, such as Driver's License numbers, that do exist. However, the Driver's Privacy Protection Act (DPPA) has limited the ability of data base companies to utilize those to supplement, or even supplant, the use of SSNs.

Wireless cell phone numbers also have the potential to serve that purpose. However, while those numbers are not used for telemarketing, Congress has, in other contexts, considered limiting the utility of these numbers for identification and fraud detection purposes, as well.

- **PUBLIC RECORDS AND THE SSN**

Public records play a vital in our society and bring value to the consumer. Bankruptcy records, tax liens and judgments are part of consumer "credit" reports used by lenders to make decisions that implicate safety and soundness. Records of eviction are critical to landlords who must themselves pay the bills and

attempt to lease properties to consumers who will do the same. Validating professional licenses for employment screening agencies is yet another use of public records, as is accessing criminal histories.

Through the development of nationwide databases of public record information, our members have solved the problems inherent in having to search through tens of thousands of federal and state court houses and agency databases. In this way, the SSN is as important an identifier in a public document as it is in a private-sector database. It is a critical identifier for all of the data management reasons we discuss above. Without an SSN, a consumer can simply alter a few items of information, such as moving to a new address, or even changing a name and thus separate himself/herself from a bankruptcy record, a tax lien, a record of eviction and even a criminal history, in some cases. Clearly this is not a positive outcome for consumers or for American businesses which are on the front lines of making, for example, fair and accurate risk based lending and employment decisions, while at the same time fighting identity theft and fraud.

Some federal proposals have suggested that state agencies must limit access to the SSN. The concern of the CDIA's members is that this apparent unfunded mandate will drive under-funded state agencies to either stop requesting the SSN when processing vital records, or to simply deny all access to public records containing SSNs.

It is important that public records, including those records containing SSNs, continue to be made available. The open public records system is the cornerstone of the U.S. democracy and economy.

The debate about the presence of the SSN in public records has suggested a possible binary solution, where SSNs could be made available electronically for certain entities, but could possibly be redacted for publicly available electronic documents, though costs associated with such an unfunded mandate will have to be addressed. It is encouraging to hear state court organizations discussing strategies for protecting SSNs, and CDIA will continue to engage in these dialogues.

However, while CDIA believes that disclosure of the SSN to the general public must be addressed, we also believe that public records must be made available, including SSNs, to those with an appropriate need. Ultimately, dialogue with state and federal agencies coupled with the advancement of technologies will address concerns about public records which contain SSNs. An unfunded mandate will destabilize the system of public records which is so important to our democracy.

- **Some Additional Notes on Other Important Issues:**

Finally, there are a few additional issues I would like to highlight before I conclude:

- **Legitimate business uses:**

It is important that any restrictions imposed on the sale or display of SSNs contain exceptions for legitimate business uses such as identity verification; detecting, preventing and investigating ID theft and fraud; locating individuals; collecting child support and other lawful debts; and for any purposes permitted under the Fair Credit Reporting Act and Gramm-Leach-Bliley Act.

- **Preemption**:

Ensuring that the Social Security number issue is addressed in a uniform fashion, so that all consumers are protected, is a vital component of this debate. Any legislation that would restrict the sale or display of SSNs must contain federal preemption so that businesses are subject to a single, national law rather than having to comply with various state laws all with differing and potentially conflicting requirements.

- **Exempt Current Law**

As discussed previously, SSNs are broadly covered by a whole host of current statutes. Instead of adding an additional compliance burden on top of those laws, we would urge the Committee to exempt practices already covered under existing laws.

- **Minimize Rulemaking Authority**

Because so many business practices rely on stable laws, CDIA would urge the Committee to codify any changes to current law, to the extent possible, rather than granting broad authority to the regulatory agencies.

- **Further Assisting Identity Theft Victims: Provide the Ability to "Ping" the SSN Database**

CRAs utilize very sophisticated tools to ensure the accuracy of their systems. However, in rare cases of identity theft, it would be useful for us to have the ability to cross-check our databases to determine if a particular SSN is associated with a particular person. This would be very useful in further helping ensure the accuracy of our databases, and could help contribute to the accuracy of our databases and the ability to help correct the records of Identity Theft victims.

CONCLUSION

In conclusion, you can see that the underlying theme in the discussion of SSN uses is that of balance and ultimately ensuring the security of the number. Law that that imposes national uniform information security regulations on all who possesses the SSN in combination with a person's name and address, is the most responsible and constructive focus for Congress. In contrast, law that overreaches in attempting to limit use of the SSN is likely to merely take fraud prevention tools out of the hands of legitimate businesses at the expense of consumers.

Ironically, to prevent fraud you must be able to crosscheck information. To maintain accurate databases, you must be able to maintain a range of identifying elements. Absent the availability of the SSN, we will be less able to build accurate data bases, to accurately identify records and to help prevent identity theft through the development of fraud prevention and authentication tools.

Ultimately consumers expect us all to accomplish the goals of protecting and securing the SSN, and also ensuring the accuracy and effectiveness of databases which contain information about them.

Thank you for this opportunity to testify.

---

[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 and also collection services. As we will discuss below, the secure and protected use of the social security number (SSN) is an important key to the effectiveness of these systems and services

[2] Kitchenman, Walter., U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns., Pp. 5 (1998).