LEGISLATIVE REPORT

SOCIAL SECURITY NUMBER STUDY

REPORT PREPARED BY
THE OFFICE OF CONSUMER CREDIT COMMISSIONER
SUBMITTED NOVEMBER 2006

SOCIAL SECURITY NUMBER STUDY

PURPOSE

Section 7.04 of House Bill 955 ("HB 955") mandates a study by the Office of Consumer Credit Commissioner ("OCCC" or "agency") "to develop and evaluate proposals to limit the use of social security numbers by businesses in this state."[1] Specifically:

> SECTION 7.04. (a) The Office of Consumer Credit Commissioner, with the assistance of the attorney general, shall conduct a study to develop and evaluate proposals to limit the use of social security numbers by businesses in this state.
>
> (b) In conducting the study, the consumer credit commissioner shall receive input from credit reporting agencies, businesses, and consumer groups.
>
> (c) The consumer credit commissioner shall evaluate whether, when a business contacts a credit reporting agency for a credit check of a customer, the business and credit reporting agency should create a unique code that:
>
> (1) would allow the business to retrieve the social security number of the customer for collection purposes; and
>
> (2) would permit the business to delete the social security number of the customer from the records of the business.
>
> (d) The consumer credit commissioner shall determine the date on which the system described by Subsection (c) of this section could be implemented and the feasibility of monitoring compliance with the system.[2]

SECTION I: BACKGROUND AND HISTORY OF SOCIAL SECURITY NUMBERS

Creation of Social Security Numbers

Social security numbers (SSNs) were originally created in 1936 and were intended to be used by the federal government for purposes of tracking worker earnings and determining

[1] HB 955, 79th Leg., § 7.04(a) (2005).

[2] *See id.* § 7.04(a)-(d).

eligibility for social security benefits.[3] However, over time, the SSN has evolved into a unique identifier used widely by businesses, governmental entities, and the public.

American Society's Dependence on SSNs

In the year 2000, it was estimated that more than 277 million people had a unique SSN.[4] Considering the fact that millions of Americans share the same last name (e.g. 2.5 million with the last name Smith; 3 million with the last name Jones), as well as many common first names resulting in common naming combinations, SSNs have been found useful in correctly identifying individuals in numerous contexts.[5] In addition, SSNs are the best method of identification in situations where last names have changed due to marriage and divorce, addresses have changed, nicknames or initials are used, and where names are shared due to generational family naming conventions.[6]

Use of SSNs by Businesses, Governmental Entities, and the Public

Private Businesses

Businesses and governmental entities typically use SSNs for two main purposes: (1) "to locate records for routine internal activities, such as maintaining and updating account information"; and (2) "to facilitate information exchanges with other organizations."[7] Examples of private businesses that commonly use SSNs include health care service organizations, financial services businesses, and information brokers.[8] According to the United States General Accounting Office, "the primary use of the SSN by information resellers, CRAs [consumer reporting agencies], and health care organizations alike was to help verify the identity of an individual."[9]

---

[3] *Social Security: Use of the Social Security Number is Widespread*, Statement of Barbara D. Bovbjerg, Associate Director; Education, Workforce, and Income Security Issues; Health, Education, and Human Services Division; United States General Accounting Office, Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, p. 1 (GAO/T-HEHS-00-111; May 9, 2000).

[4] *Id.*

[5] Hearing on "Social Security Number High-Risk Issues," Statement of Stuart K. Pratt, Consumer Data Industry Association ("CDIA"), Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, p. 3, (March 30, 2006).

[6] *Id.* at 2-4.

[7] GAO/T-HEHS-00-111, p. 3.

[8] *Id.* at 5.

[9] *Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information*, Barbara D. Bovbjerg, Director;

Health care providers use SSNs "to track patients' medical care across multiple providers," "to integrate patients' records when providers merge," and as a back-up identifier when patients forget or do not know their primary identifier as issued by the health care organization.[10]

Financial services business, such as banks, credit card companies, insurance companies, and collection agencies, routinely use SSNs.[11] Although the SSN is typically not used as the customer's primary identifier, financial businesses often use customer SSNs to request information from credit bureaus.[12] In turn, the credit reporting agencies use the SSNs "to update individuals' credit records with the monthly reports of credit and payment activity creditors send," and "to retrieve credit reports on individuals."[13]

With the volume of information readily available via the Internet, information brokers have grown in numbers and harnessed the market of "buy[ing] and sell[ing] information from and to a variety of public and nonpublic sources."[14] Information brokers often purchase the following types of records, which may contain SSNs: "public records of bankruptcy, tax liens, civil judgments, real estate ownership, driving histories, voter registration, and professional licenses."[15] Large information brokers or resellers "usually obtain SSNs from their business clients" and then use the SSNs as an identification tool "for purposes such as employment screening, credit information, and criminal history."[16]

Governmental Entities

Many federal governmental entities require the use of SSNs in order for individuals to comply with legal requirements or to apply for certain federal programs. For example, SSNs must be provided to the Internal Revenue Service ("IRS") in order for individuals to file federal tax income returns, and the Social Security Administration ("SSA") requires SSNs when individuals apply for federal benefits, such as Supplemental Security Income ("SSI"), food stamps, Temporary Assistance for Needy Families ("TANF"), and

---

Education, Workforce, and Income Security Issues; Health, Education, and Human Services Division; United States General Accounting Office, Report to the Chairman, Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, p. 9 (GAO-04-11; January 22, 2004).

[10] GAO/T-HEHS-00-111, p. 5.

[11] *Id.* at 6.

[12] *Id.*

[13] *Id.*

[14] *Id.* at 6-7.

[15] *Id.* at 7.

[16] GAO-04-11, pp. 2-3.

Medicaid.[17] State agencies utilize SSNs "to identify individuals who pay taxes, receive general public assistance, own a vehicle or drive."[18] In addition, state agencies also use SSNs in the licensing of professionals (e.g. lawyers and teachers), as well as in licensing regulated lenders and credit providers, such as the OCCC's licensees (e.g. small loan companies, second lien home equity lenders, pawnshops, and motor vehicle sales finance dealers).

The Public

Many of the public's uses of SSNs are dictated by the requirements of businesses or governmental entities, as outlined above. For example, in order to file one's personal income taxes, to apply for a government assistance program, or to obtain a professional license, members of the public are often required to provide SSNs. However, the public also uses SSNs for other purposes, including background checks on daycare workers and babysitters, or finding long lost relatives.

The clients of large information resellers typically encompass either individual public persons themselves or parties working on behalf of members of the public, such as law firms and some private businesses.[19] Examples of specific uses of personal information, including SSNs, by particular clients of large information brokers include the following:

> [L]awyers, debt collectors, and private investigators may request information on an individual's bank accounts and real estate holdings for use in civil proceedings such as divorce; automobile insurers may want information on whether insurance applicants have been involved in accidents or have been issued traffic citations; employers may want background checks on new hires; pension plan administrators may want information to locate pension beneficiaries; and individuals may ask for information to help locate birth parents.[20]

Although not all of the above purposes for purchasing and using SSNs are directly performed for the members of the public, most of these uses ultimately result in benefits to the public at large (e.g. protection of other drivers by requiring comprehensive insurance with high limits for risky drivers; protection of co-workers by not hiring employees with criminal histories that could result in repeated behavior endangering others; location of beneficiaries who may not otherwise be aware of benefits due; location of birth parents to assist adopted children with medical histories).

---

[17] GAO/T-HEHS-00-111, p. 2.

[18] *Id.* at p. 4.

[19] GAO-04-11, p. 5.

[20] *Id.*

Federal Laws Regulating Use of SSNs

Due to the widespread use of and dependence on SSNs in American society, as well as rising incidences of identity theft, several federal laws have been enacted to regulate the use of SSNs. The first of these laws was the Privacy Act of 1974 (5 U.S.C. § 552a, *et seq.*), which outlines restrictions for federal agencies in the collection and disclosure of personal information, including SSNs.[21] The Privacy Act requires federal agencies requesting SSNs to provide the following: "the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;" "the principal purpose or purposes for which the information is intended to be used;" "the routine uses which may be made of the information"; and "the effects on [an individual], if any, of not providing all or any part of the requested information."[22]

Federal laws that regulate the use of SSNs, and that are directly related to the financial services industry, include the Gramm-Leach-Bliley Act ("GLBA"; 15 U.S.C. § 6801, *et seq.*), the Fair Credit Reporting Act ("FCRA"; 15 U.S.C. § 1681, *et seq.*), and the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"). GLBA outlines procedures for the protection and disclosure of nonpublic personal information, but it is only applicable to "financial institutions" (e.g. banks, insurance providers, investment brokers, and financial advice providers) and contains many exclusions permitting the sharing of information without the consent of the consumer.[23] FCRA and the FACT Act, which amended FCRA, both strive to maintain the accuracy of credit reports while ensuring the privacy of the consumer information contained in credit reports.

Examples of other federal laws limiting the use of required SSNs include the Internal Revenue Code of 1986 (Title 26, U.S.C.), the Social Security Act (42 U.S.C. § 301, *et seq.*), and the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (Pub.L. 104-193; an expansion of the Federal Parent Locator Service).[24] Additionally, some laws provide protection for sensitive consumer information, which also protects SSNs. These laws include the Fair Debt Collection Practices Act (15 U.S.C. § 1601, *et seq.*), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA;" Pub.L. 104-191), and the Drivers Privacy Protection Act ("DPPA"; 18 U.S.C. § 2721, *et seq.*).[25]

The following is a table compiled by the United States General Accounting Office regarding the particular restrictions required by GLBA, DPPA, and HIPAA.[26]

---

[21] GAO/T-HEHS-00-111, p. 3.

[22] Privacy Act of 1974, 5 U.S.C. § 552a(e)(3).

[23] *See generally*, Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, *et seq.*

[24] GAO/T-HEHS-00-111, p. 3.

[25] Pratt Statement, p. 10.

[26] GAO-04-11, p. 14.

Aspects of Federal Laws That Affect Private Sector Disclosure of Personal Information	
Federal laws	**Restrictions**
Gramm-Leach-Bliley Act	Creates a new definition of personal information that includes the SSN and limits when financial institutions may disclose the information to non-affiliated third parties.
Drivers Privacy Protection Act	Prohibits disclosing personal information from a motor vehicle record that includes SSN except for purposes permissible under the law.
Health Insurance Portability and Accountability Act	Protects the privacy of protected health information that includes SSNs and restricts health care organizations from disclosing such information to others without the patient's consent.

Public Display of and Access to SSNs Reduced in Texas and Other States

While private businesses and governmental entities have been the objects of most regulation concerning the use of SSNs, the public's access to SSNs has also been reduced. One example involves a change in Texas law concerning confidential information contained in real property records. According to Texas Property Code, § 11.008, individuals now have the option to remove SSNs (or driver's license numbers) from real property records so that these numbers will be not be available online or subject to a public information request.[27] Furthermore, the Texas Public Information Act ("TPIA") itself was amended in 2005 and now provides that Texas governmental bodies may not disclose the SSNs of living persons in response to a public information request under TPIA.[28]

Section 35.58 of the Texas Business and Commerce Code contains several key provisions restricting the use or display of SSNs.[29] With the exception of governmental bodies, Texas law prohibits the display of SSNs on cards or other devices used to access goods or services.[30] Section 35.58 also states that individuals cannot be required to transmit their SSNs over the Internet unless done via a secure connection or the number is encrypted.[31]

---

[27] TEX. PROP. CODE, § 11.008(b) (amend. 2005).

[28] TEX. GOV'T CODE, § 552.147 (eff. 2005).

[29] TEX. BUS. & COM. CODE, § 35.58 (eff. 2005).

[30] *See id.* § 35.58(a)(2).

[31] *See id.* § 35.58(a)(3).

Access to Internet Web sites also cannot require the use of SSNs unless an additional authentication device is also required for access (e.g. password, PIN).[32] Unless required by state or federal law, printed mailings of SSNs are restricted to the following purposes: "as part of an application or enrollment process"; "to establish, amend, or terminate an account, contract, or policy"; or "to confirm the accuracy of [an SSN]."[33]

In addition to Texas, at least five other states have enacted legislation to restrict private sector uses of SSNs: Arizona, California, Georgia, Missouri, and Utah.[34] The State of California appears to be taking the lead concerning efforts to protect consumer privacy.[35] In fact, due to California's SSN legislation, some national companies have discontinued certain uses of SSNs (e.g. display on health benefit cards) in all of their locations without regard to the particular state laws for each location.[36] Moreover, some states (e.g. Vermont and North Dakota) have enacted legislation with even stronger protections for consumers beyond those found in GLBA and FCRA.[37]

SECTION II: RELIANCE ON SSNS IN COMMERCE AND RISING IDENTITY THEFT CONCERNS

Balancing Interests: Use of SSNs in Commerce vs. Consumer Privacy

While SSNs have been useful in accurately identifying individuals for various legal purposes, SSNs have also been abused by criminals in stealing the identities of members of the public. In fact, the Federal Trade Commission ("FTC") has compiled statistics for the years 2002 - 2005 regarding identity theft and fraud, broken down by different types. The Texas statistics from the FTC's Identity Theft Clearinghouse Data are attached as an Appendix to this report. Clearly, with the alarming increase in the rate of identity theft, policymakers are justifiably concerned in searching for solutions to this growing problem. The advent of the SSN as the magic code to entry into much of a consumer's financial life provides great access and convenience to consumers in the financial services marketplace, but that wide access also carries with it grave dangers in universal use of SSNs and their associated risk.

Each time that a consumer's SSN is shared or disseminated represents a vulnerability. That vulnerability is the opportunity for the consumer's SSN to be improperly accessed or stolen. Nonetheless, "[w]ithout the ability to use SSNs as a personal identifier and fraud prevention tool, the granting of credit and the provision of other financial services would

---

[32] *See id.* § 35.58(a)(4).

[33] *See id.* § 35.58(a)(5) and (f).

[34] GAO-04-11, p. 20.

[35] *Id.* at 22.

[36] *Id.*

[37] *Id.*

become riskier and more expensive and inconvenient for consumers."[38] This pernicious problem presents a careful balancing act that must be performed between the benefits of using the SSN to promote commerce and the risks of identity theft and inappropriate access.

National Identification System and the REAL ID Act of 2005

When the system of SSNs was created, it was never intended for the type of widespread commerce uses that it embodies today. Some have argued that replacing the SSN with a type of national identification number is a natural solution to reduce the reliance on SSNs as a verification method. SSNs were never intended to be used for the purpose of consumer verification. A national identification system, with presumably a unique identification number to accompany the identification card, has "long been advocated as a means to enhance national security, unmask potential terrorists, and guard against illegal immigrants."[39] Many countries have adopted such a system, but the United States continues to debate a national identification system.[40]

Meanwhile, the U.S. Congress has passed the REAL ID Act of 2005, "which mandates federal requirements for driver's licenses."[41] Some have argued that this act creates a *de facto* national identification system.[42] The states are now responding with estimates of the implementation costs. Although Congress estimated the national implementation cost at approximately $100 million, California alone estimates its costs at $500 million over five years.[43] Certainly, an alternative unique identification number that could be broadly applied across the United States carries with it heavy costs and may not be altogether successful in preventing identity theft. On a statewide level, requiring an alternate unique identification system does not seem to be feasible within the context of modern commerce.

---

[38] Prepared Statement of the Federal Trade Commission on Identity Theft and Social Security Numbers, Statement of Joel Winston, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, p. 3, (March 30, 2006).

[39] *National ID Cards and REAL ID Act*, Electronic Privacy Information Center, http://www.epic.org/privacy/id_cards/, accessed September 25, 2006.

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.*

SECTION III: THE CREDIT VERIFICATION PROCESS AND COMMERCIAL USES OF SSNS

Assuming that an alternative unique identification system is not feasible, how then are SSNs being used and how can that use minimize the opportunity for unauthorized access and disclosure of SSNs?

Use of SSNs in the Credit Verification Process

As noted above, businesses routinely use SSNs to verify a potential customer's identity and to inquire into the consumer's creditworthiness in order to determine whether and under what conditions that a business may engage in transactions with a consumer. Often a business may obtain a credit report.

A typical authorized use of a credit report occurs when a consumer applies for credit from a financial institution. The institution takes an application from the consumer that contains certain information, including nonpublic personal information. Some of this information, including almost always the SSN, is used to verify the identity of the person applying for credit and to obtain a credit report from one or more credit reporting agencies. The financial institution will make a credit decision to approve or deny the application for credit. If approved, a customer relationship is established and the financial institution may report to the credit reporting agency regarding the consumer's payment history.

Other Commercial Uses of SSNs Including Re-Verification

Other uses of nonpublic personal information, including SSNs, have become commonplace when a consumer establishes a business relationship with other retailers or vendors who are not "financial institutions,"[44] as defined under GLBA. This may include utility companies, rental property management firms, and wireless communication companies.

A particular practice that has raised a high level of concern is the re-verification of a consumer. Consumers frequently encounter a request to provide their SSNs to a business where they already have an established relationship in an attempt to access certain information about an account. The purpose of this procedure is to provide a consumer with quick and reasonable access to account information by attempting to authenticate the identity of the consumer utilizing the SSN. This re-verification or authentication practice, while well-intentioned, exposes consumers to another vulnerability point where identity thieves have the opportunity to improperly obtain SSNs.

[44] For purposes of GLBA, 15 U.S.C. § 6809 defines a "financial institution" as a business which engages in the financial activities outlined by 12 U.S.C. § 1843(k).

Alternative Re-Verification Methods

Ensuring data, including SSNs, is secure should be a top priority for everyone. Businesses and governmental entities that maintain nonpublic personal information have an obligation to safeguard the data in their custody and control. Many businesses use methods other than SSNs in order to re-verify the identity of consumers, such as Personal Identification Numbers ("PINs"), account numbers, passwords, or truncated SSNs. These methods of authentication provide consumers with greater protection and less risk of vulnerability to identity theft.

Data Encryption

However, when SSNs are still utilized for identification and re-verification of consumers, the most significant tool for accomplishing data security is the use of encryption. Encryption is defined by the American Heritage Dictionary as: "1. To put into code or cipher. 2. *Computer Science*. To alter (a file, for example) using a secret code so as to be unintelligible to unauthorized parties."[45] "Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext."[46] By encrypting files or data, only authorized users will have access to the information.

Encryption can be performed using different algorithms or standards. The federal government currently lists three (3) approved encryption algorithms: AES, Triple DES, and Skipjack, and has issued publications concerning all three standards.[47] "Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235)."[48] These three algorithms or encryption standards specify "both enciphering

---

[45] *American Heritage Dictionary of the English Language*, Houghton Mifflin Co., definition of "encryption," (4th ed. 2004).

[46] *Announcing the Data Encryption Standard*, Federal Information Processing Standards ("FIPS") Publication 46-3, National Institute of Standards and Technology, p. 1, (October 25, 1999).

[47] *Cryptographic Toolkit- Encryption*, National Institute of Standards and Technology, http://csrc.nist.gov/CryptoToolkit/Encryption.html, accessed October 10, 2006.

[48] *Announcing the Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, National Institute of Standards and Technology, p. i, (November 26, 2001).

and deciphering operations which are based on a binary number called a key."[49] Each FIPS-approved encryption algorithm is discussed in turn below.

First, the Advanced Encryption Standard ("AES") algorithm is the best encryption standard available today, and it "is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits."[50] In fact, "this standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it provides the desired security for commercial and private organizations."[51]

Second, the Triple Data Encryption Algorithm ("TDEA" or "Triple DES") incorporates a triple use of the now obsolete and unapproved Data Encryption Standard ("DES"), which was originally approved by the federal government in 1977.[52] As of May 2005,[53] "[t]he use of DES [by the federal government] is permitted only as a component function of TDEA."[54] Currently, the federal government is in a transition period, allowing a gradual conversion from the use of Triple DES to AES.[55]

Third, Skipjack actually refers to the "SKIPJACK cryptographic algorithm" and a "Law Enforcement Access Field (LEAF) creation method" which are utilized "for encrypting and decrypting telecommunications."[56] The specifics of Skipjack are classified by the National Security Agency.[57]

Of course, while the Skipjack encryption standard may not be used outside of the federal government, the other two approved encryption methods (AES and Triple DES) are available to commercial and private businesses. The three major credit reporting agencies require that consumer information be sent to them in a standardized encryption format.

---

[49] FIPS Publ. 46-3, p. 1.

[50] FIPS Publ. 197, p. i.

[51] *Id.*

[52] *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, NIST Special Publication 800-67, National Institute of Standards and Technology, p. vii, (May 2004).

[53] *Cryptographic Toolkit- Encryption*, National Institute of Standards and Technology, http://csrc.nist.gov/CryptoToolkit/Encryption.html, accessed October 10, 2006.

[54] NIST Special Publ. 800-67, p. vii.

[55] *Id.* at viii.

[56] *Announcing the Standard for Escrowed Encryption Standard (EES)*, Federal Information Processing Standards Publication 185, National Institute of Standards and Technology, (February 9, 1994).

[57] *Id.*

The credit bureaus require the use of either AES or Triple DES with at least 128-bit encryption. The two are widely used to protect sensitive financial data.[58]

Fraud Detection

Another area relating to data security is that of fraud detection. According to testimony provided by the Consumer Data Industry Association to the Subcommittee on Social Security of the House Ways and Means Committee, the uses of fraud detection tools include the location and verification of information for the public and private sector, as well as the identification of fraud.[59] Although fraud detection tools contain many differences, the following is an outline of the four key models used:

- "**Fraud databases** - check for possible suspicious elements of customer information. These databases include past identities and records that have been used in known frauds or are on terrorist watch lists, suspect phone numbers or addresses, and records of inconsistent issue dates of SSNs and the given birth years.

- **Identity verification products** - crosscheck for consistency in identifying information supplied by the consumer by utilizing other sources of known data about the consumer. Identity thieves must change pieces of information in their victim's files to avoid alerting others of their presence. Inconsistencies in name, or SSN associated with a name raise suspicions of possible fraud.

- **Quantitative fraud prediction models** - calculate fraud scores that predict the likelihood an application or proposed transaction is fraudulent. The power of these models is their ability to assess the cumulative significance of small inconsistencies or problems that may appear insignificant in isolation.

- **Identity element approaches -** use the analysis of pooled applications and other data to detect anomalies in typical business activity to identify potential fraudulent activity. These tools generally use anonymous consumer information to create macro-models of applications or credit card usage that deviates from normal information or spending patterns, as well as a series of applications with a common

---

[58] *Credit Bureaus to Require Data Encryption,* American Banker, (September 23, 2005).

[59] Hearing on "Social Security Number High-Risk Issues," Statement of Stuart K. Pratt, Consumer Data Industry Association ("CDIA"), Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, p. 8, (March 30, 2006).

work number or address but under different names, or even the identification and further attention to geographical areas where there are spikes in what may be fraudulent activity."[60]

The testimony also states that over three-fourths (78%) of the users of fraud detection tools are financial businesses.[61] Nevertheless, multiple users of fraud detection tools exist outside of the financial business world, such as:

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

- **Private use -** Journalists use fraud detection services to locate sources, attorneys to find witnesses, and individuals use them to do background checks on childcare providers."[62]

Data Security Requirements Imposed on Businesses

In addition to securing SSNs and other nonpublic personal information during their transmission in initial transactions or during the re-verification process, the proper storage and deletion of records containing SSNs is another key element involved in data security.

During the 2005 regular session, the Texas Legislature passed Senate Bill 122 ("SB 122"), also known as the "Identity Theft Enforcement and Protection Act."[63] SB 122 added a new chapter to the Texas Business and Commerce Code, Chapter 48, which outlines what is considered to be an unauthorized use of identifying information and provides for civil penalties.[64] Section 48.102 is entitled, "Business Duty to Protect and Safeguard Sensitive Personal Information," and includes guidelines for businesses in destroying "customer records containing sensitive personal information."[65] Such records must be destroyed by "shredding," "erasing," or "otherwise modifying the sensitive personal information in the records to make the information unreadable or undecipherable through any means."[66] In addition, § 48.103 requires that notifications be

---

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] SB 122, 79th Leg., § 2 (2005); codified at TEX. BUS. & COM. CODE § 48.001, *et seq.*

[64] TEX. BUS. & COM. CODE § 48.001, *et seq.* (eff. 2005).

[65] *See id.* § 48.102(b).

[66] *See id.*

given under certain procedures following a breach of security involving computerized data.[67]

Whether it is done through encryption or other means, the security of SSNs and other nonpublic personal information must be a top priority.

SECTION V: RECOMMENDATIONS

Considerations for the Texas Legislature

In conducting this study, the OCCC sought input from credit reporting agencies ("CRAs"), businesses, and consumer groups, as required by the charge under HB 955.[68] HB 955 asks whether CRAs, in conjunction with businesses, should create unique codes or "tags" intended to allow the retrieval of SSNs upfront for collection purposes and the subsequent deletion of SSNs from the business records.[69] According to CRAs providing input to the agency, the creation of a statewide system of unique codes or tags would not be a practical or viable option, as the unique code would have to be added on a business-by-business basis. Furthermore, a business's statewide unique code or tag would not cross state lines and would be unusable outside of Texas. In addition, although the costs of implementing a national identification system are estimated to be staggering (as discussed *supra* under "National Identification System and the REAL ID Act of 2005"), the expenses required to establish a statewide system, as envisioned by HB 955, are expected to be even proportionately higher.

Therefore, the OCCC believes that it would not be feasible for CRAs in conjunction with businesses, to create a unique code or "tag" intended to allow the initial, one-time retrieval of a consumer's SSN for collection purposes and the deletion of that SSN from the business's records upon receipt of the consumer's credit report from the CRA marked with the unique code or tag.

Alternatively, the Texas Legislature may consider regulating the conduct of business entities that "authenticate" a customer's identity after the establishment of a customer relationship. This may include either prescribing or prohibiting certain business practices of entities, other than financial institutions,[70] that use SSNs for re-verification of existing customers, such as the use of customer-chosen passwords, issuer-based or customer-chosen PIN numbers, or a combination of other unique identifiers (e.g. mother's maiden name or date of birth). By providing private businesses a choice of numerous re-verification methods, a recommendation could be made to significantly limit or even

---

[67] *See id.* § 48.103.

[68] HB 955, 79th Leg., § 7.04(b) (2005).

[69] *See id.* § 7.04(c).

[70] Financial institutions are subject to the privacy requirements of GLBA and FCRA, as amended by the FACT Act.

possibly eliminate the dependence on SSNs or even truncated SSNs for re-verification of existing customers.

In addition, the legislature can review standards for the safeguarding of nonpublic information. These standards found in Chapter 48 of the Texas Business and Commerce Code establish a business duty to protect and safeguard sensitive information. This addition by the 79th Texas Legislature provides good standards for the safeguarding of information; however, there may be opportunities to strengthen this area of law to some extent. One approach would be to consider a standard for business entities that collect nonpublic personal information to have an affirmative and continuing obligation to respect the privacy of their customers and to protect the security and confidentiality of those customers' nonpublic personal information. Another type of standard that may be considered would be one requiring enhanced use of encryption technology when electronically transferring SSNs.

President's Identity Task Force

The President commissioned a task force on identity theft to restrict disclosure of SSNs and reduce reliance on the use of SSNs. One of the interim recommendations released in September 2006 acknowledges the difficulty of authenticating the identity of individuals and supports the development of technological solutions.[71] The President's Identity Task Force states the following in its recommendation:

> Developing Alternative Methods of "Authenticating" Identities-
>
> Developing reliable methods of authenticating the identities of individuals, such as "biometrics," would make it more difficult for identity thieves to misuse existing accounts or open new accounts using other individuals' information. The Task Force recommends that agencies gather together academics, industry experts and entrepreneurs who are exploring ways to encourage greater development and use of authentication systems, and hold a workshop or workshops focused on developing and promoting improved means of authenticating the identities of individuals.[72]

This key recommendation aligns completely with the objectives, purpose, and findings of this report. The State of Texas should closely monitor and encourage the development of this type of technology to replace the reliance on SSNs as an authentication tool in commerce. Data security via encryption and other methods should be the focus of future efforts to limit the use of SSNs by Texas businesses.

---

[71] *Identity Theft Task Force Announces Interim Recommendations,* Press release, U.S. Department of Justice, (September 19, 2006).

[72] *Id.*

APPENDIX - SOCIAL SECURITY NUMBER STUDY
FEDERAL TRADE COMMISSION - IDENTITY THEFT CLEARINGHOUSE DATA
CALENDAR YEARS 2002 - 2005

Types of Identity Theft or Fraud Reported	2005		2004		2003		2002	
	Number of Claims	% of Total	Number of Claims	% of Total	Number of Claims	% of Total	Number of Claims	% of Total
National Totals (All States)	255,565	N/A	246,570	N/A	214,905	N/A	161,819	N/A
Texas Total Claims (% of Nat'l)[1]	26,624	10.4%	26,454	10.7%	20,634	9.6%	14,357	8.9%
Credit Card Fraud	5,591	21.0%	5,555	21.0%	5,778	28.0%	5,599	39.0%
Phone or Utility Fraud	4,260	16.0%	3,968	15.0%	3,301	16.0%	3,159	22.0%
Bank Fraud	5,857	22.0%	5,555	21.0%	4,333	21.0%	3,159	22.0%
Employment Related Fraud	5,698	21.4%	6,984	26.4%	4,209	20.4%	2,297	16.0%
Gov't Documents or Benefits*	**2,396**	**9.0%**	**2,381**	**9.0%**	**1,857**	**9.0%**	**1,292**	**9.0%**
Loan Fraud	1,331	5.0%	1,323	5.0%	1,238	6.0%	861	6.0%
Other ID Theft	5,857	22.0%	5,026	19.0%	3,508	17.0%	1,866	13.0%
Attempted ID Theft	1,118	4.2%	1,138	4.3%	1,259	6.1%	1,005	7.0%
Texas Totals[2]	32,109	120.6%	31,930	120.7%	25,483	123.5%	19,238	134.0%

Notes:

1. Second line includes total Texas claims for each year and corresponding percentage reflecting proportion of national claims occurring in Texas. The remaining percentages all reflect a breakdown of the claims within Texas and are expressed as a percentage of the Texas total claims numbers.

2. Total claims reported and percentages are based on the number reported. Percentages add to more than 100% and totals are greater than second line because approximately 20 - 22% of victims from Texas reported experiencing more than one type of identity theft.

*Subtypes of ID Theft or Fraud Reported in Texas Under Gov't Docs or Benefits	2005		2004		2003		2002[3]	
	Number of Claims	% of TX Total	Number of Claims	% of TX Total	Number of Claims	% of TX Total	Number of Claims	% of TX Total
Total Texas Claims	26,624	N/A	26,454	N/A	20,634	N/A	14,357	N/A
Fraudulent Tax Return	1,158	4.4%	1,018	3.9%	908	4.4%		
Driver's License Issued/Forged	626	2.4%	754	2.9%	557	2.7%		
Gov't Benefits Applied For/Received	399	1.5%	288	1.1%	206	1.0%		
Social Security Card Issued/Forged	53	0.2%	93	0.4%	62	0.3%		
Other Gov't Document Issued/Forged	160	0.6%	228	0.9%	83	0.4%		
Unspecified	0	>.01%	0	>.01%	41	0.2%		
Total for Subtype (Gov't Doc's)[4]	2,396	9.0%	2,381	9.0%	1,857	9.0%	1,292	9.0%

Notes (continued):

3. Subtypes not reported for 2002.

4. Total claims reported and percentages are based on the number reported. Percentages add to more than total for subtype because approximately 20 - 22% of victims from Texas reported experiencing more than one type of identity theft.

Source: Federal Trade Commission Identity Theft Clearinghouse Data, http://www.consumer.gov/idtheft/id_federal.htm, accessed October 13, 2006.