Staff Summary of Comments and Information Received Regarding the Private Sector's Use of Social Security Numbers

Division of Privacy and Identity Protection, Bureau of Consumer Protection Federal Trade Commission

November 2007

I. Introduction[1]

Virtually every American citizen has a Social Security number (SSN), a piece of information associated with an individual that is, generally speaking, permanent and unique to that individual. Originally created in 1935 to report employees' earnings for purposes of the new Social Security program, the SSN's use has greatly expanded over the ensuing years. This is due, in large part, to the SSN's value as a unique, permanent, and widely-adopted piece of information associated with an individual. Both public and private sector organizations have adopted the SSN for operational purposes as an identifier for customers, employees, and others, *i.e.*, as a means of associating an individual with records or information about him. Organizations use this identifier both for the organization's own internal tracking and to facilitate the sharing of information about the individual with other organizations and business partners. For example, the SSN often is used to prevent possible fraudulent customer transactions by serving as the common link between the organization's records and a third-party database of individuals known to have committed fraud.

Many organizations also use the SSN in the process of authentication, *i.e.,* verifying that the individual is who he claims to be. Authentication can take place at different phases of the individual's relationship with the organization, including at initial enrollment and for subsequent transactions or access to accounts. Organizations may use the SSN (alone or in combination with other information) to verify identities directly, or indirectly to access verification information offered by third parties.

In many cases, these expanded uses of the SSN have been driven by federal or state legal requirements. Businesses, for example, must collect employees' SSNs for inclusion on tax forms required by the Internal Revenue Service (IRS). Other usages of the SSN derive from convenience or efficiency. Thus, credit grantors regularly use the SSN to identify an individual

---

[1] The information collected for this summary was obtained by staff of the Federal Trade Commission (FTC), with the participation and assistance of other agencies involved in the President's Identity Theft Task Force. This summary was authored solely by FTC staff, has not been approved or endorsed by any other agency, but is submitted pursuant to the President's Identity Theft Task Force Strategic Plan. *See* The President's Identity Theft Task Force, *Combating Identity Theft, A Strategic Plan* 23-27, 45 (Apr. 2007) (hereinafter "Task Force Report"), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf.

during the credit application process, both because other identifiers (such as name, address, or date of birth) may be common among other individuals and lead to mistaken identifications, and because the SSN helps enable grantors to obtain a credit report on the applicant from a consumer reporting agency. Moreover, some entities claim that consumers find the SSN a convenient identifier, because it can be easily recalled.

The expanded usage of SSNs in the consumer identification and authentication processes, however, has a significant downside – the increased risk that SSNs will be misappropriated by criminals to steal identities and obtain benefits in the victims' names. Indeed, the more widespread SSN usage by legitimate businesses has become, the more available and valuable SSNs are for identity thieves. Criminals can obtain SSNs from many different sources, including family members, lost or stolen wallets, mailbox theft, and data compromises at organizations that maintain sensitive consumer data. Once obtained, they can be used by the thief – often in combination with other information – to impersonate the victim in opening new accounts or accessing existing accounts.

Concerns about overuse of SSNs and their role in identity theft have increased in recent years. In a recent consumer survey, 66 percent of the respondents stated that companies should stop using SSNs to identify customers, and 64 percent perceived that they were more vulnerable to identity theft when a business had their SSN.[2] Recognizing these concerns, and in light of the increased awareness of identity theft, a number of states have enacted laws restricting the collection, use, display, and/or transfer of SSNs. Several bills have been introduced in Congress that would establish national standards for protecting SSNs. At the same time, many organizations have taken steps to discontinue or limit their collection or use of SSNs, for example, by removing them from identification cards and other public display or by switching to other identifiers.

The tension between the beneficial uses of SSNs and their value for identity thieves was recognized by the President's Identity Theft Task Force ("ID Theft Task Force" or "Task Force"). The Task Force, comprising seventeen federal agencies and co-chaired by the Attorney General and FTC Chairman Deborah Platt Majoras, was formed in May 2006 with the mission of developing a comprehensive national strategy to combat identity theft.[3] In April of this year, the Task Force submitted its Strategic Plan and recommendations to the President. One of these recommendations was to develop a comprehensive record of SSN use by the private sector and evaluate the necessity of those uses.[4] The Task Force concluded that a thorough examination

---

[2] Consumer Reports National Research Center, *Social Security Number Privacy Poll* 8 (Sept. 6, 2007), *available at* http://www.ftc.gov/os/comments/ssnprivatesector/531096-00295.pdf.

[3] Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 10, 2006).

[4] *See* Task Force Report, at 23-27, 45. The Task Force also recognized the vulnerability of SSNs in the public sector to identity theft, and made a number of recommendations to limit their unnecessary usage by federal departments and agencies. *See id.* at 23-27. This summary addresses only the role of SSNs in the private sector in

would help policymakers and the private sector find ways to limit the unnecessary use of SSNs, given their prominent role in identity theft. At the same time, the Task Force recognized that "SSNs are an integral part of our financial system,"[5] and that it was important to preserve the beneficial uses of SSNs to the extent possible. The Strategic Plan called for Task Force agencies to gather information from stakeholders and make recommendations to the President as to specific steps that should be taken to balance these competing considerations.[6]

In response to the ID Theft Task Force recommendation, and in consultation with other participating agencies, FTC staff invited interested parties to comment on the various issues surrounding private sector usage of SSNs.[7] Over 300 individuals and entities provided comments.[8] FTC staff also conducted informal interviews with representatives from over 40 organizations. The comments and interviews encompass a wide range of stakeholders, including consumers, financial institutions, health care providers, insurers, universities, academics, privacy advocates, private investigators, consumer reporting agencies, mortgage companies, telecommunications companies, utilities, and fraud prevention firms. This summary is intended to provide an overview of the information provided by the stakeholders who filed comments or with whom staff spoke, and to frame the key issues prior to a workshop to be hosted by the FTC on December 10 and 11, 2007. It contains no conclusions or recommendations. Rather, this summary, along with the workshop record, will serve as the foundation for the development of recommendations by the ID Theft Task Force to the President in early 2008.

The summary first discusses the history of SSN usage and how it has evolved and expanded over time. The second section of the summary describes how criminals acquire SSNs and how they use them to commit identity theft. The third section explains how organizations use SSNs internally to identify individuals and customers and to share data with other organizations, and discusses existing alternative identifiers. The fourth section addresses SSN use for authentication purposes, both at the outset of a relationship and in subsequent encounters or transactions, as well as alternative methods of authentication. The fifth section of the summary discusses existing statutes, regulations, and private sector efforts designed to protect SSNs, including data security and data breach notification laws.

---

causing or preventing identity theft.

5 *Id.* at 26.

6 *Id.* at 26-27.

7 *See* Press Release, Federal Trade Commission, FTC Seeks Comments on the Uses of Social Security Numbers in the Private Sector: Goal to Reduce ID Theft (July 30, 2007), *available at* http://www.ftc.gov/opa/2007/07/ssn.shtm.

8 These public comments are available at http://www.ftc.gov/os/comments/ssnprivatesector/index.shtm.

II. The History of Social Security Number Usage and the Role of Government Mandates

From its inception, the history of the SSN has been one of ever-increasing collection, sharing, and usage. The Social Security Act of 1935 created the SSN to track and accurately report the earnings of employees covered under the new Social Security program for benefit purposes.[9] According to the Social Security Administration (SSA), this is still the primary purpose for which the SSA assigns an SSN to an individual.[10]

Over time, use of the SSN in both the public and private sectors has expanded well beyond its original purpose. Most commonly, organizations of all kinds use the SSN as an identifier for matching individuals with information about them. As one commenter noted, SSN usage has expanded in ways that were never envisioned, including as a tool to collect and organize personal information for commercial and other purposes.[11] This has caused many observers to raise concerns about the SSN's overuse. As early as 1973, the Department of Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems concluded that the SSN was not suitable as a universal identifier.[12] It found that because the SSN could be obtained from sources other than SSA, and was not assigned in an entirely random fashion, the SSN did not qualify as a standard universal identifier.[13] Nevertheless, many organizations adopted the SSN as an identifier, because it was the only item of personally identifiable information that was universal (or virtually so), permanent,[14] and unique to an individual.[15] The use of the SSN in identifying and authenticating individuals has become even greater in the digital age, as transactions increasingly are conducted between persons who do not

---

[9] *First in a Series of Subcommittee Hearings on Social Security Number High-Risk Issues Before the Subcomm. on Social Security of the H. Comm. on Ways and Means,* 109th Cong. 1 (Nov. 1, 2005) (Statement of Frederick G. Streckewald, Assistant Deputy Comm'r for Program Policy Office of Disability and Income Security Programs).

[10] *Id.*

[11] Comment of ARMA International, at 4.

[12] Dep't of Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens,* Chapter VII (July 1973), *available at* http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

[13] *Id.*

[14] Although the SSN is viewed as "permanent," it can be changed in rare cases. The SSA indicates, "[u]nder certain circumstances, SSA may assign you a new SSN if, after making all efforts to resolve the problems caused by someone else's misuse of your SSN, you are still being disadvantaged by the misuse." Social Security Online, When Someone Else Uses Your Social Security Number, http://www.ssa.gov/oig/hotline/when.htm.

[15] *E.g.,* Comment of Reed Elsevier Inc., at 2; Comment of Securities Industry and Financial Markets Association, at 3. Individuals' names, addresses, and other demographic information can change over time and, in many cases, are duplicates of other individuals.

know each other or, as in telephone or internet-based commerce, are not face-to-face. Moreover, the SSN has become a means for organizations to track consumers as they have adapted their business and record-keeping systems to utilize automated data processing.[16]

Federal and state governments were the first organizations to expand usage of SSNs beyond their original purpose. In 1943, President Roosevelt signed Executive Order 9397, which required federal agencies to use the SSN when creating new identification systems for individuals.[17] In the years that followed, the IRS began using the SSN as the official taxpayer identification number,[18] the SSN became the identification number for Medicare participants,[19] and the Department of Defense adopted the SSN in lieu of the military service number for identifying personnel in the armed forces.[20] In addition, various federal and state laws have authorized or required use of the SSN in a variety of settings.[21] For example, the Tax Reform Act of 1976 gave authority to states to use the SSN in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law within their jurisdiction.[22]

As many commenters highlighted, government obligations or mandates often drive the initial collection by private sector entities of a customer's SSN.[23] For example, many commenters observed that a large number of private sector uses of the SSN stem from tax reporting requirements. The IRS uses the SSN as a taxpayer identification number for individual tax reporting to the United States government.[24] Accordingly, there are a myriad of IRS forms that require private sector entities – such as banks, broker-dealers, insurance companies, and

---

16 Task Force Report, at 23.

17 Social Security Online, Social Security Number Chronology, http://www.ssa.gov/history/ssn/ssnchron.html (citing 3 C.F.R. §§ 283-284 (1943-1948)). The Task Force recommended a partial rescission of this Executive Order if doing so would assist in the implementation of other Task Force recommendations. Task Force Report, at 25.

18 Social Security Online, Social Security Number Chronology, http://www.ssa.gov/history/ssn/ssnchron.html.

19 *See* Task Force Report, at 23.

20 Social Security Online, Social Security Number Chronology, http://www.ssa.gov/history/ssn/ssnchron.html.

21 *See* Appendix, Legal Requirements for Private Sector Entities to Collect Social Security Numbers.

22 Social Security Online, Social Security Number Chronology, http://www.ssa.gov/history/ssn/ssnchron.html (citing Pub. L. No. 94-455, 90 Stat. 1520 (1976)).

23 *E.g.*, Comment of American Bankers Association, at 3; Comment of National Association of Federal Credit Unions, at 2.

24 26 U.S.C. § 6109(d).

employers – to collect SSNs for income and tax-related purposes.[25] Although some private sector commenters stated that they would prefer to truncate or mask SSNs sent to the IRS and recipient taxpayers,[26] there may be penalties for businesses that fail to include full SSNs on tax forms.[27]

Many commenters from the financial services industry pointed to the requirements of the USA PATRIOT Act,[28] which was enacted to curb money laundering and terrorist activities, as another example of a mandated collection and use of SSNs in the private sector.[29] The Customer Identification Program (CIP) rule promulgated by the federal banking agencies and the National Credit Union Administration under the USA PATRIOT Act mandates that, for new account openings, financial institutions must collect certain customer information, including name, date of birth, address, and identification number.[30] The identification number for a "U.S. Person" is that person's tax identification number, *i.e.*, the SSN.[31] In addition, regulations adopted pursuant to § 314(a) of the USA PATRIOT Act require financial institutions to report information, including the SSN, to law enforcement and regulatory authorities when individuals, entities, or organizations are engaged in, or are reasonably suspected to be engaged in, terrorist or money laundering activities.[32] This information is compared to data retained by the Treasury Department's Financial Crimes Enforcement Network (FinCEN), which includes required Suspicious Activity Reports and Currency Transaction Reports from financial institutions regarding cash transactions over $10,000 and other suspicious transactions. Both of these reports must include the subject's SSN.[33]

---

[25] *E.g.*, IRS Form 1099; IRS Form 8300. *See generally* Appendix, Legal Requirements for Private Sector Entities to Collect Social Security Numbers.

[26] *E.g.*, Comment of American Bankers Association, at 7-8.

[27] *E.g.*, 26 U.S.C. § 6722 (mandates a penalty of $50 for each return in which the servicer fails to include all of the information required on Form 1098, which includes the payee's SSN).

[28] Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered titles of U.S.C.).

[29] *E.g.*, Comment of American Council of Life Insurers, at 2; Comment of The Financial Services Roundtable, at 6; Comment of Independent Community Bankers of America, at 2; Comment of Wells Fargo & Company, at 5.

[30] 31 C.F.R. §§ 103.121(b)(2)(i)(A), 103.122(b)(2)(i)(A), 103.123(b)(2)(i)(A) & 103.131(b)(2)(i)(A). *See also* discussion at pp. 28-29, *infra*. Credit card issuers are given special treatment under the CIP rule, relaxing the requirement of acquiring personal information directly from customers and permitting them to obtain such information from a third party, such as a consumer reporting agency. 31 C.F.R. § 103.121(b)(2)(i)(C).

[31] 31 C.F.R. §§ 103.121(b)(2)(i)(A), 103.122(b)(2)(i)(A), 103.123(b)(2)(i)(A) & 103.131(b)(2)(i)(A).

[32] 31 C.F.R. § 103.100.

[33] FinCEN Forms 101, 102, 103, 104, 109 & TD F 90-22.47.

Other federal mandates require SSN collection and use by private sector businesses beyond the financial services industry. For instance, because the Medicare identification number is the SSN, doctors and hospitals must collect SSNs for their Medicare patients in order to obtain reimbursement.[34] Participants in federal student loan programs are required to provide SSNs, thereby compelling colleges and universities to collect them as well.[35]

Furthermore, there are some instances for which use of the SSN, although not explicitly mandated by law, assists businesses in complying with federal mandates. For example, the Treasury Department's Office of Foreign Assets Control (OFAC) requires private sector entities to ascertain whether a person or entity is on the "specially designated nationals" (*i.e.*, terrorists) list before making payments to or doing business with that individual.[36] When an individual's name appears on the OFAC list, the company is required to withhold any payment to that individual and report the match to OFAC. Companies use the SSN to verify that the individual in question is, in fact, the same person as the one who appears on the list. Many commenters stated that restricting the use of SSNs for this purpose would undermine the ability of financial institutions to avoid false positive matches and would result in a disruption of payments to certain payees.[37]

In addition to the federal SSN requirements, there are a number of state statutes that allow or mandate collection and use of SSNs by entities in the private sector. For example, many state "deadbeat" parent laws, which are designed to improve the collection of overdue child support payments, require financial institutions, insurers, and other entities to cross-check individuals through their SSNs with state-maintained deadbeat parent lists before making any financial or benefits payments to those individuals.[38] In addition, many states collect SSNs in applications for certain licenses, such as insurance licenses,[39] and many require SSNs for workers' compensation forms completed by employers and insurance companies.[40]

---

34 *See* Task Force Report, at 23.

35 20 U.S.C. § 1091(a)(4)(B), 20 U.S.C. § 1092.

36 *See* United States Department of the Treasury, Office of Foreign Assets Control, Frequently Asked Questions and Answers, http://www.ustreas.gov/offices/enforcement/ofac/faq/answer.shtml#22.

37 Comment of American Insurance Association, at 2; *see also* Comment of American Council of Life Insurers, at 2; Comment of First Data Corporation, at 1-2.

38 *E.g.*, R.I. Gen. Laws § 27-57-1; Mass. Gen. Laws ch. 175, § 24D & ch. 119A, § 6.

39 Pursuant to 42 U.S.C. § 666(a)(13), states must collect SSNs for certain licensing purposes in order to improve the effectiveness of the state's child support enforcement. *E.g.*, Fl. Stat. § 626.171; 28 Tex. Admin. Code § 19.1903.

40 *E.g.*, Virginia Workers Compensation Form 45-A, Report of Minor Injuries. For additional information regarding state and federal laws mandating the use and collection of SSNs, see Appendix, Legal Requirements for Private Sector Entities to Collect Social Security Numbers.

At least in part as an outgrowth of these government mandates, many businesses began to collect and use the SSN for a range of other, unrelated functions, including as an internal identifier, a customer number, a way to link information, or a means for customers to access accounts online or via telephone. For example, consumer reporting agencies (CRAs) use SSNs to help ensure that the data furnished to them about consumers is placed in the correct consumer's file.[41] Businesses and organizations such as banks, insurance companies, mortgage companies, debt collection agencies, child support enforcement agencies, credit grantors, and employment screening companies use SSNs to obtain consumer reports to identify individuals and make eligibility and pricing decisions for a variety of products and services.[42] In addition, businesses may use SSNs to match consumer information with other organizations for a variety of purposes, including fraud prevention.

In light of the broad usage of SSNs, there is widespread concern about the inherent security and identity theft risks that come with the collection, maintenance, and sharing of this sensitive information. One commenter, for example, complained that "[s]o many businesses use the 'last four digits of your SSN' as a verbal 'password' so as to make it completely meaningless."[43] The commenter expressed concern that every employee at one local utility with whom the commenter has spoken knows the same information that is used to secure his investments and some of his medical information. SSNs that are stored and transferred between entities can become available to criminals who may intercept them in transit or steal them from stored databases. SSNs that are publicly displayed are especially vulnerable to acquisition by identity thieves. As a result of these concerns, in comments and discussions with FTC staff, many businesses stated that they have begun curtailing their collection and use of SSNs, particularly in public-facing applications or transactions.[44] Federal and state regulations protecting SSNs and limiting their public display, as well as state data breach laws, also have caused private sector entities to reduce their reliance on SSNs. At the same time, both government and the private sector have increased their outreach to consumers on the importance of not using (such as for a password) or disclosing their SSNs unnecessarily. Nevertheless, businesses continue to use, and consumers to disclose, SSNs in a variety of ways.

III. SSNs and Identity Theft

SSNs generally are considered to be the most valuable piece of consumer data for identity thieves. This section will discuss how thieves are able to obtain SSNs, and how they use SSNs

---

41 Gov't Accountability Office, GAO-07-1023T, *Social Security Numbers: Use Is Widespread and Protection Could Be Improved* 9 (June 21, 2007).

42 *See, e.g.*, Comment of Boeing Employees' Credit Union, at 1-2; Comment of Credit Union National Association, at 2; Comment of HSBC Finance Corporation, at 3.

43 *See* Comment of Ethan Sommer.

44 *See, e.g.*, Comment of Boeing Employees' Credit Union, at 2.

to commit identity theft.

A. How Thieves Obtain SSNs

Criminals can obtain SSNs anywhere they are located or stored, and either use the SSNs themselves or sell them to others.[45] As described in the ID Theft Task Force's Strategic Plan, there are numerous means by which identity thieves obtain SSNs and other sensitive consumer information, ranging from the low-tech (*e.g.*, stealing workplace records, bribing insiders, pretexting, stealing mail, and "dumpster diving") to the high-tech (*e.g.*, phishing, hacking, spyware, and other electronic intrusions).[46]

There are no definitive data on the prevalence of the different methods by which criminals obtain SSNs, and none were supplied by commenters. Indeed, it would be very difficult to determine prevalence in any reliable way, because victims frequently do not know how their information was compromised,[47] and successful thieves are unlikely to share this information. Previous attempts to collect statistics from criminal law enforcement cases have not yielded meaningful data and, in any event, such data reflect only the population of thieves that have been caught. Moreover, even if prevalence information were available, it likely would become quickly outdated as new techniques for obtaining SSNs evolve. Below, we describe some of the most commonly reported sources that thieves use to misappropriate SSNs.

Publicly Available Sources

Public and private sector entities make SSNs publicly available in several ways. Individuals' SSNs may be included in public records available from city and county governments, such as death certificates, property records, tax lien records, and court records. As of 2004, 41 states and the District of Columbia, as well as an estimated 75 percent of U.S. counties, displayed SSNs in public records, although many government offices have taken steps

---

45 Tom Zeller, Jr., *Black Market in Stolen Credit Card Data Thrives on Internet*, N.Y. Times, June 21, 2005, *available at* http://www.nytimes.com/2005/06/21/technology/21data.html.

46 Task Force Report, at 13-17.

47 The FTC released an Identity Theft Survey on November 27, 2007, which indicates that 56% of identity theft victims surveyed did not know how their personal information was obtained. Federal Trade Commission, *2006 Identity Theft Survey Report* 30 (November 2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf. Similarly, the 2007 Identity Fraud Survey Report by Javelin Strategy and Research found that 58% of identity theft victims did not know how their personal information was obtained. Javelin Strategy and Research, *2007 Identity Fraud Survey Report: Identity Fraud Is Dropping, Continued Vigilance Necessary* 30 (Feb. 2007).

since then to truncate, mask, or eliminate the display of SSNs.[48]

Until relatively recently, the fact that public records were in paper form effectively limited their utility for identity thieves. Some observers have referred to the "practical obscurity" of paper records, because the effort involved in physically going to the government office and extracting information from individual records is likely to deter most prospective identity thieves.[49] Public records, however, increasingly are being posted online, making them available to anyone with internet access – including identity thieves – with little effort. For example, in one reported case, an identity thief was able to obtain new credit cards using the information posted on a court clerk website regarding the victim's speeding ticket, including his SSN, address, height, weight, date of birth, and signature.[50] Recognizing the risks presented by the electronic availability in public records of sensitive consumer information, the ID Theft Task Force recommended that it work with state and local governments to encourage the trend towards eliminating unnecessary use and display of SSNs.[51]

In addition to public records sources, some individuals, unaware of the risks, may make their own SSNs more available to others than is necessary. For instance, some individuals print their SSNs on their personal checks,[52] and some job hunters include their SSNs on resumes, which they may post on a public website.[53]

---

[48] Gov't Accountability Office, GAO-05-59, *Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards* 3 (Nov. 2004). On government actions to limit display of SSNs, *see, e.g.,* Joel Stonington, *Courts Tighten Access to Records,* Aspen Times, Aug. 28, 2007, *available at* http://www.aspentimes.com/article/20070828/NEWS/70827053/0/FRONTPAGE.

[49] *E.g.*, Privacy Rights Clearinghouse, *Public Records on the Internet: The Privacy Dilemma,* Apr. 19, 2002 & updated Mar. 2006, http://www.privacyrights.org/ar/onlinepubrecs.htm; Electronic Privacy Information Center, Privacy and Public Records, Oct. 23, 2007, http://www.epic.org/privacy/publicrecords/.

[50] Jennifer 8. Lee, *Dirty Laundry, Online for All to See,* N.Y. Times, Sept. 5, 2002, *available at* http://tech2.nytimes.com/mem/technology/techreview.html?res=9A04E4D9173EF936A3575AC0A9649C8B63.

[51] Task Force Report, at 26. It is important to note, however, that there may be important public policy reasons (as well as legal requirements) for making public record information accessible. For example, one commenter noted that limiting the use of SSNs in public records has a negative effect on important activities such as fraud prevention, background screening, and debt collection. Comment of Coalition for Sensible Public Records Access, at 2.

[52] Comment of Independent Community Bankers of America, at 5. The FTC educates consumers on ways to protect SSNs, including advising consumers not to write their SSNs on checks. *See, e.g.,* Federal Trade Commission, Fighting Back Against Identity Theft, May 2006, http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.shtm.

[53] *See* Martin H. Bosworth, *'Angel' Warns Job Seekers of Identity Theft Risk*, ConsumerAffairs.com, Aug. 10, 2006, http://www.consumeraffairs.com/news04/2006/08/job_seekers_id_theft.html.

Data Brokers

Data brokers are companies that aggregate and sell consumer information to third parties for a variety of purposes, such as building consumer credit reports, verifying identities, locating individuals, marketing, preventing fraud, or obtaining asset information for civil proceedings. Data brokers collect the personal information they sell from numerous sources, including public records. Although the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA) impose privacy and security-related obligations on data brokers under certain circumstances, there are gaps in these laws, as discussed more fully in Section VI.

Even when they are required to do so, some data brokers may fail to take appropriate steps to ensure that the entities to which they sell consumer information are not identity thieves. In a recent Florida case, identity thieves allegedly opened accounts with data brokers by fraudulently using the identity of a legitimate business. The thieves then used those accounts to obtain hundreds of credit reports with SSNs, which they used to commit identity theft.[54] In discussions with FTC staff, data brokers and their customers noted that many data brokers recently have implemented additional measures to ensure that their customers are legitimate and have a legitimate need for the data. These additional safeguards followed the FTC's 2006 settlement with ChoicePoint Inc., a large data broker that, the Commission alleged, provided sensitive personal information (including SSNs in some cases) for thousands of individuals to identity thieves who had impersonated a ChoicePoint customer.[55]

Additionally, there have been reports of unscrupulous data sellers that advertise SSNs for purchase online, sometimes for $50 or less.[56] It is not clear how widespread this practice is. Many of these entities may not actually sell SSNs to the general public, despite their claims to do so, or may require a demonstrable and legitimate need before selling them. The Government Accountability Office (GAO) found that, although a number of internet sources advertised the sale of SSNs, the reality was that it was difficult to actually purchase full SSNs from the majority

---

[54] *See* Press Release, U.S. Attorney's Office, Southern District of Florida, Four Charged in Credit Card and Identity Theft Ring (July 3, 2007), *available at* http://www.usdoj.gov/usao/fls/PressReleases/070703-01.html; Indictment at 3, *United States v. Barrios-Delgado, et. al*, No. 0:07cr60171 (S.D. Fla. June 28, 2007).

[55] The FTC alleged that ChoicePoint failed to implement reasonable verification procedures, thus allowing identity thieves who lied about their credentials to become customers and obtain consumer data, including SSNs. *See* Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief, *United States v. ChoicePoint Inc.*, No. 1:06cv0198 (N.D. Ga. filed Jan. 30, 2006); Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief, *United States v. ChoicePoint, Inc.*, No. 1:06cv0198 (N.D. Ga. settlement entered Feb. 15, 2006).

[56] *E.g.*, Newsmax.com, *Social Security Numbers Are for Sale Online*, Apr. 5, 2005, http://archive.newsmax.com/archives/articles/2005/4/4/155759.shtml; Comment of New York State Consumer Protection Board, at 2; Comment of Consumers Union, at 3-4.

of those sources.[57] The GAO attempted to purchase SSNs from 21 web sites that purported to sell them, but was able to purchase only one full SSN and four truncated SSNs.[58]

Theft From or Loss of Data by Consumers

Thieves (who may include family members or co-workers) may steal personal information, including SSNs, from consumers through such low-tech methods as purse or wallet theft, mail theft, or dumpster diving (taking documents thrown into unprotected trash receptacles).[59] Some institutions display a full or partial SSN on account statements, paychecks, applications, or other documents that are sent through the mail and may be thrown in the trash without being shredded. Further, some consumers carry in their wallets or purses government, insurance, or student identification cards that display the SSN.[60]

The display of full SSNs on identification cards and mailed documents is declining, as discussed in Section IV below. Indeed, several state laws now prohibit the disclosure of SSNs on identification cards and certain mailed materials.[61] That said, a 2007 survey conducted by one commenter found that over half of the consumers surveyed still carried on their person identification cards that displayed their SSNs.[62]

Theft from or Loss of Data by Businesses

Identity thieves may gain access to an organization's records, whether paper or in an electronic database, and obtain employee and/or customer records that contain SSNs. Access

---

57 Gov't Accountability Office, GAO-06-495, *Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs* 12-14 (May 2006).

58 *Id.*

59 Task Force Report, at 14.

60 Several types of government-issued cards display full SSNs, including Medicare cards, Department of Defense insurance cards, and Veterans Identification Cards that were issued prior to March 2004. In 2004, an estimated 42 million Medicare cards displayed full SSNs, as did approximately 8 million Department of Defense insurance cards. Task Force Report, at 23-24. Although the Veterans Health Administration (VHA) discontinued the issuance of Veterans Identification Cards that display SSNs in March 2004, and has issued new cards that do not display SSNs, the VHA estimates that between 3 million and 4 million previously-issued cards containing SSNs remain in circulation with veterans receiving VHA services. *Id.*

61 *E.g,* Cal. Civ. Code § 1798.85; Ariz. Rev. Stat. § 44-1373.

62 Consumer Reports National Research Center, *Social Security Number Privacy Poll* 24 (Sept. 6, 2007), *available at* http://www.ftc.gov/os/comments/ssnprivatesector/531096-00295.pdf.

may be gained by hacking,[63] physical theft, impersonation, insider fraud, dumpster diving, or other means. For example, in a Washington State case, identity thieves used false identification documents to impersonate employees of a medical clinic, allowing them to obtain personal information, including SSNs, from patient and other records. The thieves then used that information to gain access to victims' bank accounts.[64] In a case involving an alleged corrupt insider, a mortgage company employee allegedly obtained documents containing personal customer information. The information, which included SSNs, allegedly was used, among other things, to access existing bank accounts and to apply for credit.[65]

Sensitive data, including SSNs, can come into the possession of identity thieves when laptops, media storage devices, back-up tapes, and other portable data devices are lost or stolen, or systems are hacked. There have been numerous recent reports of companies, universities, government agencies, and hospitals losing or suffering a theft of devices that stored SSNs.[66] In many cases, the theft or loss may not result in identity theft, but there have been reports of associated identity theft linked to certain data compromises.[67]

Social Engineering: Phishing, Malware/Spyware/Loggers, and Pretexting

Identity thieves also may use various forms of trickery to obtain SSNs, whether by "phishing" or using malware, spyware, or keystroke loggers.[68] In one phishing scheme, an

---

[63] *E.g.*, Lisa Vaas, *Hack at UC Berkeley Potentially Nets 1.4 Million SSNs*, eWeek.com, Oct. 20, 2004, http://www.eweek.com/article2/0,1895,1680799,00.asp; Press Release, U.S. Attorney's Office, Western District of Texas, Former Student Sentenced for Hacking into U.T. Computer System (Sept. 6, 2005), *available at* http://www.usdoj.gov/usao/txw/press_releases/2005/ut_hacker.sen.pdf.

[64] Press Release, U.S. Attorney's Office, Western District of Washington, Forger Linked to Multiple Identity Thieves Sentenced to 5+ Years in Prison (June 8, 2007), *available at* http://seattle.fbi.gov/dojpressrel/2007/pr060807.htm.

[65] Press Release, U.S. Attorney's Office, Western District of Washington, Grand Jury Indicts ID Theft Ring That Used Insiders at a Mortgage Company and Escrow Firm to Steal Personal Information (Feb. 7, 2007), *available at* http://www.usdoj.gov/usao/waw/press/2007/feb/griffin.html.

[66] *E.g.*, Shamus Toomey, *5,800 students at risk of ID theft, Loyola warns*, Chicago Sun-Times, Aug. 10, 2007, *available at* http://findarticles.com/p/articles/mi_qn4155/is_20070810/ai_n19477869.

[67] Gov't Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, Full Extent Is Unknown* 21-28 (June 2007).

[68] "Phishing" occurs when a thief sends an email that appears to come from a legitimate source (such as a financial institution) to a consumer and asks the recipient to verify his personal information at a seemingly legitimate website linked to the email. Both spyware and keystroke loggers are types of malware – software designed to infiltrate or damage a computer system without the owner's consent. Spyware enables criminals to gain access to a user's computer without permission; keystroke loggers gather and send information on the user's internet sessions back to the hacker. The FTC provides education to consumers about protecting their personal information from these types of attacks, and it sponsors a multimedia website, OnGuard Online, www.onguardonline.gov/index.html,

identity thief was allegedly able to obtain financial and personal information of individuals, including SSNs, by sending emails to victims directing them to fraudulent web sites that looked identical to legitimate web sites maintained by banks and other businesses.[69] Even when they are not transmitted online, SSNs are vulnerable to social engineering schemes in the form of pretexting.[70]

B. Why SSNs Are Valuable to Identity Thieves

Simply put, identity thieves obtain SSNs to facilitate the opening of new accounts, gain access to existing accounts, use in medical identity theft, seek employment, or obtain government benefits. Financial institutions generally require SSNs to open new accounts, either by law or because SSNs help them access the consumer's credit report to establish the creditworthiness of the applicant. In addition, SSNs may control access to existing accounts by serving as internal identifiers to match consumers with their records, and for consumer authentication purposes.

Commenters and others with whom FTC staff spoke disagreed about the value of an SSN by itself in the commission of identity theft. Industry commenters addressing this subject generally stated that thieves need additional information beyond a consumer's name and SSN to misuse existing accounts or open new ones.[71] One commenter asserted that although the SSN "does not necessarily provide an identity thief the 'keys to the kingdom' . . . . if an identity thief has the victim's SSN, the thief is more likely to succeed in his or her efforts."[72] Other industry commenters posited that an identity thief who has an SSN can "reverse engineer" a consumer's name and address, often by using various online resources.[73] Thieves also may manufacture or purchase counterfeit identification cards, such as driver's licenses, to use in conjunction with a

---

that educates consumers about basic computer security.

[69] Press Release, U.S. Attorney's Office, Eastern District of California, Sacramento Man Charged with Computer Fraud and Aggravated Identity Theft (Apr. 26, 2007), *available at* www.usdoj.gov/usao/cae/press_releases/docs/2007/04-26-07NguyenInd.pdf.

[70] Pretexting occurs when someone contacts a financial institution or telephone company, impersonating a legitimate customer, and requests that customer's account information.

[71] *E.g.*, Comment of Boeing Employees' Credit Union, at 4; Comment of Consumer Data Industry Association, at 21; Comment of The Financial Services Roundtable, at 13; Comment of Independent Community Bankers of America, at 6; Comment of National Business Coalition on E-Commerce and Privacy, at 18; Comment of National Retail Federation, at 3; Comment of Wells Fargo & Company, at 13.

[72] Comment of Coalition to Implement the FACT Act, at 3.

[73] *E.g.*, Comment of Boeing Employees' Credit Union, at 4; Comment of Consumer Data Industry Association, at 21; Comment of The Financial Services Roundtable, at 13.

stolen SSN.[74] Some commenters also claimed that, because identity thieves can obtain the additional information they need from multiple sources, identity theft can occur even when businesses granting credit or opening accounts match multiple pieces of consumer information in addition to the SSN.[75]

Other commenters provided a different view on the ease with which identity thieves can use SSNs to commit their crimes. Some commenters stated that credit issuers in some cases may grant credit based simply on a victim's SSN and a date of birth that is consistent with the SSN's time of issuance, and that others grant credit based on applications full of inconsistencies, including mismatched names and SSNs.[76]

New Account Fraud

Thieves often acquire SSNs because, in most cases, the SSN is one of the key pieces of information required to open financial accounts and obtain other types of services or benefits. Most creditors and many other providers of certain products and services obtain a credit report on an applicant before approving him or her, and use the applicant's SSN to help ensure that they locate the right file. In some cases, the provider will ascertain whether the applicant appears on a "fraud" database (such as lists of writers of bad checks), using the applicant's SSN to ensure the right match. In short, many report that the SSN is a necessary, if not always sufficient, item of information for identity thieves.

There are innumerable examples of identity thieves using victims' SSNs and certain other identifying information to open new accounts in the victims' names.[77] For instance, in one case prosecuted in the State of Washington, thieves allegedly obtained credit using the name, date of birth, SSN, and a counterfeit driver's license for an actual individual and then made purchases at

---

[74] *See* Press Release, U.S. Attorney's Office, Western District of Washington, Grand Jury Indicts ID Theft Ring That Used Insiders at a Mortgage Company and Escrow Firm to Steal Personal Information (Feb. 7, 2007), *available at* http://www.usdoj.gov/usao/waw/press/2007/feb/griffin.html.

[75] *E.g.*, Comment of Coalition for Sensible Public Records Access, at 2; Comment of New York State Consumer Protection Board, at 1-2 (noting widespread availability of personal identifying information).

[76] *E.g.*, Comment of Samuelson Law, Technology & Public Policy Clinic, at 3; Comment of Electronic Privacy Information Center, at 4.

[77] According to the FTC's most recent identity theft survey, 21.9% of identity theft victims had their personal information used to open new accounts or commit some other type of fraud not involving an existing account. Federal Trade Commission, *2006 Identity Theft Survey Report* 13 (November 2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf. Because SSNs are generally required to open new financial and other accounts, it is likely that SSNs were involved in the vast majority of these instances of new account identity theft.

various retail stores.[78] In a Nebraska case, identity thieves allegedly were able to open fraudulent brokerage accounts using the actual SSN, date of birth, address, bank name, bank routing number, and bank account number of a victim.[79] The thieves then allegedly used these fraudulently-opened accounts to purchase thinly-traded stocks that were owned by the thieves in their own accounts, in order to artificially inflate the stocks' prices.[80]

Some new account fraud involves theft of the SSNs of individuals who have existing files at the consumer reporting agencies. In these cases, the SSN is used, among other things, to give the creditor access to the victim's credit file, which generally is a necessary part of the account-opening process. There are two other distinct forms of new account fraud that rely on SSNs. First, identity thieves may steal and utilize the SSNs of individuals, such as children, who do not have an existing credit file.[81] In these situations, when the provider attempts to access the applicant's credit file, the CRA will report that no credit file was found. At that point, the creditor may open the account anyway, albeit usually on more restrictive terms (*e.g.*, a lower credit limit) than would apply to individuals who have files.[82]

Second, thieves may couple a valid SSN with a different name and other identifying information, in what is commonly known as "synthetic identity theft."[83] Here, the thief creates a new identity, rather than using a victim's existing identity, to open new accounts. Again, a creditor attempting to access the credit file of the "synthetic" individual will receive a response from the CRAs that no match was found, but may open the account anyway.[84] In some cases,

---

[78] Indictment at 8-9, *United States v. Griffin et al.*, No. 2:07cr00027 (W.D. Wash. Jan. 31, 2007). *See also* Press Release, U.S. Attorney's Office, Western District of Washington, Grand Jury Indicts ID Theft Ring That Used Insiders at a Mortgage Company and Escrow Firm to Steal Personal Information (Feb. 7, 2007), *available at* http://www.usdoj.gov/usao/waw/press/2007/feb/griffin.html.

[79] Criminal Complaint at 18, *United States v. Marimuthu et al*, No. 8:06MJ169 (D. Neb. Dec. 21, 2006); *see also* Press Release, U.S. Department of Justice, *Hackers from India Indicted for Online Brokerage Intrusion Scheme that Victimized Customers and Brokerage Firms* (Mar. 12, 2007), *available at* http://www.usdoj.gov/opa/pr/2007/March/07_crm_141.html; Press Release, U.S. Securities and Exchange Commission, *SEC Sues Three Offshore Hackers With Scheme to Intrude Into Online Accounts, Manipulate Market* (Mar. 12, 2007), *available at* http://www.sec.gov/litigation/litreleases/2007/lr20037.htm.

[80] *Id.*

[81] *See, e.g.*, Identity Theft Resource Center, Fact Sheet 120 – Identity Theft and Children, Apr. 27, 2007, http://www.idtheftcenter.org/artman2/publish/v_fact_sheets/Fact_Sheet_120.shtml; Comment of Consumer Data Industry Association, at 13.

[82] *Id.* (discussing creation of credit file by credit bureaus in situations involving identity theft and children).

[83] *E.g.*, Comment of Samuelson Law, Technology & Public Policy Clinic, at 4.

[84] When the creditor requests the credit report on the fabricated identity, the CRA may report that no credit file is found because not enough identifying information matches a credit file on record. If the thief nonetheless is allowed to open the account, that account will then be used to start a credit file. Sophisticated thieves may actually

identity brokers sell these newly-created identities to individuals who cannot otherwise obtain SSNs, for purposes such as obtaining financing or employment.[85] Because CRAs may create a new credit file for the "synthetic" individual – rather than assign the information to an existing file – the impact typically is not experienced by actual consumers, but rather by the creditors.[86] For the same reason, this type of identity theft is difficult for individuals to detect.[87]

Existing Account Fraud

SSNs also can help thieves gain access to existing accounts of victims. This is the case because some institutions use SSNs as part of the process of authenticating customers when they are attempting to access their accounts.[88] For example, financial institutions may ask a customer for his or her full or partial SSN to access an account over the phone. Commenters noted that identity thieves have used SSNs to make purchases, obtain cash advances, and procure replacement cards on existing credit accounts.[89] Section V discusses existing account authentication issues in more detail.

Medical Identity Theft

SSNs also can be a key tool to commit medical identity theft, a crime in which the victim's identifying information is used to obtain or make false claims for medical care. In a

---

pay bills for some time on newly opened accounts to build a positive credit history for the new identity, which can be used to open accounts with progressively higher credit limits. *See* Comment of Samuelson Law, Technology & Public Policy Clinic, at 4-5.

[85] *E.g.*, Comment of Consumer Data Industry Association, at 21.

[86] Nevertheless, the consumer whose SSN was used may be harmed if a debt collector later tries to locate the delinquent debtor by using an SSN search, or if the new credit file later becomes associated with that consumer's credit file. *See, e.g.*, Leslie McFadden, *Detecting Synthetic Identity Fraud*, Bankrate.com, May 16, 2007, http://www.bankrate.com/brm/news/pf/identity_theft_20070516_a1.asp; *see also* Federal Trade Commission, *Report to Congress Under Sections 318 and 319 of the Fair and Accurate Credit Transactions Act of 2003* 57-58 (Dec. 2004) (hereinafter "FTC Report to Congress Under FACTA Sections 318 and 319"), *available at* www.ftc.gov/reports/facta/041209factarpt.pdf (explaining how a creditor may receive a different consumer report than a consumer – including additional secondary reports – because the amount of identifying information supplied by a creditor to obtain a report may be less than that provided by the consumer).

[87] *See, e.g.*, Leslie McFadden, *Detecting Synthetic Identity Fraud*, Bankrate.com, May 16, 2007, http://www.bankrate.com/brm/news/pf/identity_theft_20070516_a1.asp.

[88] *E.g.*, Comment of HSBC Finance Corporation, at 4; Comment of American Bankers Association, at 5.

[89] *E.g.*, Comment of Mortgage Bankers Association, at 8; Comment of Independent Community Bankers of America, at 6; Comment of Wells Fargo & Company, at 13; *see also* FCRA, 15 U.S.C. § 1681m (requiring the Federal banking agencies, the National Credit Union Administration, and the FTC to jointly issue "Red Flag Guidelines" that include, among other things, a provision detailing when a credit card issuer may issue a replacement credit card when a change of address has been received in the thirty days preceding the request). 16 C.F.R. Part 681.

Colorado case, for example, a man whose SSN, name, and address had been stolen discovered that he was a victim of medical identity theft when a debt collector demanded money owed to a hospital for a surgery he did not have.[90] The harms associated with medical identity theft often go beyond financial losses. Medical identity theft can introduce inaccurate information into the victim's medical history records, which can lead to improper treatment.[91]

Employment and Other Benefits

Individuals who are not legally eligible for employment may obtain and use the SSNs of others to try to obtain employment.[92] In one well-known and recent investigation, undocumented workers allegedly used the SSNs and other identity documents of U.S. citizens to gain employment at facilities owned by a national meat processing company.[93]

Because SSNs also are used frequently to control and track government benefits and programs, identity thieves may use stolen SSNs to obtain these benefits. For instance, in one Florida case, a thief allegedly was able to obtain, through health center employees, patients' names, dates of birth, SSNs, Medicare numbers, and addresses, among other information, and to use that information to make fraudulent claims for Medicare reimbursement.[94] The Department of Justice brought numerous fraud cases following Hurricane Katrina involving misuse of others' SSNs. For example, in one case, a woman allegedly was able to use other individuals' SSNs to file multiple fraudulent claims to the Federal Emergency Management Agency for disaster relief.[95] Other thieves allegedly have used stolen SSNs to file fraudulent tax returns that claim a refund.[96]

---

[90] World Privacy Forum, *Medical Identity Theft: The Information Crime That Can Kill You,* at 5 (May 3, 2006) *available at* www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf.

[91] *Id.*

[92] *See* John Leland, *Some ID Theft Is Not For Profit, But to Get a Job,* N.Y. Times, Sept. 4, 2006, *available at* http://www.nytimes.com/2006/09/04/us/04theft.html.

[93] Press Release, Immigration and Customs Enforcement, U.S. Uncovers Large-Scale Identity Theft Scheme Used By Illegal Aliens to Gain Employment at Nationwide Meat Processor (Dec. 13, 2006), *available at* http://www.ice.gov/pi/news/newsreleases/articles/061213dc.htm.

[94] Press Release, U.S. Attorney's Office, Southern District of Florida, Two Defendants Sentenced in Heath Care Fraud, HIPAA, and Identity Theft Conspiracy (May 3, 2007), *available at* http://www.usdoj.gov/usao/fls/PressReleases/070503-01.html.

[95] Press Release, U.S. Department of Justice, Fact Sheet: The Department of Justice's Efforts to Combat Identity Theft (Apr. 23, 2007), *available at* http://www.usdoj.gov/opa/pr/2007/April/07_opa_278.html.

[96] *E.g.,* Task Force Report, at 21; Comment of Electronic Privacy Information Center, at 4-5.

IV. The SSN as an Identifier

The SSN is widely used as an identifier – *i.e.*, to match an individual to information about him – throughout the public and private sectors. Private sector entities may use SSNs to identify individuals for numerous purposes, for example, as a customer number, to link internal records, or to obtain or provide information about an individual from external sources, such as a CRA.

Many commenters stated that the SSN is valuable as an identifier in part because it can be used both to distinguish among individuals and to track an individual over time. This is largely because of the SSN's permanence, uniqueness, and virtual universality. The vast majority of U.S. citizens have their own SSN, which does not change during the individual's lifetime. According to several observers, the use of the SSN to distinguish individuals, though imperfect, helps prevent mixed or duplicative records.[97] Other possible identifiers – such as name, address, and date of birth – are not unique. A parent and child, for example, may share the same name and address. Moreover, names and addresses often are subject to variations (*e.g.*, the same individual may provide his name as *John Smith, John Michael Smith, J. Smith, John M. Smith,* or *J.M. Smith*) and can change over time, making them less useful for tracking and linking individuals' records. For these reasons, many business commenters viewed the SSN as the most cost-effective, accurate, and efficient piece of information available to identify consumers and link information to them.[98] Although some observers have suggested that the same matching function can be performed by using multiple data points, *e.g.*, name and date of birth,[99] others have claimed that these other identifiers are inherently less reliable.[100]

A. The SSN as Identification Number and Internal Identifier

Many organizations still use SSNs as employee or customer identification numbers to track those individuals and link their records within the organization. In some cases, organizations may use the SSNs for these purposes – rather than some other number or data point – because they historically have done so, or for reasons of convenience or ease of use. A large number of colleges and universities, for example, have used SSNs as student identification numbers for many years. A 2006 survey of higher education institutions found that

---

97 *E.g., Protecting the Privacy of the Social Security Number from Identity Theft: Hearing Before the Subcomm. on Social Security of the H. Comm. on Ways & Means,* 110th Cong. 3 (2007) (statement of Ana I. Anton, Ph.D).

98 *E.g.,* Comment of American Bankers Association, at 5.

99 *E.g., Protecting the Privacy of the Social Security Number from Identity Theft: Hearing Before the Subcomm. on Social Security of the H. Comm. on Ways & Means,* 110th Cong. 3 (2007) (statement of Ana I. Anton, Ph.D).

100 *E.g.,* Comment of Consumer Data Industry Association, at 9.

approximately one third of the schools surveyed were using SSNs as identifiers.[101] With respect to the health care sector, some observers have reported that insurance companies have used SSNs as subscriber numbers – in part, because health insurance often is an employee benefit and many companies use SSNs as identification numbers for their employee transactions.[102] In some cases, organizations that use the SSN as an employee or customer identification number display the number on the badges or identification cards carried by the individual.

According to commenters and other sources contacted by FTC staff, even when organizations do not use the SSN as the employee or customer identification number *per se*, they may use SSNs to track and link different products and services provided to a customer, including across multiple lines of business.[103] Some entities use SSNs to recall customer information and to manage customer relations.[104] For example, some banks may use a customer's SSN to locate account information in response to a telephone request from a customer who cannot recall her account number. In addition, employers may use SSNs to identify employees in order to maintain accurate information about employment benefits or to track hours or training.[105]

Many organizations, however, have recognized the identity theft concerns raised by SSN usage and have switched to other, less sensitive numbers for identification purposes.[106] Even those organizations that continue to use SSNs as identification numbers in many cases no longer display the numbers on badges or cards.

B. Use of SSNs to Link and Share Data with External Entities

As discussed in Section II above, private sector entities are legally required to collect and communicate SSNs to other entities for certain purposes, such as reporting income to the IRS or checking databases of parents who may be in arrears for child support payments. In other

---

101 EDUCAUSE Center for Applied Research, *Identity Management in Higher Education: A Baseline Study* 63 (2006), *available at* http://www.educause.edu/ir/library/pdf/ers0602/rs/ers0602w.pdf?bcsi_scan_DA3493EE5FC9D524=0&bcsi_scan_filename=ers0602w.pdf.

102 Avrum D. Lank, *Danger in 9 digits: Most carry their Social Security number, if not their card*, Milwaukee Journal Sentinel, Apr. 17, 2004, *available at* http://www.pplusic.com/about/news.asp?newsarticle_id=3.

103 *E.g.*, Comment of American Bankers Association, at 3; Comment of American Financial Services Association, at 3; Comment of America's Community Bankers, at 2; Comment of National Business Coalition on E-Commerce and Privacy, at 15.

104 *E.g.*, Comment of Independence Bank of Kentucky, at 1.

105 *E.g.*, Comment of Securities Industry and Financial Markets Association, at 3; Comment of Society for Human Resource Management, at 2.

106 *E.g.*, Comment of American Petroleum Institute, at 3; Comment of First Data, at 4; Comment of Retail Industry Leaders Association, at 2.

instances, even though not strictly required, entities may need SSNs to communicate with government agencies regarding government programs. The U.S. Department of Education, for example, uses the SSN as the account number for student loans and provides it to schools to ensure that disbursements are credited properly.[107]

In addition, many businesses use SSNs to link or share data with other private sector entities in ways that are not legally required, such as to share data on consumer credit histories with CRAs. The consumer reporting industry uses SSNs extensively, and this use drives SSN usage in other sectors as well. According to some commenters, the SSN has evolved into a common identifier for the financial services and consumer reporting industries.[108]

The consumer reporting industry is characterized by the continuous flow of information about consumers among CRAs and businesses and other organizations, and that information is linked to individuals principally through their SSNs. CRAs most often obtain SSNs from creditors and other data furnishers, such as banks, insurance companies, and debt collection agencies. They also may obtain SSNs from public records sources and other information resellers.[109] Although errors sometimes occur, CRAs use SSNs both to direct the data furnished to them to the correct file and to link a consumer report to the correct consumer.[110]

The flow of SSNs also occurs in the other direction. Creditors and other consumer report users obtain SSNs from CRAs to make offers of credit or other benefits, when they obtain a consumer report for an applicant, or as part of the account monitoring or collections processes for existing customers.[111] In addition, SSNs may be included as part of sales of consumer loans, credit card accounts, and other assets in the secondary market, in part to facilitate credit checks by the buyer.[112]

Both furnishers and users of consumer reports commented that they collect SSNs from their customers to increase their certainty that the information they provide to CRAs, and the

---

107 *E.g.*, Comment of The Financial Services Roundtable, at 6-7.

108 *E.g.*, Comment of HSBC Finance Corporation, at 1; Comment of National Association of Federal Credit Unions, at 2.

109 *E.g.*, Gov't Accountability Office, GAO-07-1023T, *Social Security Numbers: Use Is Widespread and Protection Could Be Improved* 8 (June 21, 2007).

110 *See* FTC Report to Congress Under FACTA Sections 318 and 319, at 38-40 (Dec. 2004). *See also* Comment of ACA International, at 4; Comment of American Financial Services Association, at 3; Comment of Consumer Data Industry Association, at 3. Note, however, that CRAs do not rely exclusively on SSNs to match consumer data, but use additional data points as well. *See* FTC Report to Congress Under FACTA Sections 318 and 319, at 38-40.

111 *E.g.*, Comment of American Bankers Association, at 3.

112 *E.g.*, Comment of American Bankers Association, at 4; Comment of Visa U.S.A Inc., at 4.

consumer reports they receive from CRAs, relate to the right customer.[113] Some commenters, for example, stated that SSNs speed the process of verifying applicants' financial history, allowing them to open accounts and apply for loans with greater ease.[114] According to one commenter from the consumer reporting industry, if SSNs could not be used to match consumer credit information, more fragmented or isolated files would be created, reducing the content of an average consumer file by 15-20 percent.[115]

Beyond the credit reporting context, commenters noted several other uses of the SSN to link data across entities and sectors. For example, financial institutions use SSNs to transfer accounts or assets at one firm to another and to ensure the assets are accurately linked to the correct person and placed into the correct account.[116] In discussions with FTC staff, several organizations explained that medical providers and hospitals also may rely on SSNs to obtain and share patient records and information with other providers and insurance companies. Businesses share SSNs with their service providers to facilitate data processing, administrative, customer service, and other functions.[117] According to commenters, the SSN is useful because it helps to reduce errors and avoid misidentification of customer accounts and records.[118] In addition, employers and nonprofit organizations collect SSNs to run against various databases to verify identities and perform background and criminal history checks of prospective employees and volunteers.[119]

Commenters from a variety of industries asserted that SSNs can aid in locating individuals in an efficient and cost-effective manner. Entities can use SSNs to obtain identifying data on individuals from various sources, including CRAs and other data brokers, and this data are then used to find those individuals. Businesses collecting debt, for example, use SSNs to

---

113 *See, e.g.,* Comment of Mortgage Bankers Association, at 1; Comment of Visa U.S.A Inc., at 3-4; Comment of HSBC Finance Corporation, at 3.

114 *E.g.,* Comment of America's Community Bankers, at 1.

115 Comment of Consumer Data Industry Association, at 9.

116 *E.g.,* Comment of Securities Industry and Financial Markets Association, at 4.

117 Gov't Accountability Office, GAO-07-1023T, *Social Security Numbers: Use Is Widespread and Protection Could Be Improved* 9 (June 21, 2007); *see also* Comment of Equifax, Inc., at 4.

118 *E.g.,* Comment of American Bankers Association, at 3.

119 *E.g.,* Comment of American Financial Services Association, at 3; Comment of America's Community Bankers, at 2; Comment of Consumer Data Industry Association, at 11; Comment of National Association of Professional Background Screeners, at 2; Comment of National Business Coalition on E-Commerce and Privacy, at 6; Comment of Reed Elsevier Inc., at 6-7; *see also* Section V, below.

locate debtors.[120] Businesses also use SSNs to locate former employees to administer retirement benefits when the former employee has failed to update his or her address.[121] Private investigators and law enforcement likewise use SSNs to locate individuals. A number of private investigators and their associations submitted comments explaining how investigators attempting to locate witnesses and heirs, or to unite family members, use SSNs from credit header data[122] and public records (available through data brokers) to distinguish among individuals and locate the correct person.[123] Similarly, SSNs are used by law enforcement to locate fugitives, witnesses, deadbeat parents, and sex offenders who have failed to comply with address registration requirements.[124]

C. Alternatives to Using the SSN as an Identifier

Some private sector entities have reduced their use of SSNs in some contexts, including limiting the display of SSNs and transitioning to other identifiers. Several commenters stated, however, that switching from SSNs to another identifier entails financial and time costs and, perhaps, a loss of efficiency.[125] Many commenters claimed that, at least in some contexts, there are not yet any suitable alternatives to SSNs.[126]

In recent years, numerous entities have moved away from displaying SSNs on identification cards, in some cases in response to state laws prohibiting the practice.[127] Not displaying SSNs on cards, which are frequently carried by the holder, decreases the risk of identity theft through loss, theft, or duplication of the card. Some entities have taken the next step and have completely discontinued using SSNs as identification numbers. For example,

---

120 *See, e.g.*, Comment of American Financial Services Association, at 3; Comment of ACA International, at 6; Comment of Humphreys Debt Collection Law Firm, at 1; Comment of Direct Marketing Association, at 4.

121 *E.g.*, Comment of American Financial Services Corporation, at 4; Comment of National Business Coalition on E-Commerce and Privacy, at 7.

122 Credit header data is the personally identifying information found in the header of a credit report. It typically consists of name, address, former addresses, telephone numbers, date of birth, and SSN. It is not considered part of the credit history and therefore is not regulated under the FCRA.

123 *E.g.*, Comment of California Association of Licensed Investigators; Comment of National Council of Investigation & Security Services, Inc., at 2.

124 *E.g*, Comment of Consumer Data Industry Association, at 11-12; Comment of Reed Elsevier Inc., at 5.

125 *E.g.*, Comment of ID Analytics, at 1; Comment of Visa U.S.A. Inc., at 2, 5; Comment of Retail Industry Leaders Association, at 2; Comment of Society for Human Resource Management, at 2.

126 *E.g.*, Comment of Wells Fargo & Company, at 10; Comment of American Insurance Association, at 5-6.

127 *E.g.*, Comment of Mortgage Bankers Association, at 4-5; Comment of National Association of Mutual Insurance Companies, at 6. For a discussion of these state laws, *see* pp. 40-41, *infra*.

some health insurance providers have stopped using SSNs as subscriber identification numbers,[128] and an increasing number of colleges and universities are discontinuing their use of SSNs as student identification numbers, replacing them with university-specific numbers.[129]

Some organizations also have begun to transition from the use of the SSN as an internal identifier. Private sector entities have succeeded in developing and using alternative identification numbers for some of their internal needs.[130] Consumer advocate commenters noted that company-specific account numbers help protect consumers because, in the event a thief steals an account number, the victim's other accounts are not also at risk.[131]

Those companies that have transitioned from using the SSN on either identity cards or as internal identifiers asserted that it takes time and money to move to a new system. One organization commenter estimated that it took the organization approximately two years to complete the change from SSNs to unique employee numbers;[132] another stated that it took over four years for a similar transition.[133] According to several commenters, the cost and time involved in changing these systems and processes are part of the reason that some companies continue to use SSNs internally.[134]

Several organizations commented that, even if they were to limit SSN use for identification purposes, they would still need to rely on SSNs for data linkage. These commenters argued that customers are more likely to remember their SSNs than other identification numbers.[135] Several universities with which FTC staff consulted agreed with the

---

128 *E.g.*, WPS Health Insurance, WPS Commercial Insurance, GAMP, MCDA & HIRSP, www.wpsic.com/edi/comm_sub_p.shtml?mm=3 (explaining that non-SSN member numbers have been assigned to protect member privacy); Avrum D. Lank, *Danger in 9 digits: Most carry their Social Security number, if not their card*, Milwaukee Journal Sentinel, Apr. 17, 2004, *available at* http://www.pplusic.com/about/news.asp?newsarticle_id=3.

129 *E.g.*, Jennifer Epstein, *Moving Away From Social Security Numbers,* Inside Higher Ed, July 24, 2007, http://www.insidehighered.com/news/2007/07/24/idnumbers; EDUCAUSE Center for Applied Research, *Identity Management in Higher Education: A Baseline Study* 62-63 (2006), *available at* http://www.educause.edu/ir/library/pdf/ers0602/rs/ers0602w.pdf?bcsi_scan_DA3493EE5FC9D524=0&bcsi_scan_filename=ers0602w.pdf.

130 *E.g.*, Comment of American Bankers Association, at 6.

131 *E.g.*, Comment of Electronic Privacy Information Center, at 16.

132 Comment of First Data Corporation, at 4.

133 Comment of Mortgage Bankers Association, at 6.

134 *E.g.*, Comment of America's Community Bankers, at 3.

135 *E.g.*, Comment of National Business Coalition on E-Commerce and Privacy, at 16; Comment of Wells Fargo & Company, at 11.

commenters. They stated, for example, that alumni contacting a university to obtain a transcript several years after graduation may not recall their student identification number, and the universities need an additional way to retrieve records. According to commenters, hospitals face a similar problem locating and properly matching records of returning patients, as do banks for customers who have forgotten their account numbers.[136] In these situations, a consumer may not be *required* to provide his SSN to retrieve his records or information, but the SSN may offer an additional means of retrieving information where other identifiers have been forgotten. Several commenters asserted that, although it is possible in some instances to use customer information other than SSNs to locate records, it would be costly and difficult to do so and could create a greater risk of error. Commenters noted, for example, that name and address generally are not effective identifiers, because both can be shared by multiple individuals.[137]

Many private sector entities report that, notwithstanding the challenges, they have been able to reduce their reliance on SSNs, at least for some internal purposes. As discussed above, several commenters noted that many businesses have stopped using SSNs to identify employees (except for purposes such as tax reporting and verifying employment eligibility), and instead use other unique employee identifiers.[138] Similarly, according to the commenters, many businesses have discontinued use of SSNs as account numbers, in favor of company-specific identification numbers, although these numbers may be tied back to SSNs in some form.[139] Organizations that link to information outside the organization also typically tie any unique identifiers they use back to SSNs.[140]

Several commenters asserted that businesses at present have not found alternatives to the SSN for external linking, *i.e.*, that no other common identifier has yet been developed to permit the sharing and communication of information about individuals across institutions and sectors.[141] Some observers have advocated the use of other existing identifiers, such as names and dates of birth, stating that using a combination of these identifiers could allow for

---

136 *E.g.*, Comment of National Association of Federal Credit Unions, at 6; Comment of American Bankers Association, at 5.

137 *E.g.*, Comment of America's Community Bankers, at 1-2; Comment of Independent Community Bankers, at 2.

138 *E.g.*, Comment of Retail Industry Leaders Association, at 2; Comment of Wells Fargo & Company, at 10; Comment of American Petroleum Institute, at 3; Comment of First Data Corporation, at 4.

139 *E.g.*, Comment of National Association of Federal Credit Unions, at 5-6; Comment of Wells Fargo & Company, at 10-11.

140 *E.g.*, Comment of National Business Coalition on E-Commerce and Privacy, at 15; Comment of Wells Fargo & Company, at 10.

141 *E.g.*, Comment of Wells Fargo & Company, at 10-11; Comment of Equifax, Inc., at 1; Comment of The Financial Services Roundtable, at 10-11; Comment of Boeing Employees' Credit Union, at 2

identification as accurately as using SSNs.[142] Several business commenters, however, posited that existing, non-SSN identifiers would make sharing information across entities more difficult, more costly, and less reliable.[143] Commenters, for example, asserted that, without SSNs, credit checks would be more burdensome, take longer, and be more costly for financial institutions to process, ultimately increasing the cost of credit.[144] Another commenter stated that law enforcement and private investigators would face prohibitive costs in locating witnesses and tracking down fugitives if they were unable to use SSNs.[145]

V. The SSN in the Authentication Process

Authentication, broadly speaking, is the process used to determine that someone is who he or she claims to be. Organizations within the public and private sectors that interact regularly with the public need to authenticate individuals, whether they are applicants, existing customers, recipients of benefits, or otherwise.

In many respects, authentication is at the heart of the identity theft problem. If authentication worked perfectly, identity thieves with stolen consumer data would not be able to use it to take on another's identity. The ID Theft Task Force explained that "[e]fforts to facilitate the development of better ways to authenticate consumers without burdening consumers or business . . . would go a long way toward preventing criminals from profiting from identity theft."[146]

The authentication process can be broken down into two phases: 1) verifying the identity of the person at the outset of the relationship, and 2) later ensuring that the individual seeking access to his or her accounts is the same person who was initially enrolled. With respect to both phases, some entities have used the SSN as proof of identity itself, *i.e.*, when they accept that an individual is who he or she claims to be because the individual knows the correct SSN. Many observers have contended, however, that the SSN is ill-suited as proof of identity (*e.g.*, an authenticator) because it is so widely available and so commonly used as an identifier. Commenters from across the spectrum agreed that the dual use of the SSN as an identifier and authenticator is problematic, because an effective identifier will be widely used whereas an

---

[142] *E.g., Protecting the Privacy of the Social Security Number from Identity Theft: Hearing Before the Subcomm. on Social Security of the H. Comm. on Ways & Means,* 110th Cong. 3 (2007) (statement of Ana I. Anton, Ph.D).

[143] *E.g.,* Comment of Equifax, Inc., at 7-8; Comment of Independence Bank of Kentucky, at 1.

[144] *E.g.,* Comment of America's Community Bankers, at 2; Comment of Visa U.S.A. Inc., at 2; Comment of ACA International, at 4.

[145] *E.g.,* Comment of National Council of Investigation & Security Services, Inc., at 3-4.

[146] Task Force Report, at 6.

effective authenticator must be a secret.[147] For example, a fraud prevention business stated in its comment that "[a]s a stand-alone authenticator, SSNs have extremely limited value because they are so widely available."[148] As a result, according to the commenters and organizations contacted by FTC staff, most private sector entities currently do not use the SSN as the sole proof of identity, either for initial identity verification or existing account access.[149]

Yet, there is no assurance that use of multiple authenticators will prevent identity theft. For example, some organizations rely on checking driver's licenses to authenticate an individual, but identity thieves can obtain falsified licenses. Other organizations match identifying information provided by an applicant to that found in a third party database, such as that of a CRA, but this process only detects mismatched information and would not detect an identity thief who has provided sufficient accurate identifying information. Moreover, even when an organization's policies for authentication are robust, some employees may fail to comply with those policies.[150]

Although the SSN is often used (by itself or in combination with other personal data) as proof of identity, commenters asserted that more commonly organizations collect the SSN, not as an authenticator itself, but to enable them to access additional data that is then used to perform other authentication checks. For example, a creditor may collect an applicant's SSN to cross-check it against databases of SSNs used previously to commit fraud.

The following sections discuss the role of the SSN as proof of identity itself, as well as how it is used to facilitate other forms of authentication, both at the outset of a relationship and

---

147 *See, e.g.,* Comment of Electronic Privacy Information Center, at 13; Comment of Consumers Union, at 2; Comment of Eric Haskins; Comment of Stepp; Comment of Bryan Wiggins; *see also* Comment of Joe Smith; Comment of Samuelson Law, Technology & Public Policy Clinic, at 2-3; Lynn Lopucki, *Did Privacy Cause Identity Theft?*, 54 Hastings L.J. 1277, 1281 (2003); Janet Kornblum, *SSN is Password to Theft*, USA Today, Aug. 1, 2002, *available at* http://www.usatoday.com/tech/news/internetprivacy/2002-07-31-privacy_x.htm (explaining that identity theft occurs because SSNs are "so widely used that anyone with minimal research skills can get access to them, but they're also used as passwords to enter systems intended to be secure"). Some commenters suggested making the SSN public in order to discourage businesses from continuing to use the SSN as an authenticator. *E.g.,* Comment of Ramaswamy Aditya; Comment of Stephen Lloyd Arnold.

148 Comment of ID Analytics, at 1. Another commenter noted, however, that "[a]lthough knowing the proper SSN may not be convincing proof that someone is who he or she claims to be, ***not*** knowing the right SSN is still strong evidence that the person is an imposter." Comment of Wells Fargo & Company, at 9.

149 *E.g.,* Comment of Equifax, Inc., at 9-10; Comment of Wells Fargo & Company, at 7, 9; Comment of Securities Industry and Financial Markets Association, at 4; Comment of ID Analytics, at 1; Comment of Mortgage Bankers Association, at 5; Comment of U.S. Chamber of Commerce, at 4; Comment of Navy Federal Credit Union, at 2; Comment of National Business Coalition on E-Commerce & Privacy, at 13.

150 For example, in prior conversations with industry, FTC staff were told that employees may not always follow the financial institution's procedures and, for example, may open accounts without fully or carefully checking an applicant's identification.

for existing account access.

A. SSN Use in the Initial Identity Verification Process

Verification of identity at the initial stage of a relationship is vital to ensuring that the proper person gets the benefits for which he or she is applying, and to prevent fraud. Most of the business commenters asserted that the SSN, although not appropriate as the sole authenticator, is commonly used in the initial identity verification process to facilitate other forms of authentication.[151] For example, groups that work with children often use SSNs to check databases that allow them to verify the identity of their employees and volunteers, to ensure that sex offenders or others with a history of violent crimes do not infiltrate their organizations.[152]

Commenters described the various ways in which the SSN is used in the initial verification process, beyond simply relying on it as proof of identity. Some verification processes are directed by legal requirements, such as those covering financial institutions through the CIP rules under the USA PATRIOT Act.[153] As noted earlier, the CIP rules require financial institutions to establish a customer identification program specifying what identifying information they will collect when they open an account. This information (for U.S. persons) must include, at a minimum, the applicant's name, address, date of birth, and taxpayer identification number, which for individuals is their SSN.[154] In addition to collecting this information, financial institutions must have procedures for verifying the identity of their customers. These procedures must enable the financial institution "to form a reasonable belief that it knows the true identity of each customer."[155] This identity verification may be completed by documentary means, such as reliance on a driver's license or passport, or by non-documentary means, such as matching the identifying information provided by the applicant to that found in a third party database.[156]

---

151 *E.g.* Comment of Securities Industry and Financial Markets Association, at 3-4; Comment of Center for Information Policy Leadership, at 2-3; Comment of Consumer Data Industry Association, at 18. *See also* Comment of Equifax, Inc., at 9-10; Comment of Wells Fargo & Company, at 9-10; Comment of American Bankers Association, at 5.

152 *See, e.g.,* Comment of Safe Harbor Resources, at 1; Comment of National Business Coalition on E-Commerce and Privacy, at 6; Comment of Reed Elsevier Inc., at 6.

153 31 C.F.R. § 103.121 (banks, savings associations, credit unions, and certain non-federally regulated banks); 31 C.F.R. § 103.122 (broker-dealers); 17 C.F.R. § 270.0-11, 31 C.F.R. § 103.131 (mutual funds); and 31 C.F.R. § 103.123 (futures commission merchants and introducing brokers).

154 31 C.F.R. §§ 103.121(b), 103.122(b), 103.123(b) & 103.131(b). *See also* discussion at p. 6, *supra.*

155 31 C.F.R. §§ 103.121(b)(2), 103.122(b)(2), 103.123(b)(2) & 103.131(b)(2).

156 31 C.F.R. §§ 103.121(b)(2)(ii), 103.122(b)(2)(ii), 103.123(b)(2)(ii) & 103.131(b)(2)(ii).

Some commenters cited to the CIP rules as an example of how they conduct their initial identity verification process.[157] Although the CIP rules are intended primarily to prevent terrorism and money laundering, the enhanced verification procedures they require do likely reduce the incidence of identity theft by making it more difficult for thieves to impersonate individuals when opening an account. Yet, the CIP procedures may not always detect identity theft. As noted in the preamble to the Identity Theft Red Flags Rule, promulgated by the FTC and the federal bank regulatory agencies, "[c]ertain types of 'accounts,' 'customers,' and products are exempted or treated specially in the CIP rules because they pose a lower risk of money laundering or terrorist financing. Such special treatment may not be appropriate to accomplish the broader objective of detecting, preventing, and mitigating identity theft."[158]

Whether for legal compliance purposes or otherwise, the private sector utilizes a variety of SSN-based methods for initially verifying identity, which vary in their ability to detect identity theft. Many companies match the identifying data provided by an applicant, including the SSN, to that found in third party databases, such as that of a CRA.[159] As explained above, this practice may not prevent a thief who can provide accurate identifying information from opening an account in a victim's name. Moreover, some commenters asserted that credit issuers in some cases have opened new accounts when there is an SSN match, even though other identifying information was obviously wrong.[160] In discussions with FTC staff, officials of one bank stated that, given the transient nature of our society, a consumer would not be prevented from opening a new account solely on the basis of a mismatch between the address provided by an applicant and the address found in a third party database.

Some companies use the SSN to collect information from multiple data sources in order to develop challenge questions, the answers to which are likely to be known only by the true individual. For example, an individual may be asked what financial institution holds the mortgage on his or her home, or about previous vehicles owned. This information is linked to the consumer by his or her SSN.[161] This process is known as "knowledge-based authentication."

---

157 *E.g.*, Comment of American Council of Life Insurers, at 2; Comment of National Association of Federal Credit Unions, at 2.

158 16 C.F.R. Part 681.

159 *E.g.*, Comment of MasterCard Worldwide, at 3; Comment of Center for Information Policy Leadership, at 3; Comment of Consumer Data Industry Association, at 10; Comment of National Retail Federation, at 2; Comment of National Business Coalition on E-Commerce and Privacy, at 16; Comment of Reed Elsevier Inc., at 5; Comment of Securities Industry and Financial Markets Association, at 3.

160 *E.g.* Comment of Electronic Privacy Information Center, at 4; Comment of Samuelson Law, Technology & Public Policy Clinic, 3-4.

161 *E.g.*, Comment of Reed Elsevier Inc., at 3; Comment of Consumer Data Industry Association, at 17-18; Comment of Direct Marketing Association, at 3.

Some organizations cross-check the consumer's SSN to lists maintained by the SSA. For employers, the SSA will provide at no charge the name of a living person associated with a particular SSN. The SSA also is considering offering a Consent-Based Social Security Number Verification Service to registered private sector entities.[162] This service would verify a name and SSN combination so long as the registered company has obtained a written consent from the SSN-holder.[163] The SSA also provides the Social Security Death Index to the National Technical Information Service, which provides public access to the index for a fee. This index enables requesters to verify whether an SSN-holder has been reported deceased.[164] Additionally, the SSA High Group List identifies those ranges of SSNs that have been issued by the SSA and corresponding issuance dates, thus allowing organizations to identify proffered SSNs that are inconsistent with the individual's date of birth.[165]

Some entities cross-check an applicant's identifying information, including the SSN, against databases of identifying information previously used to commit fraud.[166] In one type of fraud database, member financial institutions contribute experiential information on check fraud and account abuse, along with the perpetrator's SSN, to a central database. Members can then cross-check an applicant's identifying information, including the SSN, against this database to assist them in detecting potential fraud.[167]

Some businesses use the SSN as an element in their quantitative fraud prediction models. These models are designed to flag suspect patterns of use of identifying information that might

---

[162] Social Security Administration, Announcement of New Consent-Based Social Security Number Verification (CBSV) Service by the Social Security Administration (Jan. 12, 2007), http://www.ssa.gov/bso/cbsvMarketing.html.

[163] *Id.* According to the SSA, there will be a "substantial fee" to register for this service.

[164] *E.g.*, Comment of Wells Fargo & Company, at 11; Comment of The Financial Services Roundtable, at 11; Comment of Equifax, Inc., at 11-12; Comment of Mortgage Bankers Association, at 7; Comment of Independent Community Bankers of America, at 4; Comment of American Bankers Association, at 6; Comment of Consumer Data Industry Association, at 17; Comment of National Business Coalition on E-Commerce and Privacy, at 16.

[165] *E.g.*, Comment of Wells Fargo & Company, at 11; Comment of The Financial Services Roundtable, at 11-17; Comment of Equifax, Inc., at 11-12; Comment of Mortgage Bankers Association, at 7; Comment of Independent Community Bankers of America, at 4-5; Comment of American Bankers Association, at 6; Comment of Consumer Data Industry Association, at 17-18; Comment of National Business Coalition on E-Commerce and Privacy, at 16. The matching of SSN with date of birth is not fool-proof, however. Especially in years past, some individuals did not apply for an SSN until they became employed. Immigrants also often apply for SSNs later in life. In these cases, the SSN will correspond with a date considerably later than the individual's date of birth.

[166] *E.g.*, Comment of America's Community Bankers, at 2; Comment of American Bankers Association, at 6; Comment of Consumer Data Industry Association, at 20; Comment of National Association of Mutual Insurance Companies, at 8; Comment of Wells Fargo & Company, at 4.

[167] *E.g.*, Comment of National Association of Federal Credit Unions, at 3.

indicate that an application or proposed transaction is fraudulent.[168] One credit card company, for example, stated that a single SSN listed on an unusually large number of applications among one or more financial institutions is potentially indicative of fraud or identity theft.[169] Although many of these fraud prevention software products and services rely on the SSN, at least one such provider commented that the SSN is just one data point among many that it uses for detecting fraud (albeit a valuable one).[170] The commenter noted that its identity risk scoring technology is effective in countries that do not have an SSN equivalent, but asserted that inclusion of the SSN improved fraud detection performance by 10-20 percent.[171]

B. Alternatives to SSN Use for Initial Identity Verification

Some observers have contended that one alternative to using the SSN for initial identity verification is to utilize combinations of other data, such as name and date of birth, to access information to be used in the authentication process.[172] These combinations of data can be used to collect information from multiple data sources to develop knowledge-based authentication questions. Because these data points are more readily available than SSNs, however, some commenters noted that it is important that they be used only to access data to perform other authentication checks, and not as authenticators themselves.[173]

The vast majority of business commenters asserted, however, that, at the present time, there is no equally efficient or accurate alternative to using the SSN in the initial identity verification process.[174] According to some commenters, as the only permanent and unique identifier, the SSN ties together the data from various sources that comprise the fraud

---

168 *E.g.,* Comment of National Association of Mutual Insurance Companies, at 8; Comment of Wells Fargo & Company, at 9; Comment of The Financial Services Roundtable, at 9.

169 Comment of MasterCard Worldwide, at 4. Under recently issued federal regulations, financial institutions and creditors are required to have an identity theft prevention program that detects these types of suspect patterns or practices, *i.e.*, "red flags." 16 C.F.R. Part 681.

170 Comment of ID Analytics, at 1-2.

171 *Id.*

172 *E.g., Protecting the Privacy of the Social Security Number from Identity Theft: Hearing Before the Subcomm. on Social Security of the H. Comm. on Ways & Means,* 110th Cong. 3 (2007) (statement of Ana I. Anton, Ph.D).

173 *Id.*

174 *See, e.g.,* Comment of MasterCard Worldwide, at 2; Comment of ACA International, at 24; Comment of First Data Corporation, at 2; Comment of National Association of Mutual Insurance Companies, at 5; Comment of National Business Coalition on E-Commerce and Privacy, at 11; Comment of Equifax, Inc., at 7-8; Comment of The Financial Services Roundtable, at 7, 12; Comment of National Association of Professional Background Screeners, at 3; Comment of Wells Fargo & Company, at 7; Comment of Visa U.S.A. Inc., at 2; Comment of American Insurance Association, at 5; Comment of National Retail Federation, at 2.

databases.[175] Some commenters asserted that including the SSN in these databases adds to their efficiency and accuracy,[176] and others noted that eliminating the SSN from this process would raise the costs and burdens associated with these fraud checks.[177] One commenter suggested that, if employers were unable to use SSNs, they might choose not to screen employees or volunteers at all, rather than risk worker retaliation over a mistaken identity.[178]

Many businesses commented that prohibiting the use of the SSN for initial identity verification would likely lead to more identity theft, because there would be less data available to match in order to verify identity.[179] Some industry commenters argued that identity theft prevention could be strengthened by adopting a more robust verification system using more data (*e.g.*, cell phone numbers and driver's license numbers), rather than fewer.[180]

Some organizations have discussed a system in which a third party verifies an individual's identity and then issues the applicant an electronic credential that could be used by the individual to prove his identity across private sector entities.[181] Some refer to these systems as identity oracles. According to organizations promoting these systems, this electronic credential could reduce or eliminate the need for private sector entities to collect SSNs directly from consumers. Although such a system would reduce the number of instances in which a consumer would have to provide his or her SSN, it would not entirely eliminate the collection of SSNs, because the consumer still would have to supply his or her SSN to the third party.

C. SSN Use for Existing Account Access

Many private sector entities use the SSN to grant consumers access to their existing accounts. Authentication for existing account access typically occurs when a person provides

---

175 *E.g.*, Comment of Mortgage Bankers Association, at 7; Comment of American Financial Services Association, at 3; Comment of National Association of Mutual Insurance Companies, at 4.

176 *E.g.*, Comment of National Association of Mutual Insurance Companies, at 4.

177 *E.g.*, Comment of America's Community Bankers, at 2; Comment of Equifax, Inc., at 12-13; Comment of American Bankers Association, at 6; Comment of HSBC Finance Corporation, at 4; Comment of Safe Harbor Resources, at 1.

178 Comment of Safe Harbor Resources, at 1.

179 *E.g.*, Comment of MasterCard Worldwide, at 3-4; Comment of American Financial Services Association, at 3.

180 *E.g.*, Comment of Consumer Data Industry Association, at 4; Comment of National Business Coalition on E-Commerce and Privacy, at 4.

181 *E.g.*, Federal Financial Institutions Examination Council, *Authentication in an Internet Banking Environment* 14 (Oct. 12, 2005) (hereinafter "FFIEC Guidance"), *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf.

valid identifying information followed by one or more authentication credentials, also known as "factors," to prove his or her identity. An authentication factor is secret or unique information linked to a specific person that is used to verify identity.[182] Existing authentication technologies and methods involve three basic factors:

- Something a person **knows** – most commonly a password or personal identification number (PIN), but also may be a question that requires specific knowledge only the customer is likely to have, such as recent transaction history on a bank account.
- Something a person **has** – most commonly a physical device, such as a Universal Serial Bus (USB) token or a smart card.
- Something a person **is** – most commonly a physical characteristic, such as a fingerprint, iris, face, voice, or hand geometry. This type of authentication is referred to as biometrics.[183]

The strongest existing account authentication systems are multi-factored, *i.e.*, the system uses at least two of the three factors listed above.[184] An example of a multi-factored authentication system is an ATM card. To access her account with an ATM card, the consumer needs both the card itself (something she has), and a PIN (something she knows). Some entities use only a single factor in authentication, but if it is compromised, there are no other fail-safes in the system to prevent unauthorized access.[185]

Some organizations treat the SSN as something the person knows for purposes of existing account access – essentially treating it as a password, or authenticator – although many have moved away from this practice.[186] As discussed above, given that the SSN is used widely as an identifier and is therefore not a secret, many observers assert that using it as an authenticator can facilitate identity theft.[187] In the view of these observers, the fact that someone knows an SSN does little to prove that he is, in fact, the person associated with the SSN. Although it is unclear to what extent private sector entities currently use the SSN as the single authentication factor for

---

182 *See* FFIEC Guidance, at 7.

183 *See* FFIEC Guidance, at 7; Task Force Report, at 43.

184 *E.g.*, Comment of Direct Marketing Association, at 3. The FFIEC Guidance, issued by the federal bank regulatory agencies in 2005, recognized the importance of multi-factor authentication for certain high-risk transactions. It specified that the banking agencies "consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties." FFIEC Guidance, at 1.

185 *See* Task Force Report, at 43; Comment of Coalition for Sensible Public Records Access, at 2-3 .

186 *E.g.*, Comment of National Association of Federal Credit Unions, at 5.

187 *See* discussion at pp. 26-27, *supra.*

access to existing accounts, many agree that such a practice creates numerous vulnerabilities to identity theft.[188] Most business commenters asserted that the SSN is used as an authenticator only in conjunction with additional measures, some of which may not be evident to the consumer.[189]

According to the commenters, private sector entities generally do not use the SSN for in-person account access, instead relying in most cases on government-issued photo identification.[190] For account access through online and telephone channels, on the other hand, businesses do appear to rely more on the SSN for authentication. The effectiveness of the authentication process for existing account access appears to vary widely, often based on costs and transaction risk (*i.e.,* conducting a more robust authentication when the risk and consequences of fraud are higher).[191]

A number of commenters stated that they no longer use the SSN as an authenticator (*i.e.,* a password) to access an online account.[192] In discussions with FTC staff, several businesses noted that it was more commonplace several years ago to use the SSN as the default password for online account access, but that the vast majority of businesses no longer do so. Some companies that no longer use the SSN as the password, however, continue to use it as an identifier, or user ID, for online account access.[193] Other companies, although no longer using the SSN for online account access, may ask the consumer for his SSN in order to reset an online password.[194]

---

188 *E.g.,* Comment of Coalition for Sensible Public Records Access, at 2-3.

189 *E.g.,* Comment of Boeing Employees' Credit Union, at 2-3; Comment of MasterCard Worldwide, at 2; Comment of National Business Coalition on E-Commerce and Privacy, at 13; Comment of American Petroleum Institute, at 5; Comment of American Bankers Association, at 5; Comment of American Council of Life Insurers, at 3; Comment of Mortgage Bankers Association, at 7; Comment of Wells Fargo & Company, at 9; Comment of Securities Industry and Financial Markets Association, at 4; Comment of Equifax, Inc., at 9-10; Comment of The Financial Services Roundtable, at 9.

190 *E.g.*, Comment of National Association of Federal Credit Unions, at 5.

191 *See* Comment of Mortgage Bankers Association, at 4 (discussing curtailing SSN use when the risk of account transactions or inquiries is low). Allowing account access based on SSN alone may be problematic, however, even for what may appear to be a low-risk transaction (*e.g.,* viewing an account balance), to the extent an identity thief is able to leverage the information obtained to gain access to the account for high-risk transactions (*e.g.,* account withdrawals).

192 *E.g.,* Comment of Boeing Employees' Credit Union, at 2; Comment of National Association of Federal Credit Unions, at 4-5; *but see* Comment of Independent Community Bankers of America, at 3 (noting that "the SSN or the last four digits can be used to verify identity when customers are using telephone or online banking applications").

193 In discussions with FTC staff, some businesses explained that although new customers no longer have the SSN as their online user identification, legacy customers may still use the SSN in this manner.

194 *E.g.,* Comment of First Data Corporation, at 3.

Commenters also noted that some online authentication processes utilize additional "behind the scenes" safeguards that are invisible to the consumer. For example, many companies use IP address verification for online transactions.[195] With the IP address, the organization is able to determine that the person logging on to an online account is using the device on the IP network they typically use. A person logging on using a different device generally must satisfy additional authentication measures.

Many companies continue to require their customers to provide their SSN, or the last four digits of their SSN, to gain access to an existing account via the phone channel.[196] As of 2005, according to a market study, 46 percent of large banks and 50 percent of mid-tier banks used the SSN for access to an account via telephone.[197] One commenter contended that relying on the SSN for this type of access facilitates telephone pretexting, the practice of using fraud or deceit to gain access to another person's telephone records.[198] Thus, if a telephone company allows access to call records based on an individual's SSN, pretexters who obtain that SSN can use it to access the records. Many industry commenters asserted that additional information beyond the SSN usually is required to access an account via the phone channel.[199] In some cases, the additional identifying information also may be widely known, such as an address or telephone number. In other cases, the additional information may be more difficult for an identity thief to obtain. For example, some companies require the caller to identify account numbers or shared secrets,[200] such as a pet's name or the amount of a monthly mortgage payment. And, as with the online channel, some companies use additional "behind the scenes" safeguards. For example, a company may verify that the person is calling from the phone number on record with the account. If the individual calls from a different phone number, additional authentication is required.[201]

---

195 *E.g.*, Comment of Mortgage Bankers Association, at 5; *see also* FFIEC Guidance, at 12-13.

196 *E.g.*, Comment of American Petroleum Institute, at 4; Comment of Boeing Employees' Credit Union, at 3; Comment of National Association of Federal Credit Unions, at 3, 6; Comment of Independent Community Bankers of America, at 3; Comment of Irwin Financial Corporation, at 3; Comment of HSBC Financial Corporation, at 4.

197 John Adams, *Knowing Customers: Banks Battle the Image of Social Insecurity: Unisys Says nearly Half of Banks Use Social Security Numbers, An Easily Nabbed Item, As Authentication*, Bank Technology News, May 1, 2005, *available at* http://www.highbeam.com/doc/1G1-132481425.html.

198 *E.g.*, Comment of Samuelson Law, Technology & Public Policy Clinic, at 2-3.

199 *E.g.*, Comment of American Petroleum Institute, at 4; Comment of National Association of Federal Credit Unions, at 5; Comment of Securities Industry and Financial Markets Association, at 4.

200 *E.g.*, Comment of National Association of Federal Credit Unions, at 5 (last transaction amount); Comment of Reed Elsevier Inc., at 3 (prior addresses or prior cars owned); Comment of American Council of Life Insurers, at 5.

201 Identity thieves have begun using voice over internet protocol (VOIP) to spoof phone numbers so that it appears to the company as if the call is coming from the victim. ConsumerAffairs.com, *"Vishing" Is Latest Twist in Identity Theft Scam*, July 24, 2006, *available at* http://www.consumeraffairs.com/news04/2006/07/scam_vishing.html.

D. Alternatives to SSN Use for Existing Account Access

In contrast to initial identity verification, many commenters stated that there are good alternatives to using the SSN for existing account access. In fact, several commenters recommended that the use of the SSN as a password be prohibited.[202] One commenter, for example, asserted that most credit unions have moved away from using the SSN for existing account access, and now ask members for passwords, PINs, or other shared secrets.[203]

In addition to or in lieu of SSNs, there are other methods of authentication that can be used by businesses to authenticate identity for access to an existing account.[204] These methods include, among other things, USB tokens, smart cards, and biometrics.[205] Some business commenters argued that alternative authentication methods present substantial cost concerns.[206] On the other hand, several business representatives told FTC staff that some available authentication techniques are relatively inexpensive. Moreover, the costs of these alternatives may be offset by a reduction in fraud losses.[207]

Some commenters argued that requiring better authentication for existing account access, although more secure, would be inconvenient or burdensome for consumers, requiring them to remember multiple passwords or PINs to prove their identity for different accounts.[208] One commenter cautioned that consumers will not accept authentication methods that are overly-complex, possibly causing a reduction in the use of online financial services.[209]

---

202 *See, e.g.,* Comment of American Financial Services Association, at 4; Comment of Consumers Union, at 8; Comment of Hamilton; Comment of ACA International, at 28; Comment of Equifax, Inc., at 7; Comment of Center for Information Policy Leadership, at 5; *see also* Comment of TRUSTe, at 2.

203 Comment of National Association of Federal Credit Unions, at 5.

204 Alternatively, some commenters have suggested that companies could utilize a truncated version of the SSN. *E.g.,* Comment of National Business Coalition on E-Commerce and Privacy, at 14. Although this would limit the number of company employees with access to an individual's full SSN, it would not prevent an identity thief who had obtained that individual's SSN from using it to gain access to his or her accounts.

205 *See* FFIEC Guidance, at 7-13.

206 *E.g.,* Comment of Missouri Credit Union Association, at 3; Comment of Mortgage Bankers Association, at 4, 6.

207 *E.g.,* Comment of Wells Fargo & Company, at 10.

208 *E.g.,* Comment of Missouri Credit Union Association, at 2; Comment of Mortgage Bankers Association, at 6.

209 *E.g.,* Comment of Wells Fargo & Company, at 9.

VI. Protecting the SSN from Misuse

Numerous laws, regulations, and industry guidelines have been promulgated to protect SSNs from identity thieves.

A. Industry Guidelines

In 1997, prior to the passage of federal SSN protection laws, several companies in the business of marketing consumer data established a self-regulatory program to restrict the collection and sale of SSNs. These companies – members of the information services industry that provide commercial services used to locate, identify, or verify the identity of individuals – formed the Individual Reference Services Group (IRSG). The IRSG principles were designed to govern the availability of information obtained from non-public sources through commercial database services, placing varying degrees of restrictions and protections depending on the sensitivity of the data and the prospective recipient.[210] Specifically, the principles prohibited members from disseminating certain sensitive non-public information, including SSNs, to the general public.[211] This self-regulatory effort has largely been supplanted by subsequent legislation protecting the SSN, in particular the Gramm-Leach-Bliley Act (GLBA).

B. Existing Laws Protecting SSNs

1. Federal laws

There are a variety of federal laws that limit the collection, transfer, and/or use of SSNs by private sector entities. The GLBA, which was enacted in 1999 and became effective in 2001, imposes privacy and security obligations on financial institutions with respect to consumer data.[212] Subject to certain exceptions, financial institutions are prohibited by Title V of the GLBA from disclosing non-public personally identifiable financial information, including SSNs, to non-affiliated third parties without first providing consumers with notice and the opportunity to opt out of the disclosure.[213] In addition, the GLBA requires financial institutions to implement appropriate physical, technical, and administrative safeguards to protect the security and integrity

---

210 *See* Federal Trade Commission, *Individual Reference Services: A Report to Congress* (Dec. 1997), *available at* http://www.ftc.gov/os/1997/12/irs.pdf.

211 *Id.*

212 15 U.S.C. § 6801 *et seq.*

213 15 U.S.C. § 6802; Privacy of Consumer Financial Information, 16 C.F.R. Part 313. The exceptions include for purposes of consumer reporting (pursuant to the FCRA), fraud prevention, law enforcement and regulatory or self-regulatory purposes, compliance with judicial process, and public safety investigations. 15 U.S.C. § 6802(e). *See also Trans Union LLC v. FTC*, 295 F.3d 42, 50-51 (D.C. Cir. 2002) (upholding FTC regulation defining personally identifiable financial information to include consumer credit report header data, such as name, address, telephone number, and SSN).

of the information they receive from customers, whether directly or from other financial institutions.[214] The Fair and Accurate Credit Transactions Act of 2003 (FACTA) amended the FCRA to allow a consumer to request that a CRA truncate his or her SSN on the consumer reports sent to the consumer.[215] FACTA further requires businesses that maintain information derived from a consumer report to adopt reasonable procedures to dispose of such information properly and safely.[216] The Health Insurance Portability and Accountability Act (HIPAA) limits the disclosure of SSNs by covered health care organizations without patient authorization.[217] The Drivers' Privacy Protection Act prohibits state motor vehicle departments from disclosing SSNs, subject to certain "permissible uses."[218]

Although there currently is no broadly applicable federal standard governing the ways in which the private sector may use SSNs, Congress recently has considered a number of bills that would restrict the collection, display, purchase, sale and/or use of SSNs, including the following:

- The Social Security Number Misuse Prevention Act, S. 238, introduced by Senator Dianne Feinstein (D-CA), would prohibit the sale or display of SSNs with exceptions for public health, law enforcement, national security, or business purposes, such as credit checks.[219] S. 238 also would limit the circumstances under which private sector entities could require customers to provide SSNs and when companies could withhold services if an individual refused to provide his or her SSN.[220] The bill was referred to the Judiciary Committee on January 10, 2007, and hearings were held on March 21, 2007.

- The Social Security Number Privacy and Identity Theft Protection Act of 2007, H.R. 3046, introduced by Representative Michael McNulty (D-NY), would prohibit the sale or display of SSNs except for certain specified purposes, such as credit reporting, tax compliance, or law enforcement.[221] The bill was reported by

---

214 15 U.S.C. § 6801(b). The FTC's Safeguards Rule and the federal bank regulatory agencies' guidance implement this requirement. *See* Standards for Safeguarding Consumer Information, 16 C.F.R. Part 314; Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. Part 364, App. B.

215 15 U.S.C. § 1681g(a)(1)(A).

216 15 U.S.C. § 1681w. The FTC's disposal rule implementing this provision is at 16 C.F.R. § 682.3.

217 45 C.F.R. Part 164.

218 18 U.S.C. § 2721 *et seq.*

219 Social Security Number Misuse Prevention Act, S. 238, 110th Cong. § 3 (2007).

220 *Id.* § 7.

221 Social Security Number Privacy and Identity Theft Protection Act of 2007, H.R. 3046, 110th Cong. §§ 2 & 8 (2007).

the House Ways and Means Committee on September 24, 2007.

- The Social Security Number Protection Act of 2007, H.R. 948, introduced by Representative Edward J. Markey (D-MA). H.R. 948 would prohibit the purchase or sale of SSNs in violation of rules to be promulgated by the FTC.[222] H.R. 948 includes exemptions from the prohibition for certain purposes such as public health and law enforcement uses.[223] The bill was reported by the House Committee on Energy and Commerce on June 13, 2007 and sequentially referred to the House Committee on Ways and Means.

Adequate data security is a critical means by which SSNs are kept out of the hands of thieves. The ID Theft Task Force's Strategic Plan describes the link between SSNs and identity theft, highlights the importance of robust data security in the private sector, and recommends the establishment of national standards that (i) extend data safeguards requirements to entities not covered by existing laws, and (ii) require businesses that experience a data breach to notify affected consumers in certain circumstances.[224] Currently, there is no national notification standard for data breaches. The FTC does enforce several existing, sector-specific laws and regulations that, explicitly or implicitly, contain data security requirements, including the GLBA Safeguards Rule, the FCRA's "know your customer" requirements,[225] the FACTA Disposal Rule, and the Federal Trade Commission Act.[226] Since 2001, the Commission has brought fourteen cases challenging businesses that failed to reasonably protect sensitive consumer information that they maintained.[227] In a number of these cases, the Commission alleged that the company had misrepresented the nature or extent of its security procedures.[228] In some cases, the alleged security inadequacies led to breaches that caused substantial consumer injury and were

---

222 Social Security Number Protection Act of 2007, H.R. 948, 110th Cong. §§ 3 & 4 (2007).

223 *Id.* § 3.

224 Task Force Report, at 32-38.

225 15 U.S.C. § 1681 *et seq.* The FCRA specifies that CRAs may provide consumer reports only for enumerated "permissible purposes" (15 U.S.C. § 1681b), and requires that they have reasonable procedures to verify the identity and permissible purposes of prospective recipients of their reports (15 U.S.C. § 1681e).

226 15 U.S.C. § 45(a) (prohibits unfair or deceptive acts or practices in or affecting commerce).

227 *See generally* Federal Trade Commission, Privacy Initiatives, http://www.ftc.gov/privacy/index.html.

228 *E.g.*, *United States v. ChoicePoint Inc.*, No. 1:06cv0198 (N.D. Ga. settlement entered Feb. 15, 2006); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of MTS Inc., d/b/a/ Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

challenged as unfair practices.[229] Several cases involved alleged violations of the Safeguards Rule, the Disposal Rule, or the FCRA.[230]

2. State laws

A number of states have enacted statutes that restrict the use or display of SSNs in certain contexts. Many of these state laws specifically restrict companies and individuals from publicly displaying SSNs, printing them on identification or membership cards, transmitting them over the Internet, or mailing them without additional safety measures.[231] California was the first state to pass a law restricting the use of SSNs. The California law bars certain companies from publicly displaying SSNs and prohibits the printing of SSNs on insurance cards and certain documents mailed to customers.[232] Many other states have followed California's lead, and as of September 2007 there were approximately 20 state laws limiting in some fashion the public display and/or use of SSNs.[233] For the most part, commenters indicated that it has not been overly difficult or costly to comply with laws prohibiting public display of SSNs.[234] Some states have gone further, however, restricting the solicitation of SSNs by private sector companies,[235]

---

229 *E.g.*, *United States v. ChoicePoint Inc.*, No. 1:06cv0198 (N.D. Ga. settlement entered Feb. 15, 2006); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005).

230 *E.g.*, *United States v. ChoicePoint Inc.*, No. 1:06cv0198 (N.D. Ga. settlement entered Feb. 15, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (Apr. 12, 2005); *In the Matter of Sunbelt Lending Services, Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005).

231 CRS Report for Congress, *The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality* 11 n.56 (Jan. 9, 2007).

232 Cal. Civ. Code § 1798.85.

233 *See, e.g.*, Ariz. Rev. Stat. § 44-1373 (prohibits, among other things, printing of an SSN on identification cards, requiring an individual to transmit an SSN over the Internet unless it is through a secure connection, requiring use of an SSN to access an Internet website unless another security device or password is used, and printing an individual's SSN on any material to be mailed to an individual, unless required by law); 815 Ill. Comp. Stat. 505/2QQ (prohibits printing of SSNs on insurance cards); *see also* Gov't Accountability Office, GAO-07-1023T, *Social Security Numbers: Use is Widespread and Protection Could Be Improved* 4 (June 21, 2007); Gov't Accountability Office, GAO-05-1016T, *Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain* 12-15 & Appendix III (Sept. 15, 2005).

234 Comment of American Council of Life Insurers, at 4-5; Comment of Coalition to Implement the FACT Act, at 3; Comment of Wells Fargo & Company, at 8.

235 *E.g.*, Tex. Bus. & Com. Code Ann. § 35.581 (prohibits a business from requiring that an individual disclose his or her SSN in order to obtain goods or services, unless the business has a privacy policy and maintains the confidentiality of that SSN).

prohibiting disclosure of SSNs or any number derived therefrom,[236] or subjecting a truncated SSN to the same restrictions on display and transfer as the full SSN.[237] Some commenters posited that these laws will be, or have been, difficult to comply with and may impede important uses of SSNs.[238]

In addition to restricting the use or display of SSNs, a number of states also have passed laws requiring organizations that collect and maintain SSNs to safeguard that information. For example, some states have required organizations to establish policies to properly dispose of documents containing SSNs,[239] limit employee access to SSNs to those employees with a necessary purpose,[240] and ensure that any transmission of SSNs be performed securely.[241]

As of August 2007, 38 states, plus the District of Columbia and Puerto Rico, had enacted laws requiring data breach notification when personally identifiable information, including SSNs, is accessed without authorization.[242] Typically, the statutes mandate that a private sector entity that suffers a breach notify affected consumers, at least under certain circumstances, although the laws vary in several particulars, including the level of identity theft risk that triggers the notice requirement.[243] Some states also require that the breached entity send notification to a designated state agency, the CRAs, or other potentially affected parties.[244] Data breach notices may help consumers avoid or mitigate injury from the compromise of their information by allowing them to take appropriate protective actions, such as placing a fraud alert on their credit file or

---

236 *E.g.*, N.Y. Gen. Bus. Law § 399-dd (effective Jan. 1, 2008) (restricting publication or transmittal of the SSN or any number derived from such number).

237 2007 Minn. Laws, Ch. 129 §§ 11, 55-57 (effective July 1, 2008).

238 *E.g.*, Comment of Consumer Data Industry Association, at 16-17; Comment of Equifax, Inc., at 9; Comment of Wells Fargo & Company, at 7-8.

239 *E.g.*, Mich. Comp. Laws § 445.84.

240 *E.g.*, 2007 Ore. Laws 759.

241 *E.g.*, N.Y. Gen. Bus. Law § 399-dd (effective Jan. 1, 2008).

242 Consumers Union, Notice of Security Breach State Laws, Aug. 21, 2007, http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf; *see also* National Conference of State Legislatures, State Security Breach Notification Laws, Jan. 9, 2007, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm; David Zetoony, *3 New State Laws Expand Data Breach Obligations*, DMNews, May 8, 2006, http://www.dmnews.com/cms/dm-news/legal-privacy/36806.html. State legislators continually introduce new legislation addressing data breach notification and SSN protection. *See* National Conference of State Legislatures, Introduced Social Security Number Legislation – 2007 Session, http://www.ncsl.org/programs/lis/privacy/SSN2007_Pending.htm.

243 *E.g.*, Cal. Civ. Code § 1798.82; Del. Code Ann. Tit. 6, § 12B-101 to 12B-106; Conn. Gen. Stat. § 36a-701.

244 *E.g.*, Vt. Stat. Ann. tit. 9, § 2435; N.Y. Gen. Bus. § 889-aa; Colo. Rev. Stat. § 6-1-716.

monitoring their accounts.[245] Moreover, various private sector entities indicated to FTC staff that the proliferation of state data breach laws has compelled companies to weigh the usefulness of the SSN against the potential liability that comes with SSN use or collection.

C. Gaps in Existing Laws and Possible Alternatives

Notwithstanding the many federal and state laws that, directly or indirectly, govern the use and collection of SSNs, there are some gaps in the regulatory framework. For the most part, existing laws protecting SSNs are limited to specific industries and/or specific states; there is no national legislative framework that applies to all entities that collect and use SSNs. For example, certain segments of the private sector, such as financial institutions, have requirements mandating that they implement safeguards to protect SSNs, whereas other entities, such as utilities, have few or no such requirements.[246] The GAO concluded that these gaps may create a risk that SSNs will be misused.[247]

Some commenters, including members of the private sector, supported imposition of safeguards requirements – similar to those set out in GLBA – for companies other than financial institutions.[248] They stated that an expanded regulatory scheme would establish a uniform legal framework for those private sector entities that collect and use SSNs.[249]

Some commenters asserted that truncation is a useful tool for protecting SSNs,[250] while others contended that truncation hinders their use of SSNs for legitimate purposes.[251] There is currently no national standard for truncating SSNs; some businesses display the first five digits, while others display the last four digits.[252] As noted earlier, the FACTA requires CRAs to

---

245 Task Force Report, at 34.

246 *See, e.g.*, Comment of Consumers Union, at 3.

247 Gov't Accountability Office, GAO-05-1016T, *Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain* (Sept. 15, 2005).

248 *E.g.*, Comment of America's Community Bankers, at 4; Comment of The Financial Services Roundtable, at 2.

249 *E.g.*, Comment of The Financial Services Roundtable, at 2.

250 *E.g.*, Comment of Wells Fargo & Company, at 7.

251 *E.g.*, Comment of Consumer Data Industry Association, at 17.

252 Gov't Accountability Office, GAO-07-1023T, *Social Security Numbers: Use is Widespread and Protection Could Be Improved* 12-13 (June 21, 2007); Comment of Consumers Union, at 3. The first five digits indicate the date and location of the number's issuance, while the last four digits are the unique portion of the SSN. A private investigator told FTC staff that he principally uses the issuance location information from the first five digits to locate people.

truncate the SSN on reports they provide to consumers, upon the consumer's request. It is not clear, however, to what extent truncation reduces identity theft or which method of truncation is preferable.[253]

Finally, some organizations with which FTC staff spoke recommended that the SSA assign a PIN to the SSN so that identity thieves are unable to use the SSN even if they are able to access it.

VII. Conclusion

Since the SSN was created in 1935, the private sector has adopted it for various purposes. Some of the private sector uses of the SSN have been driven by legal requirements, such as for tax reporting purposes. Organizations have developed other uses for the SSN, primarily because it currently is the only permanent, unique identifier that most Americans have. Thus, businesses and other entities use the SSN to link individuals to their records (both internally and externally), as well as in the authentication process to help prove that an individual is who he says he is.

As the private sector use of the SSN expanded, so too did its availability and value for identity thieves. Especially for new account fraud, the SSN generally is a necessary (if not always sufficient) piece of information for identity thieves. And, a thief with an individual's name and SSN often can leverage that information to obtain whatever other data is needed to steal the individual's identity.

Many commenters and observers have asserted that the use of the SSN by the private sector should be restricted in order to prevent fraud and identity theft. Others have argued that its use is vitally important to the financial system, and that such a restriction could have a significant negative impact, including on the ability of organizations to *prevent* fraud. Commenters differed on the feasibility and costs of switching to other identifiers and authenticators, and on the availability and merits of the alternatives.

All of these issues will be addressed at the FTC's workshop on December 10 and 11, 2007. This summary and the record developed at the workshop will substantially inform the ID Theft Task Force's recommendations as to specific steps that should be taken with respect to the future collection and use of SSNs.

---

[253] Gov't Accountability Office, GAO-07-752, *Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain* 28-30 (June 2007); Comment of Consumers Union, at 3. One commenter contended that a thief with access to the last four digits "in tandem with a little information about the individual and some guesswork . . . can determine the full SSN." Comment of Consumers Union, at 3.

APPENDIX

LEGAL REQUIREMENTS FOR PRIVATE SECTOR ENTITIES TO COLLECT SOCIAL SECURITY NUMBERS[1]

Private Sector Entity	Statute and/or Agency Requirement	Requirements
FEDERAL REQUIREMENTS		
Educational institutions	IRS Form 1098-T 26 U.S.C. § 25A	Requires filers to provide student's SSN as identifier for Hope Scholarship Credit and Lifetime Learning Credit.
Educational institutions	20 U.S.C. §§ 1091(a)(4)(B), 1092	Educational institutions must collect SSNs from students who are applying for federal financial aid.
Educational institutions	20 U.S.C. § 1090(a)(7)	Requires SSNs of parents of dependent students applying for federal financial aid.
Employers	26 U.S.C. § 6051 26 C.F.R. § 31.6051-1 Internal Revenue Service, Publication 15, at 8	Employee's SSN must be collected by employer and included on employee tax documents, including W-2.
Employers	10 C.F.R. § 25.17	Requires employers licensed by the Nuclear Regulatory Commission (NRC) to provide employee information, including SSN, to NRC in order for employees or other persons to access classified information.
Financial institutions	IRS Form 5498	SSN required to report Individual Retirement Account rollovers.
Financial institutions	Bank Secrecy Act 31 C.F.R.§§ 103.19, 103.28, 103.30 FinCEN Forms 101, 102, 103, 104, 109, TD F 90-22.47	Requires financial institutions to include SSNs for Suspicious Activity Reports and Currency Transaction Reports.

[1] This Appendix contains examples of legal requirements for private sector entities to collect Social Security numbers (SSNs) and is not meant to provide a comprehensive list of all such requirements.

Private Sector Entity	Statute and/or Agency Requirement	Requirements
Financial institutions	§ 326 of USA PATRIOT Act - CIP Rules 31 U.S.C. § 5318 31 C.F.R. §§ 103.121, 103.122, 103.123, 103.131	Requires taxpayer identification number (SSN for U.S. citizens) for all new accounts.
Financial institutions	SEC Forms U-4 and U-5	SSN required on registration forms for broker-dealers, investment advisors, and issuers of securities.
Financial institutions	IRS CP2100 and CP2100A Notices; IRS B Notices	SSN required to respond to IRS notices sent to a payor when the IRS determines that the name and taxpayer identification number (SSN) on the information return (Form 1099) filed by the payor does not match the records on the IRS master file.
Financial institutions	IRS C Notice	SSN required for backup withholding of interest and dividend payments whenever the IRS notifies the payor that the payee is an identified underreporter.
Financial institutions	SEC Rule 17Ad-17 17 C.F.R. § 240.17Ad-17	Requires transfer agents to conduct searches by taxpayer identification number (SSN).
Financial Institutions	§ 314(a) of USA PATRIOT Act 31 C.F.R. § 103.100	Requires financial institutions to report information, including SSN, to law enforcement and regulatory authorities regarding individuals, entities, and organizations engaged in or reasonably suspected of engaging in terrorist acts or money laundering activities. SSNs are used by financial institutions in required scans of their accounts and transactions to determine whether account-holders appear on FinCEN list of persons suspected of engaging in these activities.
Medical device manufacturers	21 U.S.C. § 360i(e)(2)	Requires manufacturers to track certain devices implanted in the human body by collecting identifying information, which could include SSNs. Patients may refuse to release SSN.

Private Sector Entity	Statute and/or Agency Requirement	Requirements
Mutual fund companies	SEC Rule 22c-2 17 C.F.R. § 270.22c-2	Requires mutual fund companies to enter into written agreements with their distribution intermediaries, whereby the intermediaries must provide funds with certain shareholder information, including taxpayer identification numbers (SSNs).
Organ procurement organizations, transplant programs and transplant hospitals	68 Fed. Reg. 52,950, 52,952 (Sept. 8, 2003) 42 C.F.R.§ 121.11	Requires that organ procurement organizations and hospitals collect data about donors and transplant recipients for Scientific Registry of Transplant Recipients. SSN is listed data item, although collection is voluntary.
Private blood banks	42 U.S.C. § 405(c)(2)(D)(i) 20 C.F.R. § 401.200	Mandates that states may require blood donors provide their SSN.[2] The SSN may be used to identify and locate a donor whose blood donation indicates that he or she is or may be infected with the human immunodeficiency virus.
Retail and wholesale food sellers	42 U.S.C. § 405(c)(2)(C)(iii)	Requires SSNs of officers or owners of retail and wholesale food sellers that accept and redeem food stamps.
Various	26 U.S.C. § 6109 et seq.	SSN functions as individuals' taxpayer identification number.
Various	IRS Form 1098 26 U.S.C. § 6050H(d) 26 C.F.R. § 1.6050H-2(b)(2)(1)	SSN required on all Form 1098s, which advise the IRS of the amount of interest paid on a borrower's mortgage loan.
Various	IRS Form 1099 26 U.S.C. § 6049(c) 26 C.F.R. § 1.6049-4	SSN required on all 1099 Forms, which report income other than wages, salaries, and tips. For example: 1099-MISC for payments to non-employees (e.g., research subjects), if total amount paid to an individual in a calendar year exceeds $600; 1099-DIV for dividends and distributions; 1099-H for health insurance advance payments.

[2] No state law could be identified that specifically requires SSN collection by blood banks.

Private Sector Entity	Statute and/or Agency Requirement	Requirements
Various	IRS Form 8300	Requires taxpayer identification number (SSN) and must be filed when a business receives a cash payment over $10,000 as a result of a single transaction or two or more related transactions. Used by the IRS and FinCEN in their efforts to combat money laundering.
Various	42 U.S.C. § 666(a)(13)	Requires states to collect SSNs for certain licenses; requires SSN in the pertinent records of a person subject to a divorce decree, child support order, paternity determination; requires SSNs on death certificates.
Various	Federal Parent Locator Service 42 U.S.C. § 653	Mandates collection of information (including SSN) about individuals owing child support payments and creates a national database for child support enforcement purposes.
Various	42 U.S.C. § 1320b-7(a) & (b)	As condition of eligibility for Medicaid and other federal benefits, applicants/recipients must furnish SSNs to the state administering program and employers must make reports including employees' eligibility and benefits amounts to the state agency.
Various	31 U.S.C. § 7701(c)	Requires those doing business with a federal agency (i.e., lenders in a federal guaranteed loan program, applicants for federal licenses, applicants for payments through federal programs such as Medicare, contractors of an agency) to furnish taxpayer identification numbers (SSNs) to the agency.
STATE REQUIREMENTS		
Employers	State tax forms for employment (Example: Utah, Form TC-69; Michigan, Form MI-W4)	Employers required to include employee SSNs on tax documents.

Private Sector Entity	Statute and/or Agency Requirement	Requirements
Financial institutions	529 education savings plans (Example: Montana, Mont. Code Ann. § 15-62-201)	Per 26 U.S.C. § 529, 529 education savings plans are required to collect SSNs to determine beneficiary information and aggregate accounts.
Financial institutions and insurers	Escheat and unclaimed property programs (Example: Texas, Tex. Prop. Code Ann. § 74.101)	Requires SSN of property holder (e.g., securities accounts, insurance policies) to report SSNs when transferring unclaimed property to the state.
Financial institutions and insurers	State maintained lists of deadbeat parents (Example: Massachusetts, Mass. Gen. Laws ch. 175, § 24D & ch. 119A; Rhode Island, R.I. Gen. Laws § 27-57-1)	Requires collection and use of SSNs to facilitate state law requirements prohibiting financial institutions and insurers from making financial or benefit payments to payees on state-maintained deadbeat parents list. SSNs are used to identify individuals on the list.
Hospitals and health care providers	Medical forms (Example: Pennsylvania, 28 Pa. Code § 911, Pennsylvania Uniform Claims and Billing Form)	State laws establishing required elements for medical claims and billing forms, including collection of patient's SSN.
Insurers	State licensing programs (Example: Florida, Fl. Stat. § 626.171; Texas, 28 Tex. Admin. Code § 19.1903)	State laws complying with 42 U.S.C. § 666(a)(13), which requires states to have in place procedures for collecting SSNs for certain licenses, such as applicants for insurance licenses.
Insurers	Long-term care partnerships (Example: California, Cal. Code Regs. tit. 22, § 58077)	States require long-term care insurers participating in partnership plans to electronically report certain participant information, including SSNs, to state partnership program offices.
Various	Workers' compensation (Example: Virginia, Virginia Workers' Compensation Form 45-A)	States require SSNs on forms provided by the employer and/or insurance company when workers' compensation claim is filed.

Private Sector Entity	Statute and/or Agency Requirement	Requirements
Various	Eligibility for state benefits (Example: Massachusetts, Mass. Gen. Laws ch. 62E, §§ 3-5)	States require collection of SSNs by employers, insurers and financial institutions to check against list of recipients of state-run benefits programs to identify recipients receiving benefits exceeding threshold requirements.
Various	Income withholding for child support payments (Example: Wyoming, Wyo. Stat. Ann. § 20-6-206)	Income withholding orders retained by payor (employer or other person owing income to an obligor) includes various personal data, including the SSN of the obligor.