United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Commerce, Trade and Consumer Protection, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, September 28, 2004

SOCIAL SECURITY NUMBERS

Use Is Widespread and Protections Vary in Private and Public Sectors

Statement of Barbara D. Bovbjerg, Director
Education, Workforce, and Income Security Issues

Corrections made on 10/01 to revise link and e-mail address on Highlights page and job code on last page.

September 2004

SOCIAL SECURITY NUMBERS

Use is Widespread and Protections Vary in Private and Public Sectors

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-04-1099T, a testimony before the Subcommittee on Commerce, Trade and Consumer Protection, House of Representatives

Why GAO Did This Study

In 1936, the Social Security Administration (SSA) established the Social Security number (SSN) to track workers' earnings for social security benefit purposes. Today, private and public sector entities frequently ask individuals for SSNs in order to conduct their businesses and sometimes to comply with federal laws. Although uses of SSNs can be beneficial to the public, SSNs are also a key piece of information in creating false identities either for financial misuse or for assuming an individual's identity. The retention of SSNs in the public and private sectors can create opportunities for identity theft. In addition, the aggregation of personal information, such as SSNs, in large corporate databases, as well as the public display of SSNs in various records accessed by the public, may provide criminals the opportunity to easily obtain this personal information. Given the heightened awareness of identity crimes, this testimony focuses on describing (1) how private sector entities obtain, use, and protect SSNs, and (2) public sector uses and protections of SSNs.

www.gao.gov/cgi-bin/getrpt?GAO-04-1099T.

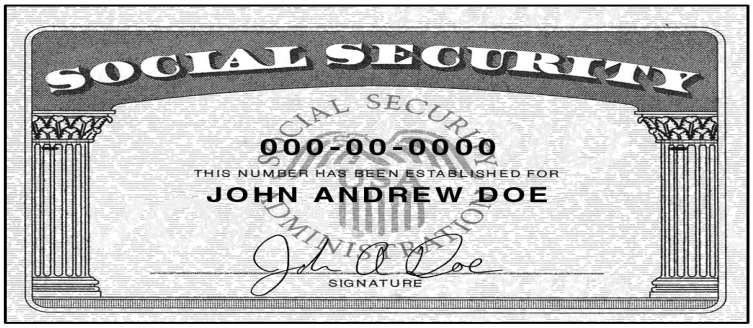
To view the full product, including the scope and methodology, click on the link above. For more information, contact Barbara Bovbjerg at (202) 512-7215 or bovbjergb@gao.gov.

What GAO Found

Private sector entities rely extensively on SSNs. We reported early this year that entities such as information resellers, consumer reporting agencies , and health care organizations routinely obtain SSNs from their business clients and public sources, such as government records that can be displayed to the public. These entities then use SSNs for various purposes, such as to verify an individual's identity or to match existing records, and have come to rely on the SSN as an identifier, which helps them determine a person's identity for the purpose of providing the services they offer. There is no single federal law that regulates the overall use or restricts the disclosure of SSNs by private sector entities. However, certain federal laws have helped to place restrictions on the disclosures of personal information private sector entities are allowed to make to their customers, and certain states have enacted laws to restrict the private sector's use of SSNs.

Public sector entities also extensively use SSNs. All three levels of government use the SSN to comply with certain federal laws and regulations, as well as for their own purposes. These agencies rely on the SSN to manage records, verify benefit eligibility, collect outstanding debt, and conduct research and program evaluations. In addition, given the open nature of certain government records, SSNs appear in records displayed to the public such as documents that record financial transactions or court documents. Despite the widespread reliance on and use of SSNs, government agencies are taking steps to safeguard the SSN. For example, some agencies are not using the SSN as the primary identification number. In a previous report, we proposed that Congress consider developing a unified approach to safeguarding SSNs used in all levels of government and particularly those displayed in public records, and we continue to believe that this approach has merit.

The use of SSNs by both private and public sector entities is likely to continue, but the more frequently SSNs are used, the more likely they are to be misused given the continued rise in identity crimes. In considering restrictions to SSN use, policy makers will have to balance the protections that could occur from such restrictions with legitimate business needs for the use of SSNs.



Source: GAO, Social Security Administration.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss private and public sector entities' use of Social Security numbers (SSNs). Although the Social Security Administration (SSA) originally created SSNs as a means to track workers' earnings and eligibility for Social Security benefits, over time the SSN has come to be used for a myriad of purposes; individuals are frequently asked to supply personal information, including their SSNs, to both public and private sector entities. In addition, individuals' SSNs can be found in a number of public sources such as records displayed to the public. Given the uniqueness and broad applicability of the SSN, many private and public sector entities rely extensively on the SSN sometimes as a way to accumulate and identify information for their databases, sometimes to comply with federal regulations, and other times for various business purposes. The potential for misuse of the SSN has raised questions about how private and public sector entities obtain, use, and protect SSNs.

Although Congress has passed a number of laws to protect the security of personal information, the continued use of and reliance on SSNs by both private and public sector entities underscores the importance of determining if appropriate safeguards are in place to protect individuals' private information or if enhanced protection of individuals' personal information is needed. Accordingly, you asked us to talk about how certain types of private and public sector entities obtain SSNs and what protections, if any, exist to govern their use. My remarks today will focus on describing (1) how private sector entities obtain, use, and protect SSNs and (2) public sector uses and protections.

To determine how private sector entities obtain, use, and protect SSNs, we relied on our previous work that looked at how private sector entities obtain and use SSNs and the laws that limit disclosure of this use.[1] To determine how the public sector uses and protects SSNs, we also relied on our previous work that looked at the government's use and protection of SSNs.[2] In addition, we are conducting structured interviews of federal agencies concerning the display of SSNs.

[1]GAO, *Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information*, GAO-04-11 (Washington D.C.: January 22, 2004).

[2]See GAO, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352 (Washington, D.C.: May 31, 2002).

In summary, entities such as information resellers, consumer reporting agencies (CRAs), and health care organizations routinely obtain SSNs from their business clients and from public sources, such as marriage licenses, paternity determinations, and professional licenses. Businesses use SSNs for various purposes, such as to build databases, verify individuals' identities, or match existing records.[3] Given the various types of services these companies offer, we found that all of these entities have come to rely on the SSN as an identifier, which they say helps them determine a person's identity for the purpose of providing the services they offer. However, certain federal laws have helped to limit the disclosures of personal information these private sector entities are allowed to make to their customers. Private sector entities are either subject to the laws directly, given the nature of their business, or indirectly, through their business clients who are subject to these laws. Some states have also enacted laws to restrict the private sector's use of SSNs. However, such restrictions vary by state.

Public sector entities also rely extensively on SSNs. These agencies often obtain SSNs for compliance with federal laws and regulations and for their own agencies' purposes. We found that federal, state, and county government agencies rely extensively on the SSN to manage records, verify benefit eligibility, collect outstanding debt, conduct research and program evaluations, and verify information provided to state drivers' licensing agencies.[4] Given that SSNs are often the identifier of choice among individuals seeking to create false identities, these agencies are taking steps to safeguard SSNs. Yet despite these actions, SSNs appear in records displayed to the public such as documents that record financial transactions or court documents. In a previous report, we proposed that Congress consider developing a unified approach to safeguarding SSNs used in all levels of government and particularly those displayed in public records, and we continue to believe that this approach has merit.[5]

Background

The Social Security Act of 1935 authorized SSA to establish a record-keeping system to help manage the Social Security program, and this

[3]GAO-04-11 (Washington D.C.: January 2004).

[4]GAO-02-352 (Washington D.C.: May 2002).

[5]GAO-02-352 (Washington D.C.: May 2002).

resulted in the creation of the SSN. Through a process known as enumeration, unique numbers are created for every person as a work and retirement benefit record for the Social Security program. SSA generally issues SSNs to most U.S. citizens, and SSNs are also available to noncitizens lawfully admitted to the United States with permission to work. SSA estimates that approximately 277 million individuals currently have SSNs. The SSN has become the identifier of choice for government agencies and private businesses, and thus it is used for a myriad of non-Social Security purposes.

The growth in the use of SSNs is important to individual SSN holders because these numbers, along with names and birth certificates, are among the three personal identifiers most often sought by identity thieves.[6] In addition, SSNs are used as breeder information to create additional false identification documents, such as drivers' licenses. Recent statistics collected by federal agencies and CRAs indicate that the incidence of identity theft appears to be growing.[7] The Federal Trade Commission (FTC), the agency responsible for tracking identity theft, reported that consumer fraud and identity theft complaints grew from 404,000 in 2002 to 516,740 in 2003. In 2003, consumers also reported losses from fraud of more than $437 million, up from $343 million in 2002. In addition, identity crimes account for over 80 percent of SSN misuse allegations according to the SSA. Also, officials from two of the three national CRAs report an increase in the number of 7-year fraud alerts placed on consumer credit files, which they consider to be reliable indicators of the incidence of identity theft.[8] Law enforcement entities report that identity theft is almost always a component of other crimes, such as bank fraud or credit card fraud, and may be prosecuted under the statutes covering those crimes.

[6]United States Sentencing Commission, *Identity Theft Final Alert (*Washington, D.C.: Dec. 15, 1999).

[7]GAO, *Identity Theft: Prevalence and Cost Appear to be Growing*, GAO-02-363 (Washington, D.C.: Mar. 1, 2002).

[8]A fraud alert is a warning that someone may be using the consumer's personal information to fraudulently obtain credit. When a fraud alert is placed on a consumer's credit card file, it advises credit grantors to conduct additional identity verification before granting credit. The three consumer reporting agencies offers fraud alerts that can vary from 2 to 7 years at the discretion of the individual.

Private Sector Entities Routinely Obtain and Use SSNs, and Certain Laws Affect The Disclosure of This Information

Private sector entities such as information resellers, CRAs, and health care organizations routinely obtain and use SSNs.[9] Such entities obtain the SSNs from various public sources and their business clients wishing to use their services. We found that these entities usually use SSNs for various purposes, such as to build tools that verify an individual's identity or match existing records. Certain federal laws have limited the disclosures private sector entities are allowed to make to their customers, and some states have also enacted laws to restrict the private sector's use of SSNs.

Private Sector Entities Obtain SSNs from Public and Private Sources and Use SSNs for Various Purposes

Private sector entities such as information resellers, CRAs, and health care organizations generally obtain SSNs from various public and private sources and use SSNs to help identify individuals. Of the various public sources available, large information resellers told us they obtain SSNs from various records displayed to the public such as records of bankruptcies, tax liens, civil judgments, criminal histories, deaths, real estate ownership, driving histories, voter registrations, and professional licenses. Large information resellers said that they try to obtain SSNs from public sources where possible, and to the extent public record information is provided on the Internet, they are likely to obtain it from such sources. Some of these officials also told us that they have people that go to courthouses or other repositories to obtain hard copies of public records. Additionally, they obtain batch files of electronic copies of all public records from some jurisdictions.

Given the varied nature of SSN data found in public records, some reseller officials said they are more likely to rely on receiving SSNs from their business clients than they are from obtaining SSNs from public records. These entities obtain SSNs from their business clients, who provide SSNs in order to obtain a reseller's services or products, such as background checks, employee screening, determining criminal histories, or searching for individuals. Large information resellers also obtain SSN information from private sources. In many cases such information was obtained

[9]Information resellers, sometimes referred to as information brokers, are businesses that specialize in amassing consumer information that includes SSNs for informational services. CRAs, also known as credit bureaus, are agencies that collect and sell information about the creditworthiness of individuals. Health care organizations generally deliver their services through a coordinated system that includes health care providers and health plans, also referred to as health care insurers.

through review of data where a customer has voluntarily supplied information resellers with information about himself or herself. In addition, large reseller officials said they also use their clients' records in instances where the client has provided them with information.

We also found that Internet-based resellers rely extensively on public sources and records displayed to the public. These resellers listed on their Web sites public information sources, such as newspapers, and various kinds of public record sources at the county, state, and national levels. During our investigation, we determined that once Internet-based resellers obtained an individual's SSN they relied on information in public records to help verify the individual's identity and amass information around the individual's SSN.

Like information resellers, CRAs also obtain SSNs from public and private sources as well as from their customers or the businesses that furnish data to them. CRA officials said that they obtain SSNs from public sources, such as bankruptcy records, a fact that is especially important in terms of determining that the correct individual has declared bankruptcy. CRA officials also told us that they obtain SSNs from other information resellers, especially those that specialize in obtaining information from public records. However, SSNs are more likely to be obtained from businesses that subscribe to their services, such as banks, insurance companies, mortgage companies, debt collection agencies, child support enforcement agencies, credit grantors, and employment screening companies. Individuals provide these businesses with their SSNs for reasons such as applying for credit, and these businesses voluntarily report consumers' charge and payment transactions, accompanied by SSNs, to CRAs.

We found that health care organizations were less likely to rely on public sources for SSN data. Health care organizations obtain SSNs from individuals themselves and from companies that offer health care plans. For example, subscribers or policyholders provide health care plans with their SSNs through their company or employer group when they enroll in health care plans. In addition to health care plans, health care organizations include health care providers, such as hospitals. Such entities often collect SSNs as part of the process of obtaining information on insured people. However, health care officials said that, particularly with hospitals, the medical record number rather than the SSN is the primary identifier.

Information resellers, CRAs, and health care organization officials all said that they use SSNs to verify an individual's identity. Most of the officials we spoke to said that the SSN is the single most important identifier available, mainly because it is truly unique to an individual, unlike an individual's name and address, which can often change over an individual's lifetime. Large information resellers said that they generally use the SSN as an identity verification tool. Some of these entities have incorporated SSNs into their information technology, while others have incorporated SSNs into their clients' databases used for identity verification. For example, one large information reseller that specializes in information technology solutions has developed a customer verification data model that aids financial institutions in their compliance with some federal laws regarding "knowing your customer." We also found that Internet-based information resellers use the SSN as a factor in determining an individual's identity. We found these types of resellers to be more dependent on SSNs than the large information resellers, primarily because their focus is more related to providing investigative or background-type services to anyone willing to pay a fee. Most of the large information resellers officials we spoke to said that although they obtain the SSN from their business clients, the information they provide back to their customers rarely contains the SSN. Almost all of the officials we spoke to said that they provide their clients with a truncated SSN, an example of which would be xxx-xx-6789.

CRAs use SSNs as the primary identifier of individuals, which enables them to match the information they receive from their business clients with the information stored in their databases on individuals.[10] Because these companies have various commercial, financial, and government agencies furnishing data to them, the SSN is the primary factor that ensures that incoming data is matched correctly with an individual's information on file. For example, CRA officials said they use several factors to match incoming data with existing data, such as name, address, and financial account information. If all of the incoming data, except the SSN, match with existing data, then the SSN will determine the correct person's credit file. Given that people move, get married, and open new financial accounts, these officials said that it is hard to distinguish among

[10]We found that CRAs and information resellers can sometimes be the same entity, a fact that blurs the distinction between the two types of businesses but does not affect the use of SSNs by these entities. Five of the six large information resellers we spoke to said they were also CRAs. Some CRA officials said that information reselling constituted as much as 40 percent of CRAs' business.

individuals. Because the SSN is the one piece of information that remains constant, they said that it is the primary identifier that they use to match data.

Health care organizations also use the SSN to help verify the identity of individuals. These organizations use SSNs, along with other information, such as name, address, and date of birth, as a factor in determining a member's identity. Health care officials said that health care plans, in particular, use the SSN as the primary identifier of an individual, and it often becomes the customer's insurance number. Health care officials said that they use SSNs for identification purposes, such as linking an individual's name to an SSN to determine if premium payments have been made. They also use the SSN as an online services identifier, as an alternative policy identifier, and for phone-in identity verification. Health care organizations also use SSNs to tie family members together where family coverage is used,[11] to coordinate member benefits, and as a cross-check for pharmacy transactions. Health care industry association officials also said that SSNs are used for claims processing, especially with regard to Medicare. According to these officials, under some Medicare programs, SSNs are how Medicare identifies benefits provided to an individual.

Certain Laws Limit the Private Sectors' Disclosure of Personal Information That Includes SSNs

Certain federal and state laws have placed restrictions on certain private sector entities use and disclosure of consumers' personal information that includes SSNs. Such laws include the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the Drivers Privacy Protection Act (DPPA), and the Health Insurance Portability and Accountability Act (HIPAA). As shown in table 1, the laws either restrict the disclosures that entities such as information resellers, CRAs, and health care organizations are allowed to make to specific purposes or restrict whom they are allowed to give the information to. Moreover, as shown in table 1, these laws focus on limiting or restricting access to certain personal information and are not specifically focused on information resellers. See appendix I for more information on these laws.

[11]During the enrollment process, subscribers have a number of options, one of which is decided whether they would like single or family coverage. In cases where family coverage is chosen, the SSN is the key piece of information generally allowing the family members to be linked.

Table 1: Aspects of Federal Laws That Affect Private Sector Disclosure of Personal Information

Federal Laws	Restrictions
Fair Credit Reporting Act	Limits access to credit data that includes SSNs to those who have a permissible purpose under the law.
Gramm-Leach-Bliley Act	Creates a new definition of personal information that includes SSNs and limits when financial institutions may disclose the information to non-affiliated third parties.
Drivers Privacy Protection Act	Prohibits obtaining and disclosing SSNs and other personal information from a motor vehicle record except as expressly permitted under the law.
Health Insurance Portability and Accountability Act	Protects the privacy of health information that identifies an individual (including by SSNs) and restricts health care organizations from disclosing such information to others without the patient's consent.

Source: GAO analysis.

We reviewed selected legislative documents of 18 states and found that at least 6 states have enacted their own legislation to restrict either the display or use of SSNs by the private sector.[12] Notably, in 2001, California enacted Senate Bill (SB) 168, restricting private sector use of SSNs. Specifically, this law generally prohibits companies and persons from certain uses such as, posting or publicly displaying SSNs and printing SSNs on cards required to access the company's products or services. Furthermore, in 2002, shortly after the enactment of SB 168, California's Office of Privacy Protection published recommended practices for protecting the confidentiality of SSNs. These practices were to serve as guidelines to assist private and public sector organizations in handling SSNs.

Similar to California's law, Missouri's law (2003 Mo. SB 61), which is not effective until July 1, 2006, bars companies from requiring individuals to

[12]On the basis of our interviews with private sector businesses and organizations, contacts with some state offices of attorney general, and identification of state laws and legislative initiatives related to the use of SSNs, we did a legislative review of 18 states that were identified as having laws or proposed laws governing SSN use. In the 18 states we researched, we reviewed more than 40 legislative documents, including relevant laws, proposed laws, legislative summaries, and other related documents, such as state regulations, executive orders, and referendums.

transmit SSNs over the Internet without certain safety measures, such as encryption and passwords. However, while SB 61 prohibits a person or private entity from publicly posting or displaying an individual's SSN "in any manner," unlike California's law, it does not specifically prohibit printing the SSN on cards required to gain access to products or services. In addition, Arizona's law (2003 Ariz. Sess. Laws 137), effective January 1, 2005, restricts the use of SSNs in ways very similar to California's law. However, in addition to the private sector restrictions, it adds certain restrictions for state agencies and political subdivisions.[13] For example, state agencies and political subdivisions are prohibited from printing an individual's SSN on cards and certain mailings to the individual. Last, Texas prohibits the display of SSNs on all cards, while Georgia and Utah's laws are directed at health insurers and, therefore, pertain primarily to insurance identification cards.[14] None of these three laws contain the provisions mentioned above relating to Internet safety measures and mailing restrictions. Table 2 lists states that have enacted legislation and related provisions.

Table 2: Provisions Included in Enacted Legislation Reviewed

Provision	States Where Provision or Restriction Enacted
Specifically prohibits display on cards	AZ, CA, GA, TX, UT
Requires Internet safety measures	AZ, CA, MO
Restricts mailing of SSNs	AZ, CA

Source: GAO analysis.

Public Sector Entities Also Use SSNs and Some Agencies Limit Their Use and Display

Agencies at all levels of government frequently obtain and use SSNs. A number of federal laws require government agencies to obtain SSNs, and these agencies use SSNs to administer their programs, verify applicants' eligibility for services and benefits, and do research and evaluation. In addition, given the open nature of certain government records, SSNs appear in some records displayed to the public. Given the potential for misuse, some government agencies are taking steps to limit their use and display of SSNs and prevent the proliferation of false identities.

[13]Political subdivisions would include counties, cities, and towns.

[14]Georgia's law (O.C.G.A. §33-24-57.1(f)) and Utah's law (Utah Code Ann. §31-22-634) were both effective July 1, 2004. However, Utah's law provides certain extensions until March 1, 2005. Texas' law (2003 Tex. Gen. Laws 341) is effective March 1, 2005.

Public Sector Entities Are Required by Laws and Regulations to Obtain SSNs and Use SSNs for Various Purposes

Government agencies obtain SSNs because a number of federal laws and regulations require certain programs and federally funded activities to use the SSN for administrative purposes.[15] Such laws and regulations require the use of the SSN as an individual's identifier to facilitate automated exchanges that help administrators enforce compliance with federal laws, determine eligibility for benefits, or both. For example, the Internal Revenue Code and regulations, which govern the administration of the federal personal income tax program, require that individuals' SSNs serve as taxpayer identification numbers.[16] A number of other federal laws require program administrators to use SSNs in determining applicants' eligibility for federally funded benefits. The Social Security Act requires individuals to provide their SSNs in order to receive benefits under the SSI, Food Stamp, Temporary Assistance for Needy Families, and Medicaid programs.[17] In addition, the Commercial Motor Vehicle Safety Act of 1986 requires the use of SSNs to identify individuals and established the Commercial Driver's License Information System, a nationwide database where states may use individuals' SSNs to search the database for other state-issued licenses commercial drivers may hold.[18] Federal law also requires the use of SSNs in state child support programs to help states locate noncustodial parents, establish and enforce support orders, and recoup state welfare payments from parents.[19] The law also requires states to record SSNs on many other state documents, such as professional,

[15]GAO, *Social Security Numbers: Government and Commercial Use of the Social Security Number is Widespread*, GAO/HEHS-99-28 (Washington D.C.: February 1999).

[16]This means that employers and others making payments to individuals must include the individuals' SSNs in reporting to IRS many of these payments. In addition, the Code and regulations require individuals filing personal income tax returns to include their SSNs as their taxpayer identification number, the SSNs of people whom they claim as dependents, and the SSNs of spouses to whom they paid alimony.

[17]Applicants give program administrators information on their income and resources, and program administrators use applicants' SSNs to match records with those of other organizations.

[18]States may also use SSNs to search another database, the National Driver's Registry, to determine whether an applicant's license has been cancelled, suspended, or revoked by another state. In these situations, the states use SSNs to limit the possibility of inappropriately licensing applicants.

[19]The law requires states to maintain records that include (1) SSNs for individuals who owe or are owed support for cases in which the state has ordered child support payments to be made, the state is providing support, or both, and (2) employers' records of new hires identified by SSN.

occupational, and marriage licenses; divorce decrees; paternity determinations; and death certificates.

Government agencies use SSNs for a variety of reasons. We found that most of these agencies use SSNs to administer their programs, such as to identify, retrieve, and update their records. In addition, many agencies also use SSNs to share information with other entities to bolster the integrity of the programs they administer. As unique identifiers, SSNs help ensure that the agency is obtaining or matching information on the correct person.

Government agencies also share information containing SSNs for the purpose of verifying an applicant's eligibility for services or benefits, such as matching records with state and local correctional facilities to identify individuals for whom the agency should terminate benefit payments. SSNs are also used to ensure program integrity. Agencies use SSNs to collect delinquent debts and even share information for this purpose. In addition, SSNs are used for statistics, research, and evaluation. Agencies responsible for collecting and maintaining data for statistical programs that are required by statute, make use of SSNs. In some cases, these data are compiled using information provided for another purpose. For example, the Bureau of the Census prepares annual population estimates for states and counties using individual income tax return data linked over time by SSN to determine immigration rates between localities.[20] SSNs also provide government agencies and others with an effective mechanism for linking data on program participation with data from other sources to help evaluate the outcomes or effectiveness of government programs. In some cases, records containing SSNs are sometimes matched across multiple agency or program databases.[21]

Government agencies also use employees' SSNs to fulfill some of their responsibilities as employers. For example, personnel departments of these agencies use SSNs to help them maintain internal records and provide employee benefits. In addition, employers are required by law to use employees' SSNs when reporting wages. Wages are reported to SSA,

[20]The Bureau of the Census is authorized by statute to collect a variety of information, and the Bureau is also prohibited from making it available, except in certain circumstances.

[21]The statistical and research communities refer to the process of matching records containing SSNs for statistical or research purposes as "record linkage." See U.S. General Accounting Office, *Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information*, GAO-01-126SP (Washington, D.C.: Apr. 2001).

and the agency uses this information to update earnings records it maintains for each individual. The Internal Revenue Service (IRS) also uses SSNs to match the employer wage reports with amounts individuals report on personal income tax returns. Federal law also requires that states maintain employers' reports of newly hired employees, identified by SSNs. States must forward this information to a national database that is used by state child support agencies to locate parents who are delinquent in child support payments.

Finally, SSNs appear in some government records that are open to the public. For example, SSNs may already be a part of a document that is submitted to a recorder for official preservation, such as veterans' discharge papers. Documents that record financial transactions, such as tax liens and property settlements, also contain SSNs to help identify the correct individual. Government officials are also required by law to collect SSNs in numerous instances, and some state laws allow government entities to collect SSNs on voter registries to help avoid duplicate registrations. In addition, courts at all three levels of government also collect and maintain records that are routinely made available to the public. SSNs appear in court documents for a variety of reasons such as on documents that government officials create like criminal summonses, and in many cases, SSNs are already a part of documents that are submitted by attorneys or individuals as part of the evidence for a proceeding or a petition for an action. In some cases, federal law requires that SSNs be placed in certain records that courts maintain, such as child support orders.

Government Agencies Are Taking Steps to Limit the Use and Display of SSNs

Despite the widespread use of SSNs at all levels of government, not all agencies use SSNs. We found that some agencies do not obtain, receive, or use SSNs of program participants, service recipients, or individual members of the public.[22] Moreover, not all agencies use the SSN as their primary identification number for record-keeping purposes. These agencies maintain an alternative number that is used in addition to or in lieu of SSNs for certain activities.

Some agencies are also taking steps to limit SSNs displayed on documents that may be viewed by others who may not have a need to view this personal information. For example, the Social Security Administration has truncated individuals' SSNs that appear on the approximately 120 million

[22] GAO-02-352 (Washington D.C.: May 2002).

benefits statements it mails each year. Some states have also passed laws prohibiting the use of SSNs as a student identification number. Almost all states have modified their policies on placing SSNs on state drivers' licenses.

At the federal level, SSA has taken steps in its enumeration process and verification service to help prevent SSNs from being used to proliferate false identities. SSA has formed a task force to address weaknesses in its enumeration process and has (1) increased document verifications and developed new initiatives to prevent the inappropriate assignment of SSNs to noncitizens, and (2) undertaken initiatives to shift the burden of processing noncitizen applications from its field offices.[23] SSA also helps prevent the proliferation of false identities through its verification service, which allows state driver licensing agencies to verify the SSN, name, and date of birth of customers with SSA's master file of Social Security records.[24] Finally, SSA has also acted to correct deficiencies in its information systems' internal controls. These changes were made in response to the findings of an independent audit that found that SSA's systems were exposed to both internal and external intrusion, increasing the possibility that sensitive information such as SSNs could be subject to unauthorized access, modification, and disclosure, as well as the risk of fraud.

With regard to the courts, in a prior report we suggested that Congress consider addressing SSN security and display issues in state and local government and in public records, including those maintained by the judicial branch of government at all levels.[25] We proposed that Congress convene a representative group of officials from all levels of government to develop a unified approach to safeguard SSNs used in all levels of government and particularly those displayed in public records.

[23]See GAO, *Social Security Administration: Actions Taken to Strengthen Procedures for Issuing Social Security Numbers to Noncitizens but Some Weakness Remain*, GAO-04-12 (Washington D.C.: October 15, 2003). See GAO, *Social Security Numbers: Improved SSN Verification and Exchange of States' Driver Records Would Enhance Identity Verification*, GAO-03-920 (Washington D.C.: September 15, 2003).

[24]GAO-03-920 (Washington D.C.: September 2003).

[25]GAO-02-352 (Washington D.C.: May 2002)

Conclusions

Public and private entities use SSNs for many legitimate and publicly beneficial purposes. However, the more frequently SSNs are obtained and used, the more likely they are to be misused. Individuals may voluntarily provide their SSNs to the private and public sectors to obtain services, but they should be able to be confident that their personal information is safe and secure. As we continue to learn more about the entities that obtain SSNs and the purposes for which they obtain them, policy makers will be able to determine if there are ways to limit access to this valuable piece of information and prevent it from being misused. However, restrictions on access or use may make it more difficult for businesses and government agencies to verify an individual's identity. Accordingly, policy makers will have to balance the potential benefits of restrictions on the use of SSNs on the one hand with the impact on legitimate needs for the use of SSNs on the other.

We are continuing our work on protecting the privacy of SSNs in the private and public sectors, and we are pleased that this Subcommittee is considering this important policy issue. That concludes my testimony, and I would be pleased to respond to any questions the subcommittee has.

Contacts and Acknowledgments

For further information regarding this testimony, please contact Barbara D. Bovbjerg, Director or Tamara Cross, Assistant Director at (202) 512-7215.

Appendix I: Federal Laws Affecting Information Resellers, CRAs, and Health Care Organizations:

Gramm-Leach-Bliley Act (GLBA):

GLBA requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some, but not all, sharing of their nonpublic personal information. Financial institutions are permitted to disclose consumers' nonpublic personal information without offering them an opt-out right in the following circumstances:

- to effect a transaction requested by the consumer in connection with a financial product or service requested by the consumer; maintaining or servicing the consumer's account with the financial institution or another entity as part of a private label credit card program or other extension of credit; or a proposed or actual securitization, secondary market sale, or similar transaction;
- with the consent or at the direction of the consumer;
- to protect the confidentiality or security of the consumer's records; to prevent actual or potential fraud, for required institutional risk control or for resolving customer disputes or inquiries, to persons holding a legal or beneficial interest relating to the consumer, or to the consumer's fiduciary;
- to provide information to insurance rate advisory organizations, guaranty funds or agencies, rating agencies, industry standards agencies, and the institution's attorneys, accountants, and auditors;
- to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies, self-regulatory organizations, or for an investigation on a matter related to public safety;
- to a consumer reporting agency in accordance with the Fair Credit Reporting Act or from a consumer report reported by a consumer reporting agency;
- in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business if the disclosure concerns solely consumers of such business;
- to comply with federal, state, or local laws; an investigation or subpoena; or to respond to judicial process or government regulatory authorities.

Financial institutions are required by GLBA to disclose to consumers at the initiation of a customer relationship, and annually thereafter, their

privacy policies, including their policies with respect to sharing information with affiliates and non-affiliated third parties.

Provisions under GLBA place limitations on financial institutions disclosure of customer data, thus affecting some CRAs and information resellers. We found that some CRAs consider themselves to be financial institutions under GLBA.[1] These entities are therefore directly governed by GLBA's restrictions on disclosing nonpublic personal information to non-affiliated third parties. We also found that some of the information resellers we spoke to did not consider their companies to be financial institutions under GLBA. However, because they have financial institutions as their business clients, they complied with GLBA's provisions in order to better serve their clients and ensure that their clients are in accordance with GLBA. For example, if information resellers received information from financial institutions, they could resell the information only to the extent that they were consistent with the privacy policy of the originating financial institution.

Information resellers and CRAs also said that they protect the use of non-public personal information and do not provide such information to individuals or unauthorized third parties. In addition to imposing obligations with respect to the disclosures of personal information, GLBA also requires federal agencies responsible for financial institutions to adopt appropriate standards for financial institutions relating to safeguarding customer records and information. Information resellers and CRA officials said that they adhere to GLBA's standards in order to secure financial institutions' information.

Drivers Privacy Protection Act (DPPA):

The DPPA specifies a list of exceptions when personal information contained in a state motor vehicle record may be obtained and used (18 U.S.C. § 2721(b)). These permissible uses include:

- for use by any government agency in carrying out its functions;
- for use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls,

[1]Under GLBA, the term financial institution is defined as "any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956," which goes into more detail about what are "activities that are financial in nature." These generally include banking, insurance, and investment industries.

or advisories; motor vehicle market research activities, including survey research;

- for use in the normal course of business by a legitimate business, but only to verify the accuracy of personal information submitted by the individual to the business and, if such information is not correct, to obtain the correct information but only for purposes of preventing fraud by pursuing legal remedies against, or recovering on a debt or security interest against, the individual;

- for use in connection with any civil, criminal, administrative, or arbitral proceeding in any federal, state, or local court or agency;

- for use in research activities;

- for use by any insurer or insurance support organization in connection with claims investigation activities;

- for use in providing notice to the owners of towed or impounded vehicles;

- for use by a private investigative agency for any purpose permitted under the DPPA;

- for use by an employer or its agent or insurer to obtain information relating to the holder of a commercial driver's license;

- for use in connection with the operation of private toll transportation facilities;

- for any other use, if the state has obtained the express consent of the person to whom a request for personal information pertains;

- for bulk distribution of surveys, marketing, or solicitations, if the state has obtained the express consent of the person to whom such personal information pertains;

- for use by any requester, if the requester demonstrates that it has obtained the written consent of the individual to whom the information pertains;

- for any other use specifically authorized under a state law, if such use is related to the operation of a motor vehicle or public safety.

As a result of DPPA, information resellers said they were restricted in their ability to obtain SSNs and other driver license information from state

motor vehicle offices unless they were doing so for a permissible purpose under the law. These officials also said that information obtained from a consumer's motor vehicle record has to be in compliance with DPPA's permissible purposes, thereby restricting their ability to resell motor vehicle information to individuals or entities not allowed to receive such information under the law. Furthermore, because DPPA restricts state motor vehicle offices' ability to disclose driver license information, which includes SSN data, information resellers said they no longer try to obtain SSNs from state motor vehicle offices, except for permissible purposes.

Health Insurance Portability and Accountability Act (HIPAA):

The HIPAA privacy rule also defines some rights and obligations for both covered entities and individual patients and health plan members. Some of the highlights are:

- Individuals must give specific authorization before health care providers can use or disclose protected information in most nonroutine circumstances, such as releasing information to an employer or for use in marketing activities.

- Covered entities will need to provide individuals with written notice of their privacy practices and patients' privacy rights. The notice will contain information that could be useful to individuals choosing a health plan, doctor, or other service provided. Patients will be generally asked to sign or otherwise acknowledge receipt of the privacy notice.

  Covered entities must obtain an individual's specific authorization before sending them marketing materials.

  Health care organizations, including health care providers and health plan insurers, are subject to HIPAA's requirements. In addition to providing individuals with privacy practices and notices, health care organizations are also restricted from disclosing a patient's health information without the patient's consent, except for purposes of treatment, payment, or other health care operations. Information resellers and CRAs did not consider themselves to be "covered entities" under HIPAA, although some information resellers said that their customers are considered to be business associates under HIPAA. As a result, they said they are obligated to operate under HIPAA's standards for privacy protection, and therefore could not resell medical information without having made sure HIPAA's privacy standards were met.

Fair Credit Reporting Act (FCRA):

Congress has limited the use of consumer reports to protect consumers' privacy. All users must have a permissible purpose under the FCRA to obtain a consumer report (15 USC 1681b). These permissible purposes are:

- as ordered by a court or a federal grand jury subpoena;
- as instructed by the consumer in writing;
- for the extension of credit as a result of an application from a consumer or the review or collection of a consumer's account;
- for employment purposes, including hiring and promotion decisions, where the consumer has given written permission;
- for the underwriting of insurance as a result of an application from a consumer;
- when there is a legitimate business need, in connection with a business transaction that is initiated by the consumer;
- to review a consumer's account to determine whether the consumer continues to meet the terms of the account;
- to determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status;
- for use by a potential investor or servicer or current insurer in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation; and
- for use by state and local officials in connection with the determination of child support payments, or modifications and enforcement thereof.

Under FCRA, Congress has limited the use of consumer reports[2] to protect consumers' privacy and limits access to credit data to those who have a legally permissible purpose for using the data, such as the extension of credit, employment purposes, or underwriting insurance. However, these

[2]The FTC has determined that certain types of information, including SSNs, do not constitute as consumer report under FCRA because they are not factors in determining credit eligibility.

limits are not specific to SSNs. All of the CRAs that we spoke to said that they are considered consumer reporting agencies under FCRA. In addition, some of the information resellers we spoke to who handle or maintain consumer reports are classified as CRAs under FCRA. Both CRAs and information resellers said that as a result of FCRAs restrictions they are limited to providing credit data to their customers that have a permissible purpose under FCRA. Consequently, they are restricted by law from providing such information to the general public.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov(202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548