

GAO

Report to the Chairman, Subcommittee
on Social Security, Committee on Ways
and Means, House of Representatives

January 2004

SOCIAL SECURITY NUMBERS

Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information





Highlights of [GAO-04-11](#), a report to Subcommittee on Social Security, Committee on Ways and Means, 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. However, the SSN is also used for a myriad of non-Social Security purposes. Today, public and private sector entities view the SSN as a key piece of information that enables them to conduct their business and deliver services. However, given the apparent rise in identity crimes as well as the rapidly increasing availability of information over the Internet, Congress has raised concern over how certain private sector entities obtain, use, and safeguard SSN data. In previous reports, we discussed the benefits of government and commercial entities using SSNs. We also examined how certain private sector entities and the government obtain, use, and safeguard SSNs. This report provides additional information on private sector uses of SSNs.

You asked that GAO examine the private sector use of SSNs by businesses most likely to obtain and use them including information resellers, consumer reporting agencies (CRAs), and health care organizations. Specifically, our objectives were to (1) describe how information resellers, CRAs, and some health care organizations obtain and use SSNs and (2) discuss the laws and practices relevant to safeguarding SSNs and consumers' privacy. GAO makes no recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-04-11.

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

SOCIAL SECURITY NUMBERS

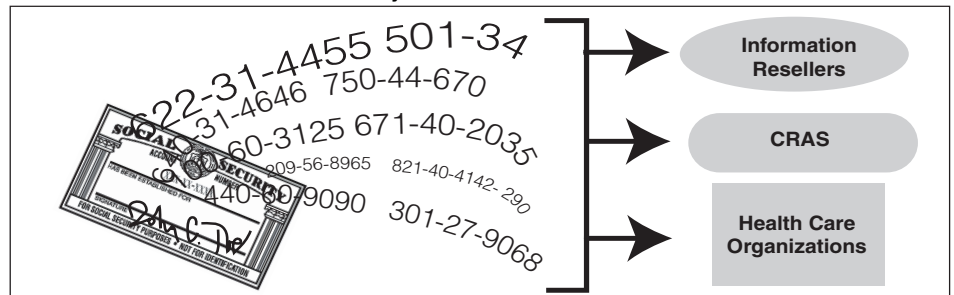
Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information

What GAO Found

Information resellers, consumer reporting agencies, and some health care organizations routinely obtain SSNs from their customers and have come to rely on SSNs as identifiers that help them determine an individual's identity and accumulate information about individuals. Larger information resellers usually obtain SSNs from their customers and use them to determine the identity of an individual for purposes such as employment screening, credit information, and criminal history. Other Internet-based information resellers whose Web sites we accessed also obtain SSNs from their customers and scour public records and other publicly available information to provide the information to persons willing to pay a fee. CRAs, too, are large users of SSNs. They obtain SSNs from businesses that furnish individuals' data to them and use SSNs to determine consumers' identities and match the information they receive from businesses with information stored in consumers' credit files. Finally, health care organizations obtain SSNs from individuals themselves and companies that offer health care plans and use them as identifiers. Some health care organizations use SSNs as member identification numbers.

Certain federal laws help to safeguard consumers' personal information, including SSNs, by restricting the disclosure of and access to such information, and private sector officials we spoke with said that they indeed take steps to safeguard the SSN information they collect. Information resellers, CRAs, and health care organizations told us they take steps to safeguard SSN data in part for business purposes but also because of federal and state laws that require such safeguards. Finally, some states are taking steps, legislatively, to address consumer concerns regarding SSN use and privacy of their personal information. Of the 18 states we examined, at least 6 had enacted laws specifically restricting private sector use and display of SSNs. California's law, in particular, has had some nationwide effect on business practices in places where some businesses have discontinued the display of SSNs in all of their locations. Also, our review shows that several state laws are similar to California's. In addition, while some state laws and regulations we reviewed did not restrict or prohibit SSN use or display specifically, they did extend beyond federal restrictions regarding the sharing of personal information.

Private Sector Users of Social Security Numbers



Source: Social Security Administration and GAO Analysis.

Contents

Letter		1
	Results in Brief	2
	Background	4
	Private Sector Entities Routinely Obtain SSNS from Their Business Clients and Use Them Largely as a Tool to Identify Individuals	6
	Federal and State Laws Affect the Disclosure of Personal Information, and Businesses Say They Have a Proprietary Interest in Safeguarding SSNs	13
	Concluding Observations	23
	Agency Comments	24
Appendix I	Scope and Methodology	25
Appendix II	Federal Laws Affecting Information Resellers, CRAs, and Health Care Organizations	27
	GLBA	27
	DPPA	28
	HIPAA	29
	FCRA	29
Tables		
	Table 1: Aspects of Federal Laws That Affect Private Sector Disclosure of Personal Information	14
	Table 2: Provisions Included in Enacted Legislation Reviewed	22

Abbreviations

CRA	consumer reporting agencies
DPPA	Drivers Privacy Protection Act
FCRA	Fair Credit Reporting Act
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
SSA	Social Security Administration
SSN	Social Security Number

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



G A O

Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

January 22, 2004

The Honorable E. Clay Shaw
Chairman
Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

Dear Mr. Chairman:

The Social Security number (SSN) is used for a myriad of non-Social Security purposes. Private and public sector entities frequently ask individuals for SSNs in order to conduct their business and sometimes to comply with federal laws. Certain private sector entities, such as consumer reporting agencies (CRAs), information brokers or resellers¹, and health care organizations, use the SSN as a key piece of information that enables them to conduct their business and deliver services to their customers. For example, business clients or individual customers provide SSNs to these entities, and the numbers are used to produce credit reports or verify information about individuals for employment and other purposes. However, given the apparent rise in identity theft crime, as recently reported by the Federal Trade Commission,² as well as the rapidly increasing availability of personal information over the Internet, Congress has expressed concern over how certain private sector entities obtain, use, and safeguard SSN data.

We previously reported on the benefits to government and commercial entities of using SSNs.³ To build on that work and to address Congress' ongoing concern about certain commercial entities' use of SSNs, in this report we focus on information brokers or resellers, CRAs (sometimes

¹Information resellers are companies that amass consumer information from various sources for the purpose of reselling such information for fraud prevention and risk management data solution products, retail marketing, and investigative research tools.

²Federal Trade Commission, *Identify Theft Survey Report*, Washington, D.C.: September 2003.

³See U.S. General Accounting Office, *Social Security: Government and Commercial Use of the Social Security Number Is Widespread*, [GAO/HEHS-99-28](#) (Washington, D.C.: Feb 16, 1999) and *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, [GAO-02-352](#) (Washington, D.C.: May 31, 2002).

referred to as credit bureaus), and health care organizations, which are the same industries that we focused on in our previous work. You requested that we (1) describe how information resellers, CRAs, and some health care organizations obtain and use SSNs and (2) discuss the laws and practices relevant to safeguarding SSNs and consumers' privacy.

To determine how information resellers, CRAs, and health care organizations obtain and use SSNs, we conducted on-site structured interviews with six large information resellers, three large and well-known CRAs, two large health care plans, and two health care industry associations. We also had our investigators access the Web sites of six Internet-based information resellers that specialize in searching for people or obtaining information about individuals by the use of SSNs, and our investigators paid them a fee to obtain their information. To determine the laws and practices relevant to safeguarding SSNs, we questioned information resellers, CRAs, health care organizations, and the Federal Trade Commission about the relevant federal laws that limit these entities' ability to obtain and use individuals' personal information that includes SSNs. We also questioned the private sector entities about the safeguards they had in place to protect SSNs and reviewed some of their policies and procedures. However, we did not verify the extent to which these businesses comply with their own policies, procedures, and safeguards. To discuss actions taken by states to safeguard consumers' privacy, we conducted site visits to two states—one that had passed privacy legislation and one that had issued an executive order on personal information, surveyed state audit officials in each of the 50 states, and interviewed select industry and state officials in person or via telephone. We also conducted a legislative review of 18 states that were identified by state officials as having laws or proposed laws governing SSN use.

We conducted our work between November 2002 and December 2003 in accordance with generally accepted government auditing standards. (See app. I for more information about our scope and methodology.)

Results in Brief

We found that information resellers, CRAs, and some health care organizations routinely obtain SSNs from their business clients and individual customers and have come to rely on SSNs as identifiers that help them verify an individual's identity and accumulate information about that person. This is particularly true of information resellers, who amass personal information, including SSNs, from public and private sources, and provide their products and services to a variety of customers. Large information resellers generally limit their services to their business clients,

including law firms and financial institutions that establish accounts with them. Officials from these entities told us that they usually obtain SSNs from their business clients and use the information as a factor in determining the identity of an individual for purposes such as employment screening, credit information, and criminal history. Other Internet-based information resellers whose Web sites we accessed also obtain SSNs from their individual customers and scour public records and other publicly available information to obtain information about individuals. These resellers provide information about individuals through the Internet to persons willing to pay a fee to obtain the information. CRAs obtain SSNs from businesses that furnish individuals' data, including SSNs, to them and they also receive information from other information resellers and public records. CRA officials told us that they use SSNs to determine consumers' identities and match the information they receive from businesses with information stored in consumers' credit files. Finally, health care organizations obtain SSNs from individuals themselves and from companies that offer health care plans. These organizations use SSNs as member identification numbers, which enable them to identify the correct individual, the type of coverage the individual has under the health plan, and other information, such as medical services and prescription drugs provided to that individual.

Certain federal laws help to safeguard consumers' personal information, including SSNs, by restricting the disclosure of and access to such information, and private sector officials we spoke with said that they indeed take steps to safeguard the SSN information they collect. Federal laws, such as the Gramm-Leach-Bliley Act, the Drivers Privacy Protection Act, and the Health Insurance Portability and Accountability Act, have placed restrictions on the ways in which information resellers, CRAs, and health care organizations may use and disclose consumers' personal information, including SSNs. Information resellers, CRAs, and health care organizations said that they take steps to safeguard SSN data, in part for business purposes but also because of federal and state laws that require such safeguards. Officials from these entities said that they employ certain safeguards to protect against the unauthorized use and disclosure of SSNs, such as controlling employees' access to records that contain SSNs. In addition, officials from large information resellers and CRAs said they require their business clients to sign formal agreements saying that their use of SSN data will only be for legally permissible purposes under the law. We found that some Internet-based information resellers whose Web sites we accessed also require customers to affirm the permissible purpose under the law for which they are obtaining the information. However, these Internet-based information resellers did not attempt to verify how

we used the information we purchased from them. Finally, some states are taking steps, legislatively, to address consumer concerns regarding SSN use and the privacy of their personal information. Of the 18 states we examined, at least 6 of them enacted laws specifically restricting private sector use or display of SSNs.⁴ California's law has influenced business practices and some states have adopted laws similar to California's. Also, while some state laws and regulations we reviewed did not restrict or prohibit SSN use or display specifically, they did extend beyond federal restrictions regarding the sharing of personal information.

Background

The Social Security Act of 1935 authorized the Social Security Administration (SSA) to establish a record-keeping system to help manage the Social Security program, and this 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. Because of the number's uniqueness and broad applicability, 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.

With the enhancement of computer technologies in recent years, private sector businesses are increasingly computerizing their records; as a result, these enhancements have spawned new business activities involving the aggregation of personal information.⁵ Such entities aggregate large numbers of both public and private data, including SSNs, from record-keeping systems throughout the country into centralized databases and use those databases, in many cases, for the purpose of providing consumer services. Businesses and others rely on entities such as information resellers and CRAs to use SSNs to build credit reports, extract or retrieve data from consumers' credit histories, verify individuals' identities, market their products, and prevent financial fraud.

Information resellers, sometimes referred to as information brokers, are businesses that specialize in amassing consumer information that includes

⁴Arizona, California, Georgia, Missouri, Texas, and Utah.

⁵See [GAO/HEHS-99-28](#).

SSNs for informational services. They may provide their services to a variety of customers, either to specific business clients or through the Internet to anyone willing to pay a fee. Large information resellers limit their services to businesses that establish accounts with them. Law firms, private businesses, law enforcement agencies, and others are usually their clients. For example, lawyers, debt collectors, and private investigators may request information on an individual's bank accounts and real estate holdings for use in civil proceedings such as divorce; automobile insurers may want information on whether insurance applicants have been involved in accidents or have been issued traffic citations; employers may want background checks on new hires; pension plan administrators may want information to locate pension beneficiaries; and individuals may ask for information to help locate birth parents. When requesting information, customers may ask for nationwide database searches or searches of only specific geographical areas. Other information resellers, particularly those that are Internet-based, generally offer their services to the public at large for a fee.

CRAs, also known as credit bureaus, are agencies that collect and sell information about the creditworthiness of individuals. CRAs collect information that is considered relevant to a person's credit history. These agencies then use this information to assign a credit score to an individual, indicating the person's creditworthiness. Prospective creditors purchase credit reports about specific individuals from CRAs, and then use this information to decide how much credit, if any, to extend to the individual.

Organizations that provide health care services also commonly use consumers' SSNs. These organizations generally deliver their services through a coordinated system that includes health care providers and health plans (insurers).⁶ While both providers and insurers are within this coordinated system, they are distinct from each other. For instance, in conducting business, health care providers offer medical or health services to patients and bill either the patient or the health plan for those services. In contrast, health plans offer insurance to individuals or groups of employees, who then make premium payments in exchange for services. Some health care organizations play dual roles of both health care provider and health insurer, which makes the distinction in how they obtain and use SSNs more complex.

⁶Health plans are also referred to as health care insurers.

Because of the myriad of uses of the SSN, Congress has previously asked GAO to review various aspects of SSN use in both the public and the private sectors.⁷ In our previous work, our reports have looked at how private businesses and government agencies obtain and use SSNs.⁸ In addition, we have reported that the perceived widespread sharing of personal information and instances of identity theft have heightened public concern about the use of Social Security Numbers.⁹ We have also noted that the SSN is used, in part, as a verification tool for services such as child support collection, law enforcement enhancement, and issuing credit to individuals.¹⁰ Although these uses of SSNs are beneficial to the public, SSNs are also key elements in creating false identities. We testified before the Subcommittee on Social Security, House Committee on Ways and Means, about SSA's enumeration and verification processes, and reported that the aggregation of personal information, such as SSNs, in large corporate databases, as well as the public display of SSNs in various public records, may provide criminals the opportunity to commit identity crimes.¹¹

Private Sector Entities Routinely Obtain SSNS from Their Business Clients and Use Them Largely as a Tool to Identify Individuals

Information resellers, CRAs, and health care organizations routinely obtain SSNs from their business clients and use SSNs for various purposes, such as to build tools that verify an individual's identity or match existing records. In addition to acquiring SSNs from various public sources, officials from these firms said they often obtain SSNs from their business clients wishing to use their services. For example, health care organizations obtain SSNs from the subscriber or policyholder of the employer group during the enrollment process. Given the various types of services these companies offer, we found that all of them 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. These officials said that because the SSN is a unique number, it is the most reliable factor

⁷GAO-02-352, and U.S. General Accounting Office. *Identity Theft: Prevalence and Cost Appear to Be Growing*, GAO-02-363 (Washington, D.C.: March, 2002).

⁸GAO/HEHS-99-28.

⁹U.S. General Accounting Office. *Social Security: Government and Other Uses of the Social Security Number are Widespread*, GAO/T-HEHS-00-120 (Washington, D.C.: May 18, 2000).

¹⁰GAO/HEHS-99-28.

¹¹U.S. General Accounting Office. *Social Security Numbers: Ensuring the Integrity of the SSN*. GAO-03-941T (Washington, D.C.: July 10, 2003).

in determining an individual's identity. However, most of the large information resellers said that the SSN is not needed to develop many of their products, such as products that launch e-mail marketing or telemarketing programs, but when the SSN is used, it provides increased accuracy and completeness in terms of trying to determine an individual's identity.

Large and Internet-Based Information Resellers Obtain SSNs from Their Business Clients, as Do CRAs and Health Care Organizations

Information resellers generally obtain SSNs from their business clients, who often provide SSNs to obtain a reseller's services or products. However, most of the large information reseller officials we spoke to said that many of the products they offer do not incorporate SSN data. They said they generally amass demographic information about households in order to provide marketing products such as detailed data lists of e-mails and postal addresses, and telephone numbers, or information for retailers and others to use to obtain new customers. As a result, their business concentrates more on marketing such products. However, these officials said that they obtain SSNs from their business clients because they also offer specific services, such as background checks, employee screening, determining criminal histories, or searching for individuals. For example, business customers of some of the information resellers who specialize in employee screening provide them with SSNs in order to have background checks done on potential employees.

Large information resellers also said they can obtain SSNs from various public and private sources. For example, they obtain SSN data from public records such as bankruptcies, tax liens, civil judgments, criminal histories, deaths, real estate ownership, driving histories, voter registration, and professional licenses. These officials said, however, that the availability of SSN information in public records varied depending on the state and county. For example, some states and counties included SSNs in their filings of tax liens and court records, but not in other records. Bankruptcy information, which is governed at the federal level, always includes SSNs. All of the resellers that we spoke to said that they obtain SSNs from public records where possible, and to the extent the information is provided on the Internet, they are likely to obtain it from such sources. However, 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 them from public records. Our investigators also used the Web sites of the Internet-based resellers to try to determine the sources they used to obtain information on SSNs. We reviewed the sources of information the resellers listed on their Web sites. They found that they relied mostly on public information and public

record data. For example, they listed various kinds of public record information at the state, county, and national levels, as well as other publicly available information, such as newspapers. As with large information resellers, once they obtained an SSN they relied on information in public records to help verify an individual's identity and obtain additional information.

Some large information resellers may also obtain SSN information from private sources. In many cases such information was obtained 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. For example, officials from one large reseller said they obtained lists of their retail customers' credit card holders. The list includes the names, addresses, SSNs, and other data of the credit card holders. The reseller then uses the list to match the names of the retail company's delinquent payment holders with the most recent bankruptcy records. In addition, Federal Trade Commission (FTC) staff said that information resellers also obtain information from CRAs.

We found the Internet-based 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. We found these entities to be primarily focused on amassing information around an individual's SSN, which in most cases they obtain from customers trying to use their Web sites. To discover what type of information could be obtained from such sources, our investigators accessed the Web sites of six Internet-based information resellers and paid a fee to gain access to the personal data. We found that when we supplied a SSN, these resellers provided with us information such as the corresponding name, address, and telephone number and, on two occasions, a truncated SSN such as 123-45-xxx. All but one of the Internet-based resellers required our investigators to provide both the name and SSN of the person who was the subject of our inquiry.

Like information resellers, CRAs also obtain SSNs from their customers or the businesses that furnish data to them, as well as from private and public sources. CRA officials said that they obtain SSNs 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. These businesses voluntarily report consumers' charge and payment transactions, accompanied by SSNs, to CRAs. Individuals provide these businesses with

their SSNs for reasons such as applying for credit. CRA officials said that they also obtain SSNs from public sources. For example, some officials said SSNs can be obtained from bankruptcy records, a fact that is especially important in terms of determining that the correct individual has declared bankruptcy. CRA officials told us that they also obtain SSNs from other information resellers, especially those that specialize in obtaining information from public records.

CRA and information reseller officials we spoke to also said that they would support limiting the public display of SSNs, especially where the general public might be able to retrieve such information. For example, they said they support removing the SSN from identification cards, health care insurance cards, and university student identification numbers. None of these officials, however, support removing the SSN from public records or restricting their access to SSN data in public records. They said such restrictions would slow some business transactions and likely increase costs to consumers because many of the conveniences currently enjoyed by consumers, such as obtaining instant credit, would take much longer and, in some cases, cease to exist.

Finally, health care organization officials said that they obtain SSNs from individuals themselves and 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.

Businesses Use SSNs to Verify Individuals' Identities and to Compile Information about Individuals

We found that the primary use of the SSN by information resellers, CRAs, and health care organizations alike was to help verify the identity of an individual. In addition, the SSN was also used to compile and match data about individuals with information already in company databases. This was particularly true of CRAs, whose officials said they usually match individuals' SSNs with records in their data sets. Most information reseller, CRA, and health care organization 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 and Internet-based Information Resellers Use the SSN as an Identifier

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 client's 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." According to this company's information, the data model compares information provided by the applicant, such as name, address, and SSN, with the data they already have in their databases, which is composed of multiple public and private sources. Another information reseller that specializes in mortgage services uses the SSN as the main factor in identifying individuals for their product reports and also for conducting investigations for their clients for resident screening or employment screening. Yet another large information reseller uses SSNs for internal matching purposes of its databases. For example, this company has various database products that compile information to provide such products as insurance underwriting tools.¹² We also found that Internet-based information resellers use the SSN as a factor in determining an individual's identity. Although the Internet Web sites we accessed advertised by saying they would be able to find a person's SSN or find a person using an SSN, these resellers in all but one case required us as the client to supply the SSN. The information they then provided back to us was information that usually restated what we had given them or verified the person's SSN.

Most of the 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 said that they provide their clients with a truncated SSN, an example of which would be 123-45-xxxx. In one case, one large information reseller provides business products with three different access levels, which includes the general public, subscriber products, and select products for entities such as law enforcement. Company officials said the subscriber level provides subscribers with truncated SSNs, while full SSNs are viewable at the select group product level, giving the user

¹²Officials from this company stated that information in this database comes from a variety of sources, such as government agencies, insurance companies, and CRAs.

CRA's Use SSNs as Identifiers
and to Match Incoming Data
with Their Existing Databases

group a tool to authenticate data about specific individuals.¹³ With regard to the Internet-based information resellers we accessed, only one provided the complete SSN back to us. These resellers usually provided information related to the SSN we had provided them, such as name, address, or date of birth.

CRA's use SSNs as the primary identifier of individuals that enables them to match the information they receive from their business clients with the information stored in their databases on individuals. Because these companies have various commercial, financial, and government agencies furnishing data to them, the SSN is the primary factor that ensures that incoming data is matched correctly 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 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.

We found that CRA's 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. For example, information resellers that assemble or evaluate consumer credit information for the purpose of furnishing consumer reports to third parties would be considered CRA's under federal law, and the law restricts what they can do with the credit report information. Five of the six large information resellers we spoke to said they were also CRA's. CRA officials said that they also build their own databases or purchase databases from other companies, and then resell the information in these databases to their customers. However, CRA officials said that information furnished for credit reports can only be used for credit reporting purposes and

¹³ Officials at this company said that full SSNs are obtainable by entities or individuals who have been approved through authentication and verification methods for access to the specific information. Such individuals or entities would include, state, local, and federal government entities; special investigative units and claims departments of public and private insurance companies; collection departments of companies that own their debt; and other public and private entities, on a case-by-case basis, for the purposes of detecting, investigating, or preventing fraud or other criminal activities.

cannot be resold. Information not covered by federal law that CRAs use to build their databases or buy from other databases can be resold as consulting solutions or direct-marketing products. In our discussions with CRAs, some officials said that information reselling constituted as much as 40 percent of CRAs' business.

Health Care Organizations Also Use SSNs to Identify Individuals but in Some Cases Such Use Is Being Discontinued

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, or they 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,¹⁴ to coordinate member benefits, and as a cross-check for pharmacy transactions. For example, health care officials said that when people purchase pharmaceuticals, the SSN is used to help identify the person that is authorized to receive the pharmaceuticals and medical benefits. 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 to an individual.

Given the increased interest in the use and protection of SSNs as well as the recent passage of federal and state laws, health care organization officials said that in some instances health care organizations are limiting their use of SSNs to be in compliance with the laws. For example, one health care organization we spoke to said that certain of its regions no longer use SSNs as a basis for providing member records or for identification purposes. Another region does not use the SSN to verify the identity of members, but instead relies upon the medical record number, date of birth, or address. In yet another region, health care insurers use a unique account number because SSN's cannot be used as the health care insurer's account number.

¹⁴During the enrollment process, subscribers have a number of options, one of which is deciding 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.

Federal and State Laws Affect the Disclosure of Personal Information, and Businesses Say They Have a Proprietary Interest in Safeguarding SSNs

Information resellers, CRAs, and health care organization officials said that certain federal laws have helped to limit the disclosures they are allowed to make to their customers. Officials from these companies said that they are either subject to the laws directly, given the nature of their business, or indirectly, through their business clients subject to these laws. In addition, we found that information resellers, CRAs, and health care organizations take steps to safeguard SSN data, sometimes by employing safeguards to protect against the unauthorized use and disclosure of SSNs or, in the case of large information resellers and CRAs, requiring their clients to sign formal agreements saying that their use of SSN data will be only for activities permissible under the law. We also found that Internet-based information resellers also require customers to affirm the permissible purpose under the law for which they are obtaining the information. Finally, at least six states have enacted laws to restrict the private sector's use of SSNs, and California's SSN law has had some effect nationwide. In addition, some state regulations and laws regarding the sharing of personal information have extended beyond federal restrictions.

Certain Federal Laws Limit Disclosure of Personal Information That Includes SSNs

According to officials we spoke to, certain federal laws have placed restrictions on their use and disclosure of consumers' personal information that includes SSNs. These laws include 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.

GLBA Limits Disclosure of Nonpublic Personal Information That Includes SSNs

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

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

Source: GAO analysis.

Prior to GLBA, financial institutions had few limitations as to where, why, and to whom they could provide customer data. GLBA helps protect consumers’ privacy and limits when a financial institution may disclose certain types of a consumer’s financial information. GLBA created a new definition of personal information, referred to as nonpublic personal information, which means personally identifiable financial information that is

1. provided by a consumer to a financial institution (for example, name, address, income, SSN, or other information on an application);
2. the result of any transaction with the consumer or any service performed for the consumer (for example, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or
3. otherwise obtained by the financial institution (for example, information from a consumer report).¹⁵

Provisions under GLBA limit when a financial institution may disclose a consumer’s nonpublic personal information to non-affiliated third parties.

¹⁵Nonpublic personal information does not include information that is “publicly available.” In other words, the information is generally made lawfully available to the public, and an individual can direct that it not be made public.

Financial institutions must notify their customers about their information sharing and tell consumers of their right to opt out if they do not want their information shared with certain non-affiliated third parties.¹⁶ GLBA covers a broad range of financial institutions, including many companies not traditionally considered to be financial institutions, because they engage in certain “financial activities.” In addition, any entity that receives consumer financial information from a financial institution under one of the GLBA exceptions may be restricted in its reuse and redisclosure of that information.

We found that some CRAs consider themselves to be financial institutions under GLBA.¹⁷ 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 pursuant to notice and opt-outs, they could resell the information only to the extent that they were consistent with the privacy policy of the originating financial institution and any opt-outs.

Information resellers and CRAs also said that they protect the use of consumers’ nonpublic 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

¹⁶An exception to this opt-out requirement is that a financial institution may provide nonpublic personal information to a non-affiliated third party that is performing services for or functions on behalf of the financial institution, including marketing of the financial institution’s own products or services. The financial institution must, however, fully disclose this to the consumer, and the non-affiliated third party must enter into a contractual agreement to maintain the confidentiality of such information.

¹⁷Under 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.

resellers and CRA officials said that they adhere to GLBA's standards in order to secure financial institutions' information.

FTC staff said that although GLBA helps to limit the disclosure of consumers' nonpublic personal information, GLBA also includes certain broad exceptions that are unspecific (see app. II for information on GLBA's exceptions). FTC officials said that they receive many inquiries from CRAs and information resellers concerning the application of GLBA's exceptions, such as whether the exceptions apply to certain circumstances. As a result, they said it is difficult to determine how and whether certain entities are appropriately interpreting the exceptions.

DPPA Limits Disclosure of Personal Information from a Motor Vehicle Record That Includes SSNs

DPPA was enacted to prohibit the release and use of certain personal information from state motor vehicle records. DPPA prohibits any person from knowingly obtaining or disclosing personal information from a motor vehicle record for any use not permitted under DPPA. DPPA specifies certain exceptions when personal information contained in a state motor vehicle record may be obtained and used, such as use by an employer or its agent or insurer to obtain information relating to the holder of a driver's license (see app. II for a list of permissible uses).

As a result of DPPA, information resellers said they were restricted in their ability to obtain SSN 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.

HIPAA Restricts Disclosing Protected Health Information That Includes SSNs

HIPAA requires health care organizations and providers to meet certain privacy standards with respect to personal health information. HIPAA's privacy rule specifically states that "a covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." The privacy rule provides patients access to their medical records, control over how their health information may be used and disclosed, avenues for recourse if their medical privacy is compromised, and a number of other privacy rights (see app. II for more details on covered entities and individuals' obligations and rights). HIPAA gives individuals the right, in most cases, to obtain and

inspect copies of health information about themselves. In addition, it generally restricts health care plans and certain health care providers from disclosing such information to others without the patient's consent, except for purposes of treatment, payment, or other health care operations. There are, however, exceptions to facilitate compliance with state reporting requirements and other public health purposes.

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 do 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.

FCRA Limits Access to Information in Credit Data

Under FCRA, Congress has limited the use of consumer reports¹⁸ 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 (see app. II for a list of FCRA's permissible purposes). However, these limits are not specific to SSNs. All of the CRAs that we spoke to said that they are considered to be 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 FCRA's 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.

¹⁸The FTC has determined that certain types of information, including SSNs, do not constitute a consumer report under FCRA because they are not factors in determining credit eligibility.

Large Information Resellers, CRAs, and Health Care Organizations Employ Safeguards to Protect SSN Information

Large information resellers, CRAs, and health care officials said they employ certain safeguards to mitigate the risk of individuals gaining unauthorized access to SSNs or making improper disclosure or use of SSNs. These officials said that potential risks occur from internal sources such as employees' unauthorized access to information and from external sources such as business clients and computer hackers. To address internal risks, these officials said they (1) conduct background checks on employees, (2) train employees on the appropriate way to handle sensitive information, (3) teach employees about the federal and state laws governing certain information, (4) require employees to sign written agreements that specify what they are allowed to do with information that includes an SSN, and (5) terminate employees and take legal actions against employees that improperly use or disclose SSNs. For example, health care organization officials said they train their employees on how to comply with HIPAA and how to safeguard medical records and other types of personal information. Some information resellers said that they take steps to control and monitor employee access to computerized records that contain SSNs by assigning different levels of access. Employees are, therefore, only given access to information that they need to perform their job. In addition, employees' access to records that contain SSNs was also monitored. For example, some officials said they track employees browsing in records in certain databases and monitor any unusual transactions. In some cases, CRA and health care officials said they created audit trails for every transaction, and these trails allow them to track employees' activities.

Officials from large information resellers and CRAs also told us that they take action to mitigate external risks that could result in the unauthorized use and disclosure of SSNs. Some of these officials said they have "know your customer" policies in place. For example, one information reseller told us that prior to the sale of information, they verify the identity of their customers and make sure they have the necessary credentials to obtain access to their information database. Large information resellers and CRA officials also said they always determine the eligibility of their customers to have access to their information by conducting audits of their customers prior to entering into a contract with them. For example, they determine prior to entering into a formal contract that in the case of a CRA, the financial institution is what it says it is and is eligible to receive credit reports. Or, in the case of an information reseller, that a law enforcement agency is in fact a law enforcement agency and is eligible to receive motor vehicle information. In conducting their audits, these entities review customers' business licenses, perform background and credit checks, and often visit the entity itself. Some officials did say,

however, that they face certain challenges in protecting SSN data, such as ensuring that they provide their information to legitimate businesses or government agencies that have appropriate, legally permissible purposes to have such information. Nonetheless, there have been cases when the unauthorized use and disclosure of SSNs have occurred. For example, CRA officials told us that through their audit process they discovered instances where their clients have violated their written agreement by using personal information for non-permissible purposes.

Large information reseller and CRA officials also said they require their clients to sign formal agreements acknowledging that the information provided to them will be used in accordance with permissible activities under federal and state law. For example, if a business client wanted to obtain information from a state motor vehicle agency, the client would have to sign a formal agreement saying that such information would be used only for permissible purposes, such as the verification of personal information for the purpose of preventing fraud or the pursuit of legal remedies against an individual. Representatives of one large reseller that we spoke to said that they not only require their clients to indicate which permissible use applies before they give access to information, but they also have specific access levels, depending on their client's formal agreement with them. For example, if the client was an investigative police unit, then it could be granted full access to the reseller's databases under the formal agreement, which included full SSN disclosure as well as other personally identifiable information. Clients granted this level of access were subject to background checks and other verification techniques, such as on-site verifications, by the reseller.

Once a formal contract has been entered into with a customer, large information resellers and CRA officials said that they audit their clients to ensure that they are complying with the legal and contractual restrictions, such as obtaining credit reports for legitimate business purposes. In addition, these audits may be conducted either on-site or by mail requiring the customer to provide documentation regarding the permissible purposes for the information requested by the customer. Officials from one entity told us they conduct an Internet "secret shopper" program whereby they police certain Internet Web sites that sell SSNs to make sure that their customers are not supplying these sites. In addition, health care officials said that health insurance companies are audited by state insurance departments to ensure that, among other things, appropriate computer safeguards are in place.

Large information resellers and CRA officials also told us that they are frequently audited by their customers, who need to ensure that they are in turn in compliance with the same laws and restrictions they impose on their clients. For example, CRA officials told us that especially with regard to GLBA requirements, financial institutions are frequently auditing their computer systems to make sure they meet standards under GLBA.

We found that Internet-based information resellers require customers, upon accessing their Web site, to acknowledge that they will abide by their “terms and conditions” and indicate the permissible purpose for which they are obtaining the information. For example, we found that they required our investigators to concur with the site’s terms and conditions before any informational service was provided. In addition, two of the Internet-based resellers provided a list of permissible purposes from which we had to select, such as collection purposes. At these resellers’ Web sites, only after we indicated the permissible purpose for which we would like to purchase information were we allowed to purchase personal information by credit card. We did not find that the Internet-based resellers attempted in any way to audit us, determine who we were, or determine that we were indeed using the information for the permissible purpose we had selected.

At Least Six States Have Enacted Laws to Restrict Private Sector Use of SSNs

At least six states have enacted their own legislation to restrict private sector uses of SSNs. Based on our review of select legislative documents within 18 states, California, Missouri, Arizona, Georgia, Utah, and Texas had enacted laws to restrict either the display or the use of SSNs.¹⁹ In 2001, California enacted Senate Bill (SB) 168, restricting private sector use of SSNs. Specifically, this law generally prohibits companies and persons from:

- posting or publicly displaying SSNs,
- printing SSNs on cards required to access the company’s products or services,
- requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted,

¹⁹In 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.

-
- requiring people to log onto a Web site using an SSN without a password, or
 - printing SSNs on anything mailed to a customer unless required by law or the document is a form or application.²⁰

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 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.²¹ 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 the Georgia and Utah laws are directed at health insurers and, therefore, pertain primarily to insurance identification cards.²² 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.

²⁰Cal. Civ. Code§1798.85.

²¹Political subdivisions would include counties, cities, and towns.

²²Georgia's law (O.C.G.A. §33-24-57.1(f)) and Utah's law (Utah Code Ann. §31-22-634) are 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.

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.

California’s SSN Law Appears to Have Had Some Nationwide Effect

During the course of our work, we found that California is at the forefront with respect to its consumer privacy protection efforts and that the enactment of its SSN law restricting private sector display of SSNs appears to have had some nationwide effect on business practices. For example, a senior manager for at least one private company with locations in California stated that the company identified 175 areas within its organization where SSNs were being used, and 130 of these (over 74 percent) were in connection with health care organizations providing health care services to its employees. As a result, the company has asked all of its health care providers nationwide—regardless of respective state laws—to discontinue their display of SSNs on health benefit cards. In addition, according to officials representing one health care association, as a result of the California law, by January 2006 all of its health care plans—located in various states—are required to discontinue displaying SSNs on their cards. In addition, our review of state legislation and interviews of state and industry officials show several state laws are very similar to California’s law.

Some State Laws and Regulations Extend beyond Similar Federal Restrictions

We found that regulations and laws in 2 of the 18 states we reviewed do not address SSNs specifically but do extend beyond federal restrictions regarding the sharing of “personal information,” which may include SSNs. As previously mentioned, GLBA requires that financial institutions provide consumers the opportunity to opt out of sharing personal information with certain third parties, meaning that unless a consumer notifies the financial institution not to, the institution may share this information. Alternatively, financial institutions may disclose nonpublic information to non-affiliated third parties, including other financial institutions, pursuant to certain exceptions in GLBA, without providing consumers a right to opt out of those disclosures. In addition, FCRA allows those with a legitimate, legally defined purpose or permissible purpose access to consumers’ credit information. To better address consumer concerns about privacy and the protection of personal information, however, states such as Vermont and North Dakota have issued regulations or enacted laws that extend beyond the provisions of these two federal laws. For example, an Assistant

Attorney General in Vermont stated that while Vermont does not have any specific laws governing the use of SSNs, it has regulations requiring banking, insurance, and securities companies to obtain consumers' permission prior to sharing consumers' personal information—opt-in provisions. The Assistant Attorney General added that Vermont's Fair Credit Reporting Act has a similar opt-in requirement before permitting access to consumer credit reports. Furthermore, until Congress passed the GLBA, North Dakota had a banking privacy law to protect personal information. This banking law also prohibited financial institutions in North Dakota from selling or sharing customer data with other companies unless the individual provided consent. The North Dakota legislature amended the state's opt-in privacy law to make it consistent with GLBA's opt-out requirement. However, in June 2002, following public outcry, North Dakota voters passed a referendum reinstating the former opt-in law, again requiring consumer consent before sharing personal information.

Concluding Observations

Information resellers, CRAs, and health care organizations are likely to continue obtaining and using SSNs primarily to match records, since the SSN is a key factor in determining the identity of an individual and there is no widely accepted alternative. While these entities told us that they typically do not resell SSNs they obtain, there are few restrictions placed on their ability to obtain and use SSNs for their businesses, including information obtained from public records—a primary source of personal data for most information resellers. Certain state laws, however, limit the disclosure of some personal information that includes SSNs. Federal laws that have some restrictions on reselling nonpublic personal information, such as GLBA, have broad exceptions, which entities can broadly interpret. This broad interpretation combined with the uncertainty about the application of the exceptions suggests that reselling personal information—including SSNs—is likely to continue.

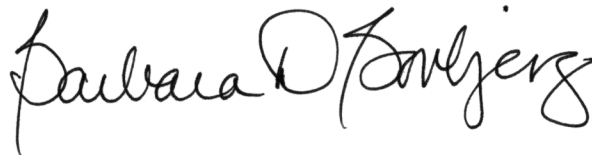
Private sector officials we spoke to agreed that, given the continued rise in identity crimes, removing SSNs from public display is a step in the right direction. However, these officials stated that they had legitimate uses for the SSN and that restricting business-to-business access or use of such information would hurt consumers and possibly aid identity thieves in their attempts to assume an individual's identity by making it more difficult for businesses to verify an individual's identity. Thus, any restrictions Congress deems necessary regarding SSNs will have to weigh the consequences of restricting the use of SSNs on the one hand with legitimate business needs for the use of SSNs on the other.

Agency Comments

We provided a draft of this report to the Commissioner of the Social Security Administration and the Chairman of the Federal Trade Commission for their review and comment. Neither agency provided a formal comment letter. However, the FTC provided technical comments, which we incorporated as appropriate.

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its issue date. At that time, we will send copies of this report to the Commissioner of the Social Security Administration and the Chairman of the Federal Trade Commission. Copies will also be made available to others on request. In addition, the report will be available at no charge on GAO's Web site at <http://www.gao.gov>.

If you have any questions concerning this report, please contact me on (202) 512-7215 or George Scott at (202) 512-5932. Other major contributors include Gwen Adekun, Richard Burkard, Tamara Cross, Jason Holsclaw, Raun Lazier, Kevin Murphy, and James Rebbe.



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

Appendix I: Scope and Methodology

To describe how information resellers, CRAs, and health care organizations obtain and use SSNs, we expanded on previous GAO work in this area and we interviewed officials from large information resellers, CRAs, health care organizations, the Consumer Data Industry Association (an international trade association that represents consumer information companies), and the Social Security Administration. We then selected six large and well-known information resellers and conducted structured interviews about how they obtained and used SSNs. We also had our investigators access six Internet-based information resellers' Web sites. We researched such resellers on the Internet and choose six that specialized in finding people by their SSN or searched for people by their SSN. To understand how CRAs obtain and use SSNs, we interviewed three large, well-known CRAs. Finally, to determine how health care organizations were obtaining and using SSNs, we talked to two large and well-known health care plans. One submitted our questions to its eight regions, and the other also sought the views of its various regions. We also talked to two health care organizations—one that represents 1,000 health care plans, and one whose 300 members are primarily insurers. Each association asked some of its members to determine how they obtained and used SSNs. We were unable to determine the extent to which some of their responses were representative of associations with similar memberships.

To determine the laws and practices relevant to safeguarding SSNs, we determined what federal laws were helping to protect SSNs through our discussions with information resellers, CRAs, health care organizations, and the Federal Trade Commission. We then researched the relevant laws and reviewed them to determine what limits were placed on the use and disclosure of an individual's personal information, including SSN. To report on the safeguards that information resellers, CRAs, and health care organizations have in place to protect SSNs, we conducted site visits and in-depth interviews with certain of these entities. We asked them about the types of safeguards they employ to protect SSNs from both internal and external misuse. We also reviewed their policies and procedures for protecting SSNs. However, we did not assess the safeguards that they used to protect SSNs. Also, the information we obtained from these entities was self-reported and was not independently verified by GAO. Finally, to gain an understanding of what states are doing legislatively to restrict SSN use, we conducted site visits to two states—California and Washington; conducted interviews with federal, state, and industry officials; and reviewed pertinent state legislation. More specifically, our interviews at the federal level were with officials from the Federal Trade Commission, the Secret Service, and the Department of the Treasury. At the state level,

we interviewed officials from Washington's Office of the Attorney General and California's Office of Privacy Protection. Also at the state level, we surveyed state audit officials in each of the 50 states to determine whether they had conducted reviews relating to our work, whether they were familiar with state laws affecting private sector use of SSNs, and whether they were aware of any notable practices (within the public or private sector) aimed at protecting consumer privacy and personal information. In addition, we interviewed private sector businesses and organizations and contacted some state offices of the attorney general, and identified state laws and legislative initiatives related to the use of SSNs. This resulted in our legislative review of 18 states (including the 2 states we visited) that were identified as having laws or proposed laws governing SSN use.

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

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.

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, 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.

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.

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.

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

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. General Accounting 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

Public Affairs

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