United States Government Accountability Office

GAO

Report to Congressional Requesters

January 2006

SOCIAL SECURITY NUMBERS

Stronger Protections Needed When Contractors Have Access to SSNs

GAO-06-238

January 2006

SOCIAL SECURITY NUMBERS

Stronger Protections Needed When Contractors Have Access to SSNs

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-238, a report to congressional requesters

Why GAO Did This Study

Recent data breaches highlight how identity theft may occur when businesses share individuals' personal information, including Social Security Numbers (SSNs), with contractors. Because private sector entities are more likely to share consumers' personal information via contractors, members of Congress raised concerns about the protection of this information in contractual relationships. In response, GAO examined (1) how entities within certain industries share SSNs with contractors; (2) the safeguards and notable industry standards in place to ensure the protection of SSNs when shared with contractors; and (3) how federal agencies regulate and monitor the sharing and safeguarding of SSNs between private entities and their contractors.

What GAO Recommends

GAO recommends that Congress consider possible options for addressing gaps in federal requirements for safeguarding SSNs shared with contractors. None of the seven agencies GAO talked to provided formal written responses. However, six of the seven agencies provided technical comments, which were incorporated as appropriate.

www.gao.gov/cgi-bin/getrpt?GAO-06-238.

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.

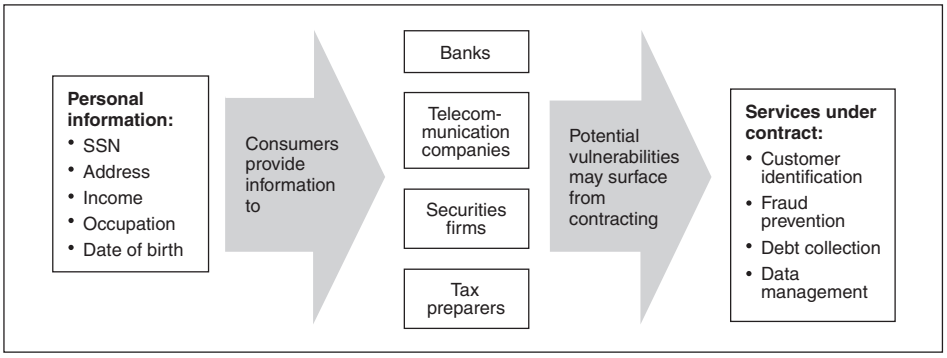
What GAO Found

Banks, securities firms, telecommunication companies, and tax preparation companies share SSNs with contractors for limited purposes. Firms GAO interviewed routinely obtain SSNs from their customers for authentication and identification purposes, and contract out various services, such as data processing and customer service functions. Although these companies may share consumer information, such as SSNs, with contractors, company officials said that they only share such information with their contractors when it is necessary or unavoidable.

Companies in the four business sectors GAO studied primarily relied on accepted industry practices and used the terms of their contracts to protect the personal information shared with contractors. Most company officials stated that their contracts had provisions for auditing and monitoring to assure contract compliance. Some noted that their industry associations have also developed general guidance for their members on sharing personal information with third parties.

Federal regulation and oversight of SSN sharing varied across the four industries GAO reviewed, revealing gaps in federal law and agency oversight in the four industries GAO reviewed that share SSNs with contractors. Financial services companies must comply with the Gramm-Leach-Bliley Act (GLBA) for safeguarding customers' personal information and regulators have an examination process in place to determine whether banks and securities firms are safeguarding this information. IRS has regulations and guidance in place to restrict the disclosure of SSNs by tax preparers and their contractors, but does not perform periodic reviews of tax preparers' compliance. Because the Federal Communications Commission (FCC) believes that it lacks statutory authority to do so, it has not issued regulations covering SSNs and also does not periodically review telecommunications companies to determine whether they are safeguarding such information.

Personal Information and Contracting



Source: GAO.

Contents

Abbreviations

SSN	Social Security Number
CPNI	Customer Proprietary Network Information
ERO	Electronic Return Originator
FACTA	Fair and Accurate Credit Transaction Act
FCC	Federal Communications Commission
FCRA	Fair Credit Reporting Act
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act
IRC	Internal Revenue Code
IRS	Internal Revenue Service
OCC	Office of the Comptroller of the Currency
OTS	Office of Thrift Supervision
SEC	Securities and Exchange Commission

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.

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

January 23, 2006

The Honorable Jim McCrery
Chairman
Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

The Honorable E. Clay Shaw
House of Representatives

Today, the Social Security number (SSN) is a vital piece of information needed to function in American society. United States' citizens and legal residents need an SSN to obtain employment, a driver's license, or government benefits, among other uses. For these reasons, the SSN is highly sought by individuals seeking to create false identities or commit financial fraud or both. In light of the number of reported data breaches over the past year and the rising reports of identity theft, there are concerns about the way businesses and other organizations obtain, use, and safeguard the SSNs in their possession. A recent series of data breaches has highlighted how identity theft may occur when governments or businesses share individuals' personal information with contractors. For example, in 2005, it was reported that one financial service company's consumer information was compromised when the shipping company it contracted with lost data storage tapes that contained the account information, including SSNs, of roughly 4 million individuals.

Businesses and other institutions routinely use outside contractors to perform activities or functions related to their operations. In some cases, the businesses perform a particular function or activity but nonetheless decide to contract it out—a practice widely known as outsourcing. In other cases, outside contractors are hired to perform tasks that a company does not have the capacity to perform itself, such as computer systems maintenance or doing credit checks. When a business has collected personal information from its customers and shares that information with its contractors, the contractors become third party users of that information. Because private sector entities are increasing their use of contractors and are more likely to share personal information about customers with them, including SSNs, you asked that we determine (1) how entities within certain industries share SSNs with contractors; (2) the safeguards and notable industry standards in place to ensure the

protection of SSNs shared during such contracting; and (3) how federal agencies regulate and monitor the sharing and safeguarding of SSNs between the entities they oversee and the entities' third party contractors.

We focus in this report on the uses and protections of SSNs when they are shared with contractors and subcontractors within the banking, securities, telecommunications, and tax preparation industries. We selected these industries because they are known to collect personal information, including SSNs, and outsourcing and information security experts we interviewed said these industries were among the most likely to share SSNs with contractors. We conducted interviews with 12 companies in these industries, five companies that provide services under contract, and six associations for these industries to better understand why they use the SSN and the types of contracts in which SSNs are shared. To identify safeguards and notable industry practices that were followed, we reviewed standard contract forms from companies in the four selected industries. We also asked companies we met with about the safeguards they had in place to protect SSNs, and we 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 determine the federal and state laws relevant to the sharing of consumer information during third party contracting, we questioned federal and state agencies—such as Federal Trade Commission (FTC), Federal Communications Commission (FCC), the Internal Revenue Service (IRS), banking regulators, and California's Office of Privacy Protection—as well as company and industry association officials about the relevant laws that govern the private sector's ability to share consumer information with a third party.

We conducted our work between July 2004 and January 2006 in accordance with generally accepted auditing standards. Appendix I discusses our scope and methodology in further detail.

Results in Brief

Officials we interviewed from banks, securities firms, telecommunication firms, and tax preparation firms all said their companies engaged in third party contracting, but only share SSNs with their contractors for limited purposes. Company officials told us that they collect SSNs from their clients for identification purposes and, in some cases, because companies are required to by federal law, such as for taxpayer identification purposes or to verify a customer's identity in an effort to combat money laundering and other financial crimes. These officials also said that they used contractors for various reasons, such as financial statement processing,

maintenance services, and information technology management. In some cases, officials said their companies shared SSNs with contractors for administrative and data management functions. For example, one tax preparation company we interviewed said that it shared SSNs with a data storage company that archived and managed its paper files. Officials from several banks said that they would share SSNs with contractors to comply with federal customer verification requirements, while officials from a securities firm told us they shared SSNs with a contractor that collects delinquent payments for a mortgage division it acquired. Additionally, one telecommunication company also told us that it shares SSNs and other personal information with its customer contact center contractor for customer verification.

Companies we interviewed in the four industries relied on accepted industry practices and primarily used the terms of the companies' contracts to safeguard personal information, including SSNs they shared with outside contractors. According to our discussions with company officials and our review of contract documents, most of the companies' standard contract forms included several types of safeguards to prevent the unauthorized use or disclosure of their customers' personal information, which was consistent with documented widespread industry practices for sharing confidential information with contractors. We also found that most companies' have developed procedures for identifying and reviewing suitable contractors, and adopting safeguards for consumer information shared with those contractors. In addition, 12 companies reported that their contracts contain audit provisions to evaluate contractual compliance. Finally, some banking and securities industry associations have developed voluntary guidance for their members regarding the sharing of personal information with third parties, although banking and securities officials said they relied more on generally accepted practices for protecting personal information and guidance from federal regulators than from professional associations.

Federal regulation and oversight of SSN sharing varies among the four industries:

- In the banking and securities industries, companies must comply with the provisions of the Gramm-Leach-Bliley Act (GLBA) to establish safeguards that protect the confidentiality of personal information of customers or clients. GLBA generally permits financial institutions to share customers' personal information with contractors without customers' permission, provided that institutions fully disclose they are doing so and enter into contracts requiring the contractor to maintain

the confidentiality of the information. However, financial institutions may share customers' personal information without their permission under other limited circumstances. Through periodic examinations of bank and securities dealers and service provider exams, the federal agencies with oversight responsibility for these entities review their compliance with the agencies' GLBA regulations.

- Tax preparers are subject to Section 7216 of the Internal Revenue Code (IRC), IRS regulations, and FTC's GLBA regulations that generally prohibit disclosure of taxpayers' personal and tax-related information without the taxpayer's formal consent. IRS does not perform routine assessments to determine whether tax preparers are complying with IRS requirements. Regulations recently proposed by IRS state that tax preparers may, in certain circumstances, disclose a taxpayer's information to contractors they use, without that taxpayer's consent, for purposes related to preparing tax returns.[1]

- There are no clear federal protections for SSNs collected and shared by telecommunications firms. Although the Telecommunications Act of 1996 limits the ways in which telecommunications firms can use and disclose certain information about their customers, such as their call records, these limitations do not extend to SSNs. Therefore, the FCC—the federal agency responsible for overseeing the telecommunication industry—does not regulate how SSNs are used by telecommunications companies. However, under its authority to prohibit unfair business practices and subject to certain limitations, FTC may be able to take action against telecommunications firms that do not comply with their own company's privacy policies, but cannot enforce GLBA requirements on telecommunications companies because such companies are not considered financial institutions under the GLBA statute.

In addition to federal laws and regulations, company officials we met with also said that certain state laws affect their ability to share SSNs with third parties. Currently, California has a law affecting business interactions with

[1]Specifically, the proposed regulations would allow tax return preparers to disclose tax return information to contractors in connection with the programming, maintenance, repair, testing, or procurement of equipment or software used for purposes of tax return preparation only to the extent necessary for the person to provide the contracted services, and only if the tax preparer ensures that all individuals who are to receive disclosures of tax return information receive a written notice that informs them of the applicability of IRC sections 6713 and 7216 to them and describes the requirements and penalties of section 6713 and 7216. 70 Fed. Reg. 72954 (Dec. 8, 2005).

nonaffiliated third parties that requires the use of reasonable security procedures to protect customers SSNs and other personal information. Although other state laws the companies cited do not explicitly regulate the sharing of SSNs or other personal information with third party contractors, company officials we met with said these laws indirectly affect how they share such information with their contractors.

Because the differences in the protections for SSNs shared with contractors have allowed gaps to occur in federal law and oversight for protection of SSNs, this report includes a Matter for Congressional Consideration designed to address these gaps. In response to our draft report, no agency provided a formal written response. However, six of the seven agencies covered by our review provided technical comments, which we incorporated as appropriate.

Background

In recent years, companies have increasingly relied on the use of contractors to perform certain activities and functions related to their business operations. This trend has often been referred to as outsourcing. However, no commonly recognized definition of outsourcing exists, and there has been confusion over whether it encompasses only activities a company originally performed in-house or includes any activity a company may contract out. According to outsourcing experts, approximately 90 percent of businesses contract out some activity because they find either it is more economical to do so or other companies are better able to perform these activities. Some of the activities companies outsource will require that contractors be provided personal information about the companies' customers in order to perform those activities; in some cases, this information includes SSNs.

Originally, the Social Security Administration (SSA) created the SSN as part of a recordkeeping system to help manage the Social Security program.[2] SSA uses the SSN as a means to track workers' earnings and eligibility for Social Security benefits and assigns a unique number to every person as a work and retirement benefit record. Today, SSA generally issues SSNs to all U.S. citizens, but they are also available to non-citizens lawfully admitted to the United States as permanent residents.

[2]The Social Security Act of 1935 created the Social Security Board and authorized it to establish a record-keeping system. The board was renamed the Social Security Administration in 1946.

However, because of the number's unique nature and broad applicability, the SSN has become the identifier of choice for government agencies and private businesses and is used for numerous non Social Security purposes, such as opening a bank account and receiving health insurance.

As shown in table 1, certain federal laws have been enacted that place restrictions on some private sector entities' use and disclosure of consumers' personal information, including SSNs.

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

Federal Laws	Restrictions
Fair Credit Reporting Act of 1970 (FCRA), 15 U.S.C. § 1681b	Limits access to credit data that includes SSNs to those who have a permissible purpose under the law.
Fair and Accurate Credit Transactions Act of 2003 (FACTA), 15 U.S.C § 1681g and § 1681w	Amends FCRA to allow, among other things, consumers who request a copy of their credit report to also request that the first 5 digits of their SSN (or similar identification number) not be included in the file; requires consumer reporting agencies and any business that uses a consumer report to adopt procedures for proper disposal.
Gramm-Leach-Bliley Act of 1999 (GLBA), 15 U.S.C. § 6801 - § 6809	Creates a new definition of nonpublic personal information that includes SSNs and limits when financial institutions may disclose the information to nonaffiliated third parties. It also requires that financial services regulatory agencies establish standards for the entities under their agencies' jurisdiction relating to administrative, technical, and physical safeguards to: • insure the security and confidentiality of customer records and information; • protect against any anticipated threats or hazards to the security or integrity of such records; and • protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

Source: GAO analysis of federal legislation.

To ensure compliance with these federal laws, some federal regulators conduct examinations of their respective institutions' operations. For example, in the financial industry, federal agencies, such as the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), the Federal Deposit Insurance Corporation (FDIC) and the Securities and Exchange Commission (SEC) regulate banking or securities firms. OCC charters, regulates, and supervises all national banks, while FRB regulates bank holding companies and state-chartered banks that are members of the Federal Reserve System. FDIC regulates banks that are state-chartered banks that are not members of the Federal Reserve System. These banking regulators examine banking institutions for safety and soundness and compliance with applicable laws, including the Fair and Accurate Credit Transaction Act (FACTA), and GLBA. SEC regulates and examines investment advisers registered with the Commission and investment companies, including mutual funds, that engage primarily in investing, reinvesting, and trading in securities and that offer their own securities to

the investing public. SEC also regulates and examines other market participants, including broker-dealers and self-regulatory organizations (SRO).[3] As part of its examinations, SEC reviews these firms for compliance with GLBA's safeguard provisions. In addition, SRO's such as the New York Stock Exchange (NYSE) and National Association of Securities Dealers (NASD) examine their member broker-dealers to ensure compliance with applicable laws, self-regulatory rules, and SEC regulations, including GLBA's safeguard provision.

In 1978, the Federal Financial Institutions Examination Council (FFIEC) was created as a formal interagency body authorized to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. The council's membership is composed of the federal bank regulators—FDIC, FRB, OCC—plus the regulators for credit unions and thrift institutions—the National Credit Union Administration (NCUA) and the Office of Thrift Supervision (OTS), respectively. The FFIEC has issued guidance related to outsourcing services that provides a framework for the FFIEC agencies to examine their banks' contractor management programs and exercise enforcement options if financial institutions do not establish and maintain adequate information security programs. The FFIEC also coordinates examinations of banks' information technology service providers and separate guidance has been issued for conducting these examinations.

Along with OTS, the three bank regulators have jointly issued regulations that generally require each financial institution to develop, implement, and maintain, as part of its existing information security program, appropriate measures to properly dispose of consumer information derived from consumer reports.[4] Together, these agencies have also issued interpretive guidance requiring every financial institution to develop and implement a response program, including customer notice provisions, designed to address incidents of unauthorized access to customer information

[3]A broker-dealer is any individual or firm in the business of buying and selling securities for itself and others. Broker-dealers generally must register with the SEC. When acting as a broker, a broker-dealer executes orders on behalf of his/her client. When acting as a dealer, a broker-dealer executes trades for his/her firm's own account.

[4]69 Fed. Reg. 77610 (Dec. 28, 2004).

maintained by the institution or its service provider.[5] Under the Bank Service Company Act, as amended, the federal banking agencies have authority to regulate and examine certain services provided to banks by third parties—including contractors—to the same extent as if those services were performed directly by the bank.[6]

IRS is responsible for ensuring that tax preparers are complying with certain confidentiality provisions in the IRC, primarily Section 7216. IRC § 7216 prohibits the unauthorized use or disclosure of tax return information by tax return preparers. Tax return preparers are also subject to GLBA. However, those provisions do not supersede, alter, or affect the preexisting requirements of IRC § 7216, although FTC has oversight and enforcement authority over tax preparers' compliance with GLBA.

FCC is responsible for regulating interstate and international communications by radio, television, wire, satellite, and cable, and enforcing the provisions of the Telecommunications Act of 1996, which restricts the use of customer proprietary network information (CPNI).[7] CPNI is the data collected by telecommunications corporations on a consumer's telephone calls. It includes the time, date, duration, and destination number of each call, the type of network a consumer subscribes to, and any other information that appears on the consumer's telephone bill. SSNs are not part of CPNI.

FTC is an independent agency whose mission is, in part, to prevent business practices that are anticompetitive, deceptive, or unfair to consumers. As part of its responsibilities, FTC enforces consumer privacy provisions and safeguards of FCRA, FACTA, and GLBA not enforced by other federal agencies. FTC is also required to collect identity theft complaints.

FTC statistics currently indicate that identity theft is growing. For 2004, FTC reported that it received about 247,000 complaints from individuals stating that they were victims of identity fraud, which was up from just

[5]70 Fed. Reg. 15736 (Mar. 29, 2005). The bank regulatory agencies jointly issued this as interpretive guidance for GLBA and the joint guidelines issued by the agencies for implementing GLBA's safeguard requirements—Interagency Guidelines Establishing Information Security Standards.

[6]12 U.S.C. § 1867(c).

[7]47 U.S.C. § 222.

over 86,000 complaints reported in 2001. While the reported number of victims and likely identity crimes has increased, the extent to which these statistics represent company security breaches is not well documented. However, various news reports and identity crime experts have attributed some identity thefts and credit card fraud to security breaches involving third party companies.

Private Sector Companies We Interviewed Routinely Use Third Party Contractors and Occasionally Share SSNs with Them

Banks, securities firms, telecommunication companies, and tax preparation companies we interviewed routinely obtain SSNs from their customers for authentication and identification purposes. All the companies we interviewed contracted out various services, such as data processing, administrative, and customer service functions. Although these companies may share consumer information, such as SSNs, with contractors that provide services to their customers, company officials said that they only share such information with their contractors for limited purposes, generally when it is necessary or unavoidable.

Private Sector Companies We Interviewed Obtain and Use SSNs Primarily for Identification Purposes

Officials from selected banking, securities, telecommunications, and tax preparation companies told us that they obtain and use SSNs primarily for authentication and identification purposes related to fraud prevention, credit verification, and complying with federal law. However, these officials told us that SSNs were not distinguished from other types of customers' personally identifiable information.[8] Company officials also told us that the same safeguards applied to SSNs as all other pieces of their customers' personal information.

Officials from banks and securities firms we interviewed said that their companies obtained SSNs directly from their customers to comply with federal law when the customer opened a new account or conducted certain financial transactions. For example, the Bank Secrecy Act, as amended by the USA Patriot Act mandates that, among other things, financial institutions must verify each new account holder's identity when opening an account, in an effort to curtail money laundering and terrorist financing. According to company officials we interviewed, other federal laws and regulations require both banks and securities firms to use SSNs

[8]Personally identifiable information refers to any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains. This includes information that can easily be derived, including, but not limited to, name, address, phone number, fax number, email address, financial profiles, SSN, and credit card information.

for tax-reporting and customer-identity-verification purposes. In addition, some bank and securities firm officials said that due to its uniqueness, their companies also incorporated the SSN into their fraud prevention and authentication programs.

Telecommunication company officials we interviewed said that their companies are not required by federal law to collect or use the SSN, but that potential customers are asked to provide their SSN before establishing an account. These officials explained that their companies primarily use the SSN to query credit reporting agencies' records in order to verify a potential customer's creditworthiness, without which their companies would not be able to extend services to an individual quickly. In those instances where an individual did not have an SSN or refused to provide it, company officials said that their companies offered customers the option of using a pre paid service or providing a monetary deposit. Telecommunication companies we interviewed also used the SSN for customer account authentication and verification as well as fraud prevention. For example, officials from one company told us that they used the SSN as a key piece of information to ensure that a person inquiring about their account was the actual account holder.

Unlike the telecommunication companies, tax preparation companies are required by federal law to collect and use SSNs. IRC requires that individuals who have been assigned a number include their SSNs on their tax returns as a taxpayer identification number and that such information be kept confidential by these companies. Tax preparation officials and tax industry representatives we interviewed said that they also used the SSN as the identification number for refund payments to customers and other internal purposes. For example, officials from one tax preparation company told us that they used the SSN as the identification number for tracking any additional taxes owed in the event of an error by the preparer.

Private Sector Companies We Interviewed Contract Various Services

Banks, securities firms, telecommunication companies, and tax preparation entities we interviewed all contracted out services, such as administrative, information technology, and customer service functions. We found that every company we interviewed used contractors for a variety of services, ranging from maintenance functions to software development. We found the following examples:

- Officials from one bank told us that they contracted administrative functions such as financial statement processing and shipping services.

- Some banks contract out services, such as Internet banking, check imaging, telephone banking, and debit and ATM processing services.

- Officials from a securities firm told us that they contracted with software data vendors for the development and maintenance of specific data products.

- Tax preparation representatives told us that some individual tax preparers may contract with or use electronic return originators (ERO's).[9]

- Some financial sector regulators and industry representatives had conducted surveys to determine the types of services being contracted by the financial services industry. In 2004, economists from the Federal Reserve Bank of Kansas City, Missouri, found that certain types of banks relied on third-party vendors to provide an array of services, such as electronic banking and payment processing.[10] In addition, NYSE and NASD conducted a joint survey in 2004 of a select number of their members. The survey revealed that some of their member firms routinely contracted out accounting, finance, administrative, and information technology functions. NASD has specific restrictions that prohibit its members from contracting certain functions, such as supervisory and compliance activities.

Private Sector Companies We Interviewed Only Share SSNs with Contractors for Limited Purposes

Banking, investment, telecommunication, and tax preparation officials we interviewed said that they share SSNs with their contractors only for limited purposes and even then, only when it is necessary or unavoidable. In general, most of the financial services companies we spoke to said they shared SSNs with contractors to assist with services involving

- employee background checks,
- debt collections,
- fraud prevention,
- accessing credit reports, and
- information technology, such as data management.

[9]EROs are individuals or companies that can file and transmit tax returns to the IRS on behalf of individual preparers. However, ERO's generally do not prepare the return.

[10]Federal Reserve Bank of Kansas City, "Technology Outsourcing: A Community Bank Perspective." *Financial Industry Perspectives* (Fourth Quarter 2004).

Officials from one securities firm said that they shared SSNs with their contractors who assisted them in complying with federal customer identification requirements. For example, some financial services company officials told us that they used service providers to cross-reference potential customers against a government-provided "watch list" of known terrorists, suspected terrorists, and individuals being investigated for possible suspicious activity. Some large financial service provider officials also told us that in most cases their client only granted them access to SSNs in those instances where they believed SSNs were needed, such as when servicing their clients' accounts or storing data.

Telecommunication and tax preparation companies we interviewed also shared SSNs for limited purposes. Telecommunication companies generally shared SSNs with contractors for services, such as customer/client contact centers, debt collection, and data storage functions.[11] For example, officials from one telecommunication company told us that they shared SSNs and other personally identifiable information with their contracted customer contact center. The company shared their customers' account information, including SSNs, with contact center employees so that the contracted employees could authenticate, identify, and service their customers' accounts. However, company officials said that these employees could only access account holder information needed to fulfill specific requests and SSNs were not needed for some types of requests. According to tax industry representatives, tax preparation companies shared SSNs with their contractors primarily for administrative and data management functions. For example, one tax preparation company told us that their contractors had access to their customers' SSNs for services involving data analysis and preparation of reports for internal company use, tracking, and processing of customer services and archiving and storage of tax return data.

Company officials we spoke to from all industries told us that they are cautious about providing third party contractors access to their customers' personal information, including SSNs. In many cases, company officials cited multiple risk factors that could result if their customer's sensitive data were exposed by their service providers, such as compliance and

[11]A customer contact center services a company's customers by providing a focused customer service orientation for priority requirements. For example, some customer contact centers provide immediate access to worldwide customers and customer service representatives 24 hours a day, 7 days a week for all supply and logistics problems and concerns.

reputation risks.[12] For example, in the last year, several large banks experienced data security breaches in which their customers' personally identifiable information, including SSNs, was compromised, exposing individuals' information to potential misuse. Many company officials said that in order to reduce such risks, they consider multiple financial and operational factors before sharing sensitive data, such as SSNs, with their contractors. For example, bank officials from one bank told us that they request the financial statements of their prospective service providers to ensure that each service provider is financially sound.

Private Sector Companies We Interviewed Have Established Safeguards to Protect SSNs

The private sector companies we contacted provided us with standard contract forms they use in contracting with service providers to safeguard customers' personal information, such as SSNs, from misuse. In general, the types of provisions these companies included in their standard contract forms included electronic and physical data protections, audit rights, data breach notifications, subcontractor restrictions, and data handling and disposal requirements. We found that most of the companies we interviewed had established some type of due diligence or credentialing process to verify the reliability of potential contractors prior to and during contract negotiations. Furthermore, we found that some industry associations have voluntarily developed guidance for their members regarding the sharing of personal information with third parties.

Provisions in Selected Service Provider Contracts Help Safeguard SSNs from Misuse

Private sector companies we contacted often included provisions in their service provider standard contract forms to safeguard customers' personal information, such as SSNs, from misuse. In general, these contract provisions included but were not limited to

- electronic and physical data protections,
- audit rights,
- subcontractor restrictions,
- data breach notifications, and
- data-handling and disposal requirements.

[12]Compliance risk is the risk to earnings or capital arising from violations of laws, rules, or regulations or from nonconformance with internal policies and procedures or ethical standards. Reputation risk is the risk to earnings or capital arising from negative public opinion.

While company officials told us that the extent to which they included safeguard provisions varied with the type of service being contracted, most said that they included the above safeguard provisions when sharing personally identifiable information, including SSNs, with their contractors. To verify these claims, we asked each company to provide us with copies of their standard information security contract provisions and any other policies and procedures associated with such agreements.[13] Our review of the standard contract forms and the associated documentation for 10 companies found that they included most of the above safeguard provisions, but the level of specificity of the safeguard provisions varied across company contracts. For example, each standard contract form we reviewed included provisions requiring contractors to establish both electronic and physical information security safeguards.[14] However, in many cases, the standard contract form did not require the contractor to implement a specific type of electronic or physical safeguard, but only made reference to employing overall administrative, technical, and physical safeguards to prevent the unauthorized use or disclosure of their customers' personal information, such as the SSN. Some company officials told us that the information security safeguard provisions were intentionally vague to provide the contractor with flexibility in instituting such electronic and physical safeguards. However, we found that one large service provider included specific security controls in its standard contract form, which ranged from physical seals and alarms on their data centers' exterior windows to the prohibition of printers on computer terminals with access to sensitive data.

Almost all of the 10 standard contract forms we reviewed also granted companies the right to audit their service providers with notice, which is

[13]Although the majority of the companies we met with agreed to provide us with this documentation, only 10 of the companies subsequently provided it. Furthermore, some of the companies that did provide us with their contracts only supplied us with excerpts of their contracts pertaining to information security and privacy.

[14]In general, electronic safeguards restrict access to system resources and involve effective control mechanisms that can limit access to key information system assets. Physical safeguards include protections from risks, such as physical penetration by malicious or unauthorized people through the use of detection devices like alarms and surveillance cameras or damage resulting from environmental contaminants, such as fire or water.

consistent with industry standards.[15] For example, one tax preparation company's standard contract provisions stated that the company had the right to audit or independently evaluate any security processes or controls, but would only exercise such rights in a manner that limited unnecessary interference in the contractor's operations. In addition, most company standard contract forms required service providers to obtain written consent from the client company before employing a subcontractor to conduct any service on the company's behalf. Some industry sector officials told us that their standard contract forms contain provisions that explicitly require subcontractors to comply with the same safeguard requirements that the original contractor was required to follow. However, some company officials in the securities industry stated that their subcontractors are rarely granted access to consumer information, such as SSNs.

Most of the standard contract forms we reviewed also included security breach notification provisions, which typically required the contractor to notify the company in the event of any information security breach. Also, the contract language varied on the type of information that would prompt a notification and the degree to which a contractor should be involved in rectifying such a breach across industries. For example, officials from one of the banks we spoke to told us that their company required their contractors to notify them within 24 hours of any security breach or suspicious behavior, and they provided their contractors with a 24 hour telephone hotline. We were also told by most industry officials that any action taken against the contractor would depend on the extent of the breach, although in most cases, these companies had established some form of initial response program to address such breaches. However, we only found that the financial services companies had included provisions in their standard contract forms specifically outlining their response program.

Finally, we also identified companies that included data-handling and disposal requirements provisions in their standard contract forms. In these cases, the companies included general language restricting the use and disclosure of personal information to only those parties involved in

[15]According to some industry standards, companies should retain the right to audit their service providers' general controls environment, implementation of certain policies, adherence to customer-specific processing policies, adherence to security and customer-information requirements, and adherence to procedures associated with the relationships with the company.

executing the contracted service. For example, one large bank's standard contract form stated that the contractor had no legal right to access, receive, accept, transmit, or store any of its confidential information for any purpose not related to fulfilling the contract unless it was granted such rights by the bank.

Selected Companies Follow a Common Process in Selecting Contractors but Monitoring of Contractors Varies

The private sector companies we contacted spoke of similar processes for acquiring and negotiating services with potential contractors. Some company officials said that before services were contracted, they conducted some form of due diligence that is part of the overall contracting process and may include on-site visits and reviews of security policies. In addition, the due diligence phase may also include reviewing financial and independent audit statements or reports, in an effort to shed light on how contractors handle consumer data.

We found that the most sophisticated due diligence among the four industries, was the multi-tiered, risk-based process used by the companies in both the banking and securities industries. Officials from two banks told us that their due diligence practices include administering questionnaires to ascertain the amount of consumer data needed by the contractor to perform their duties. After reviewing the contractor's responses, these banks used their risk based classification system to assign a priority rating to indicate the level of information to which a contractor will have access—the higher the priority rating, the more personal information the contractor is cleared to use. Officials from one bank said they were in the process of developing a system to share the information obtained through the due diligence process with other banks. Bank officials said this collaboration effort is designed to minimize the disruption contractors' face when their potential clients review them.

Unlike the common process for selecting contractors, we found that performance review and monitoring practices for contractors varied across companies. Two companies, from the banking and tax preparation sectors, stated that they use risk-based audit systems. This means that "high risk" contractors—which include contractors that have access to SSNs—are audited more frequently than those that are lower risk. However, a few other companies stated that they periodically audit contractors, although the impetus for the audit is not based on degree of access the contractors have to SSNs, but on other factors such as the size of the contractor. One company in particular told us that it frequently engages in spontaneous audits of its contractors when they sense something is awry with the data-sharing relationship.

Some Industry Associations Provide Outsourcing Guidance, and Safeguards Used Are Generally Consistent with Established Practices for Safeguarding Information

The banking and securities firms we met with relied on established industry practices and international standards in developing contract terms and safeguards. According to officials in this sector, one of the foremost sources of guidance is from an industry-led consortium consisting of 100 of the largest financial institutions known as BITS.[16] Among other things, this consortium has developed a framework for developing and managing outsourced relationships. The framework consists of nine sections and addresses topics such as: (1) governing the practice of outsourcing consumer information through information technology, (2) developing due diligence considerations and, (3) contractual, service level and insurance considerations.

Financial companies also mentioned an international standard for information security—ISO 17799—that identifies 10 security controls used in a range of situations when exchanging consumer information through information systems. For example, this standard handles scenarios such as allowing access for traveling data users, as well as those users in remote locations, to authenticating users and passwords. Additionally, the banking sector has established a financial services roundtable which discusses a range of topics including privacy issues related to protecting consumer information. Bank officials told us that two of their specific efforts are to develop identity theft assistance and establish shared assessment centers in conjunction with BITS. The shared assessment center provides members with information about contractors based on their practices for security and privacy.

The telecommunications and tax preparation industries have not developed guidance similar to that developed by BITS. According to officials at a large telecommunications company, though, their contractors are expected to abide by accepted industry practices. However, these practices were not specified in the standard contract form for this company. An official with the National Association of Tax Preparers (NATP) said that, given the many types of tax preparers, such as certified

[16]BITS is a nonprofit, CEO-driven industry consortium whose members are 100 of the largest financial institutions, which includes banks and securities firms, in the United States. BITS was formed by the CEOs of these institutions to address issues in financial services, technology and commerce. BITS also facilitates cooperation between the financial services industry and other sectors of the nation's critical infrastructure, government organizations, technology providers, and third-party service providers. At its inception, BITS stood for "Banking Industry Technology Secretariat." However, with financial modernization and the emergence of integrated financial services companies involving insurance, securities and banking, that term is no longer used.

public accountants, enrolled agents, individual practitioners, attorneys and financial planners, establishing specific guidance on sharing consumer data would not be worthwhile.

However, in 2004, the American Institute of Certified Public Accountants (AICPA) issued a ruling for its members clarifying their responsibilities to their clients when using third party contractors, including offshore providers. This action was prompted by congressional and regulatory concerns about the outsourcing of tax preparation work and maintaining the confidentiality of personal financial information that is provided to contractors, especially those in other countries. The ruling applies to all client services in addition to tax preparation and requires members to take the following steps:

- Inform clients, preferably in writing, that the tax preparer may use an outside contractor in providing services to the client and share client information with that contractor. Members are not required to provide this notification if a contractor is only used for administrative support services such as record storage or authorized e-file tax transmittal services.

- Provide adequate oversight of all services performed by the contractor and adequately plan and supervise the services provided by the contractor. The ruling does not elaborate on what is adequate as it may vary depending on the nature of the service provided.

- Enter into a contractual agreement requiring the contractor to maintain the confidentiality of clients' information and be reasonably assured the contractor has appropriate procedures in place to prevent the unauthorized release of confidential client information. This provision applies to contractors that provide administrative support and professional services and does not require the member to obtain specific consent from the client to share information with the contractor.

In our review, we found that information security policies and procedures of the companies we contacted were generally consistent with established industry practices for maintaining the confidentiality of personal information. For example, 12 of the companies we interviewed had incorporated or told us that they had provisions in their contracts restricting their subcontractor's access and use of consumer information, such as SSNs. In addition company documents included other types of safeguards that are consistent with considered established practices we

identified such as confidentiality provisions, information disposal requirements, audit rights, data security breach procedures, and physical safeguards. In addition, several company officials from the financial sector said that they also relied on these established industry standards when developing their internal policies and procedures, although we could not determine the extent to which the companies had actually incorporated these established practices.

Federal Regulation and Oversight of SSN Sharing Varies Widely Among the Industries We Reviewed

Federal regulation and oversight of SSN sharing varies across the four industries we reviewed, revealing gaps in the federal law and oversight in different industries that share SSNs with their contractors. Federal law and oversight of the sharing of personal information in the financial services industry is very extensive: Financial services companies must comply with GLBA requirements for safeguarding customer's personal information, and regulators have an examination process in place that includes determining whether banks and securities firms are safeguarding this information. Oversight in the tax preparation and telecommunications industries' sharing of SSNs is not as comprehensive as it is in the financial services industry. IRS has regulations and guidance in place to restrict the disclosure of SSNs by tax preparers and their contractors, but does not perform periodic reviews of tax preparers' compliance. Because it believes that it lacks statutory authority to do so, FCC has not issued regulations covering SSNs and also does not periodically review telecommunications companies to determine whether they are safeguarding such information.

Federal Oversight in the Financial Services Sector Is Extensive

In the financial services sector, banks and securities firms, among others, must comply with the provisions of GLBA to establish safeguards that protect the confidentiality of nonpublic personal information about their customers or clients. GLBA generally permits banks to share customers' personal information with contractors without the customers' permission, provided that the bank fully discloses it is doing so and enters into a contract requiring the contractor to maintain the confidentiality of the information.[17] Through periodic bank and securities firm examinations, the federal agencies with oversight responsibility for these entities review their compliance with the agencies' GLBA and other regulations.

[17]Banks may share customers' nonpublic personal information without their permission under other limited circumstances. See 15 U.S.C. § 6802(b) and (e).

Bank Regulatory Agencies Monitor Compliance with GLBA through Regulations and Examinations for Compliance

The federal bank supervisory agencies jointly issued guidelines to implement the GLBA safeguarding requirements.[18] These guidelines require banks to establish information security programs that include using due diligence in selecting contractors, requiring contractors to take steps to meet the safeguard standards, and, in certain situations, monitoring contractors to confirm that they are meeting the safeguard requirements. The three agencies base portions of their examinations and supervisory practices on these guidelines. The FFIEC has also issued guidance outlining the following four steps banks should follow in establishing contractual relationships with technology service providers:

- Conduct appropriate risk assessments.
- Maintain adequate due diligence procedures.
- Closely evaluate all contracts to ensure necessary provisions for assuring security and confidentiality are included.
- Establish ongoing monitoring and oversight procedures.

These steps are also incorporated into FFIEC's examination procedures manual for reviewing technology service providers. Appendix II describes these steps in more detail.

The bank regulatory agencies conduct periodic examinations in which compliance with GLBA and the guidance for sharing information with contractors are assessed. The frequency of examinations at a particular bank depends on a series of risk assessments. For example, OCC examiners we met with said that, in general, the more a bank shares nonpublic personal information (as defined by GLBA) with contractors, the greater its risk potential is, and therefore, the more scrutiny information security will receive.

OCC performs targeted examinations that focus on specific subjects along with ongoing supervision activities to assess the banks' overall operations and performance.[19] Information security, contractor management, and compliance with GLBA and other privacy laws are among the targeted

[18]66 Fed. Reg. 8616 (Feb.1, 2001).

[19]Based on our discussions with the OCC examiners for these banks and our review of related documentation, the process of ongoing supervision starts with development of an annual examination strategy outlining subjects for targeted examinations to be undertaken that year. The strategy also outlines ongoing large bank supervision activities such as holding regular meetings with bank officials and reviewing internal and management reports. OCC also has a separate supervisory program for community banks.

examinations that have been conducted or planned at the three banks we met with. The targeted examinations can also include reviews of offshore contractors. One such examination was aimed exclusively at reviewing risk management practices and controls of the banks' contractor management unit in India. FDIC and FRB also conduct examinations of state-chartered banks and bank holding companies in which two regulators also assess information security, contractor management, and GLBA compliance.[20] We reviewed examination reports and related workpapers for three large national banks supervised by OCC that we met with. Our review of the examination reports found that they draw overall conclusions on whether the bank is satisfactorily meeting both OCC's requirements for complying with GLBA and its guidance for sharing sensitive information with contractors and then the reports discuss any areas of weakness in detail. When there are findings that require corrective action by bank management, the examiners will report these as matters requiring attention.[21] In some instances, concerns were raised about banks consistently implementing their information security policies among all their business units; however, the reports indicate that the banks' management is addressing these issues.

Certain bank contractors are also examined periodically under the purview of the FFIEC, using examiners from all FFIEC member agencies. These bank service contractors—referred to as technology service providers—often have access to sensitive personal information. We reviewed 66 bank contractor examination reports and found the examinations addressed information security issues including GLBA compliance, the sufficiency of both internal and independent IT audits, the adequacy of system controls and written policies and procedures, and the use of or need for risk and vulnerability assessments.[22] About two thirds of the examination reports concluded that the service providers' overall information security is satisfactory but make recommendations for specific improvements. Some of the examinations focused on GLBA

[20]We did not review FDIC or FRB examination reports because banks they supervise were not included in the scope of our review.

[21]These are typically requirements to improve such things as clarifying contractor management roles and responsibilities in the bank's organization, formalizing strategic planning for contractor management, or adding components to employee training programs.

[22]Because this sample was not representative, our findings cannot be generalized. We reviewed the most recent examination reports for 16 large national service providers and any others that were available electronically.

compliance, and examiners recommended improvements that contractors could make to their internal processes to better ensure they are complying with GLBA.

SEC and Self-Regulatory Agencies Also Use Examinations to Oversee Requirements for Safeguarding Sensitive Customer Information

Securities firms are also required to meet the GLBA standards for safeguarding customer's personal information. To implement GLBA, SEC issued regulation S-P, which applies to the financial institutions subject to SEC's jurisdiction under GLBA—investment advisors registered with SEC, investment companies and broker-dealers.[23] Regulation S-P directs these securities firms to adopt policies and procedures that are reasonably designed to

- insure the security and confidentiality of customer records and information,
- protect against anticipated threats or hazards to the security and integrity to customer records and information, and
- protect against unauthorized access to or use of customer records and information that could bring substantial harm or inconvenience to any customer.

Under Regulation S-P, securities firms, similar to banks, generally may share customers' personal information with contractors without customers' permission, provided that the firms notify customers they are doing so, and prohibit contractors, through the terms of the contract, from disclosing or using the information for any purposes other than those for which the information was provided.[24]

SEC's Office of Compliance, Inspections, and Examinations (OCIE) conducts periodic exams of securities firms that include compliance with Regulation S-P. OCIE uses a risk assessment framework to target firms for examination. Any known concerns or questions about a firm's practices for protecting customer information are among the components factored into the risk assessment. OCIE's examination process covers such steps in the contract management process as due diligence in selecting contractors, contract provisions for protecting information privacy, and monitoring compliance with the contract terms including the use of audits

[23]17 C.F.R. Part 248.

[24]Securities firms may share customers' nonpublic personal information without their permission under other limited circumstances. See 17 C.F.R. § 248.14 and § 248.15.

or other reviews of contractors' procedures and performance.[25] Examiners are also expected to obtain and review certain documents in addition to the contracts, such as any relating to specific security controls. Although the bank regulatory agencies have authority to examine contractors, SEC officials told us that they cannot examine contractors unless they happen to be another securities firm.

In addition to its ongoing examinations, OCIE initiated two examination sweeps focused solely on firms' protection of personal information. The first—performed during 2002 and 2003—focused on large securities firms policies and procedures for preventing identity theft. The examinations reviewed how well they complied with the safeguarding requirements and also scrutinized the firms' vendor management processes to see if they were designed to ensure compliance with the safeguarding requirements. These examinations found that, while the firms were generally in compliance, some were confused about specific things they needed to do to meet the requirements. In the fall of 2005, OCIE began the second sweep—examining the outsourcing practices of securities firms. OCIE plans to conduct these examinations with NYSE at a small number of firms selected to be as representative of the industry as possible. According to the procedures developed by OCIE, the examinations will be very detailed and explore what specific measures have been taken by firms in the areas of:

- Due diligence in selecting contractors;
- Adequacy of privacy and security provisions in the contracts;
- Contractors' policies and procedures for safeguarding customer information;
- Oversight and monitoring for compliance with the contract terms, including offshore contractors' ability to comply with applicable U.S. information privacy laws.

After completing this program, OCIE plans to incorporate the procedures for examining outsourcing activities into its regular examinations.

[25]The International Organization of Securities Commissions (IOSCO) and the Joint Forum (established under the aegis of the Basel Committee on Banking Supervision, the International Association of Insurance Supervisors and IOSCO) have issued guidance on the principles of outsourcing in financial services. SEC is a member of both of these organizations and, according to agency officials, participated in the process by which these organizations issued this guidance. SEC does not currently contemplate developing a separate advisory guidance for securities firms to follow in using outside contractors.

NASD and NYSE have issued their own guidance on safeguarding customer information. NASD has issued guidance outlining procedures and safeguards for sharing customer information with contractors, and overseeing compliance with any applicable securities laws and NASD rules.[26] In response to concerns about the growing use of contractors in the securities industry, NYSE has proposed a similar rule governing its members' use of contractors, which will require member firms to follow certain steps in selecting and overseeing contractors.

NASD and NYSE also examine member firms to ensure compliance with Regulation S-P. However, similar to SEC, neither SRO has the authority to examine or review contractors that are not member firms. NASD officials said a Regulation S-P review will be included in an examination if their examiners believe there is a Regulation S-P compliance or information security issue at a member firm. They added that the examiners review the firm's procedures and internal controls for monitoring contractors and review each contract to ensure it includes clauses protecting the confidentiality of customer information and barring the contractor from using it for purposes not related to the contracted service.[27] NYSE examinations review third-party contracts to ensure that they contain confidentiality clauses prohibiting the contractor from using or disclosing customer information for any use other than the purposes the contractor was provided the information. We reviewed 10 NYSE examination reports, documenting each instance of noncompliance with Regulation S-P found by NYSE examiners since January 2003. We found several cases where the examiners found that third party contracts did not contain the necessary confidentiality clauses.

[26]NASD Notice to Members 05-49, Safeguarding Confidential Customer Information (July, 2005).

[27]NASD took one enforcement action in 2005 for a Regulation S-P violation, but the action did not involve contractors' safeguarding of customer information.

Tax Preparers Must Follow IRS and FTC Information Nondisclosure Requirements, but IRS Has No Process for Routinely Monitoring Compliance

Tax return preparers are required to protect the confidentiality of taxpayer information under IRS provisions and FTC's GLBA regulations. Under Sections 6713 and 7216 of IRC and IRS regulations, tax return preparers may, under certain circumstances, disclose tax information to other tax preparers, including contractors, or to other employees of the tax preparers' firm. Tax return preparers and contractors who provide certain services in connection with the preparation of tax returns—including contractors used in preparing and processing electronic tax returns-—are required to protect the confidentiality of taxpayer information, and they may be subject to civil and criminal penalties for the unauthorized use or disclosure of tax return information, including SSNs.[28]

Tax return preparers must also follow FTC's GLBA regulations for maintaining the security and confidentiality of customer information. Among other protective measures, FTC's GLBA regulations state that entities such as tax return preparers may use contractors and provide customers' information to those contractors, but only if certain conditions are fulfilled. Thus, in the case of tax return preparers, the preparer must provide its customers with initial notice of its privacy policies and practices before it shares sensitive information with contractors, and contracts the tax return preparer enters into with its contractors must prohibit the contractors from disclosing or using customers' tax return information for any purposes other than those for which the information was provided. FTC's GLBA regulations also specify that entities such as tax return preparers oversee their contractors by (1) taking reasonable steps to select and retain service providers that can maintain appropriate safeguards for the customer information being shared and (2) requiring provisions in the contracts to implement and maintain these safeguards.

Unlike the bank regulatory agencies and SEC, IRS does not conduct periodic examinations of tax preparers. IRS monitors and oversees tax preparers, including how well they safeguard taxpayer information, by investigating complaints, which may come from clients or referrals from local IRS offices. IRS officials said the agency has plans to start conducting more self-initiated reviews of a sample of tax preparers but the agency has limited resources for this effort. IRS also performs background

[28]In 2000, IRS issued clarifying guidance that stated that contractors used in preparing and processing electronic tax returns are also considered tax return preparers and are therefore covered by Sections 6713 and 7216 of IRC. Revenue Procedure 2000-31. This guidance was updated and superseded in August 2005. Revenue Procedure 2005-60.

checks of applicants who provide electronic return services and plans to review a sample of Electronic Return Originators each year.

During the course of our work we found that some IRS and professional association officials were concerned that IRS regulations did not adequately cover tax return preparers who submit taxpayer returns electronically. For example, officials from a professional association for tax return preparers said there were no explicit provisions restricting what various third party providers participating in electronic filing could do with taxpayer information once they possess it. In response to this concern, however, IRS officials stated that any participant in its e-file program performing any role that handles tax return data is covered by IRC 7216.[29] IRS has also recently issued proposed regulations intended to, among other things, clarify that the rules also apply to tax return preparers who submit taxpayer returns electronically.[30] The proposed regulations also clarify that a tax return preparer may disclose tax return information to another tax return preparer located in the United States, including a contractor, without the taxpayer's consent under certain conditions.[31] They also provide that contractors, under certain circumstances, are subject to criminal penalties for unauthorized use or disclosure of tax return information. In addition, the proposed regulations contain a new provision that states that disclosure of tax information may be made to certain types of contractors, but only if the tax return preparer ensures that all individuals who are to receive tax information receive written notice that criminal penalties for improper disclosure apply to them.

No Federal Law Requires Safeguards for SSNs Collected or Shared by the Telecommunications Industry

FCC officials told us that they know of no federal law that restricts the sharing of SSNs by telecommunications firms with their contractors and that they do not regulate or oversee the privacy of customer information maintained or shared by telecommunications firms unless the information is included in customer proprietary network information (CPNI). The Telecommunications Act of 1996 restricts the use and disclosure of CPNI, which is defined as information relating to the quantity, technical configuration, type, destinations, location and amount of use of a

[29]Revenue Procedure 2005-60, Section 6.01.

[30]70 Fed. Reg. 72954 (Dec. 8, 2005).

[31]Such conditions include for the purposes of preparing or assisting in the preparation of a tax return so long as the contractor does not make any substantive determinations or provide advice affecting the taxpayer's tax liability.

telecommunications service subscribed to, and information contained in the bills pertaining to telephone service received by a customer. Currently, the act does not include SSNs in its definition of CPNI. Agency officials also stated that FCC has enacted regulations governing disclosure of CPNI (but not SSNs) to certain types of third parties.[32]

Although FCC has authority to take enforcement action against telecommunications companies for inappropriate use and disclosure of CPNI, the limited definition of CPNI precludes FCC from taking enforcement action when SSNs are used or disclosed. It also has no authority to oversee the use of contractors by telecommunications firms other than its authority to oversee compliance with its regulations affecting the sharing of CPNI. Agency officials told us FCC is considering a request by the Federal Bureau of Investigation to regulate foreign storage of CPNI and foreign-based access to CPNI based on national security and law enforcement concerns.

Despite FCC's lack of authority with regard to SSNs being shared by telecommunications companies, under certain circumstances, FTC may be able to take action against telecommunications companies for improperly sharing SSNs. An FTC staff member and representatives from the telecommunications companies we met with said that under Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive business practices, FTC may be able to take action against companies that fail to meet the terms of their own privacy policies in certain circumstances.[33] For example, if a telecommunications company stated in its privacy policy that it would only share a consumer's personal information with contractors for certain purposes and a contractor used the SSNs for a purpose not covered by the privacy policy, FTC could consider this a deceptive business practice. However, according to FTC, no actions have been taken against telecommunications carriers under Section 5 because of a failure to comply with statements made in their privacy policies about information shared with contractors.

[32]47 C.F.R. § 64.2007(b)(2).

[33]FTC action is limited to the extent that a company's activities are covered by the common carrier exemption in Section 4 of the Federal Trade Commission Act (15 U.S.C. § 44). Telecommunications companies are also not considered to be financial institutions under GLBA and therefore, not subject to GLBA's safeguard requirements.

State Laws Also Affect the Disclosure and Sharing of SSNs with Third Parties

Company officials informed us of laws in 15 states they believe either affect how they share sensitive personal information including SSNs with their contractors or limit both their own and their contractors use and handling of this information. The laws cover areas such as limiting the use and display of SSNs, specifying record disposal requirements, prohibiting requiring SSNs to complete a business transaction, privacy policy provisions, and security breach notification requirements.[34]

A few of the company officials we spoke to said that California's privacy laws were particularly significant to the development of their information confidentiality and security policies. As a result, many told us that their companies have adapted the requirements of the California laws for companywide application. The California law that most directly affects how businesses can share personal information with their contractors was enacted in September 2004 and requires that businesses incorporate provisions to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, disclosure, use, modification, or destruction into their contracts with third party service providers.[35] This law identifies SSNs, when used in conjunction with customer names, as one of several forms of personal information covered. Some company officials also said California's security breach notification statute significantly affected their information security and confidentiality procedures. These officials also told us this statute was the impetus for formulating their own breach notification requirements and procedures.

Company officials in each of the industry sectors said that they will incorporate the requirements of state laws they believe affect how they share sensitive personal information into their company's security and confidentiality policies or operations, effectively applying them to all states they do business in. For example, officials from one company told us it is more efficient to apply these state requirements nationwide than to design systems for specific states.

[34]We found some instances in which the laws cited either did not affect the industries we reviewed or did not apply to the sharing of personal information. We did not include these in our analysis.

[35]California Civil Code 1798.81.5(c).

Conclusions

With millions of Americans at risk of identity theft, it is vital that any entity with access to personal information, especially to SSNs, take every precaution to protect this information from misuse. Inadequate database security and improper handling, disposal, and sharing of such personal information creates vulnerability to identity theft, with its attendant costs to individuals and businesses.

Officials from each of the industries we met with clearly felt that safeguarding SSNs and other personal information was very important and had taken steps to do so. However, as we found in the telecommunications sector, companies are not always required to include in their service-provider contracts provisions that would safeguard SSNs. Gaps in existing federal law or agency oversight, such as what we found in the industries we looked at, do not provide incentives for companies to commit to protecting personal information. Each industry is subject to different federal oversight and is often left to decide what established practices for safeguarding SSNs and other consumer information it wishes to follow. Federal action to strengthen safeguards for SSNs that companies in non-financial service industries collect could avert disclosures of this important personal information and better protect Americans from the cost and inconvenience of identity theft.

Matter for Congressional Consideration

We recommend that Congress consider possible options for addressing the gaps in existing federal requirements for safeguarding SSNs shared with contractors. One approach would be to require industry-specific protections for the sharing of SSNs with contractors where such measures are not already in place. For example, Congress could consider whether the Telecommunications Act of 1996 should be amended to address how that industry shares SSNs with contractors.

Alternatively, Congress could take a broader approach. For example, in considering proposed legislation that would generally restrict the use and display of SSNs, Congress could also include a provision that would explicitly apply this restriction to third party contractors. With either approach, Congress will also want to establish a mechanism for overseeing compliance by contractors and enforcement.

Agency Comments

We requested comments on a draft of this report from FCC, FDIC, the Federal Reserve Board, FTC, IRS, OCC, and SEC. None of the agencies provided formal, written comments. With the exception of FDIC, all

provided technical, editorial, and other clarifying comments which we incorporated in the report as appropriate.

We are sending copies of this report to the Secretary of the Treasury, the Chairmen of the Federal Reserve Board, FDIC, FTC, FCC, SEC, the Office of the Comptroller of the Currency, the Commissioner of the IRS, and other interested parties. Copies will also be made available at no charge on GAO's Web site at http://www.gao.gov. If you have questions concerning this report, please call me on (202) 512-7215. Key contributors to this report are listed in appendix VI.

Director, Education, Workforce,
and Income Security

Appendix I: Scope and Methodology

In this report, we focused on the uses and protections of SSNs when they are shared with contractors and subcontractors within the financial services, telecommunications, and tax preparation industries. To describe the types of services that companies in these industry sectors contract, we identified and interviewed company officials in the banking, securities, telecommunication, and tax preparation industries. We selected these industries because they collect large volumes of personal information including SSNs and experts in the fields of outsourcing and information security we interviewed believed these industries were among the most likely to share SSNs with contractors. We contacted 17 of the largest companies, based on asset size, from each of the industry sectors. We also contacted seven large service providers—companies whose sole business is to provide services to other businesses under contract.[1] Based on the response to our request, we conducted structured interviews with a total of 17 of these companies—3 banks, 4 securities firms, 4 telecommunication companies, 1 tax preparation company, and 5 service providers—regarding the types of services they contracted and whether SSNs were shared between the companies and contractors. The remaining seven companies did not respond to our request. Furthermore, we conducted structured interviews with six industry associations. These included three associations that represented enrolled agents and tax professionals within the tax preparation industry. We contacted these to obtain more perspectives from the tax preparation industry since only one tax preparation firm agreed to meet with us. However, we were unable to determine the extent to which some of the member's responses were representative of associations with similar membership. Our interviews with the companies and industry associations are not statistically representative of either their industries or the business sector as a whole, and therefore should not be considered to represent the views of the sectors as a whole. In addition, we also reviewed academic and consultant's studies, a professional trade associations' outsourcing survey, self-regulatory organizations' research, and bank examinations to determine the types of services that companies from the different industry sectors commonly contracted.

[1]We selected the companies we interviewed in the banking, securities and telecommunications industries from industry sector rankings for the 2004 Fortune 500 list of the largest American companies. However, these listings could not be used to select tax preparation firms, because too few were included. We identified other tax preparation firms from information compiled by professional and industry associations. In addition, we selected service providers to contact based on our discussions with company and government officials and published information about large bank service providers.

To identify company safeguards to protect SSNs during the contracting process, we conducted structured interviews with company officials from each industry to gain a better understanding of their safeguards and the stages of the contracting process. We requested copies of standard contract forms from each of the companies. Ten companies provided copies to us. We reviewed the forms to identify specific provisions that addressed the security and confidentiality of personal information. We also obtained and reviewed internal security policies and procedures from companies willing to provide them and compared these security measures across the different industry sectors. We did not verify the extent to which these businesses complied with their own policies, procedures, and safeguards. Finally, we contacted these industries' trade associations to identify any best practices or notable industry practices for the safeguarding of customer's personally identifiable information. Because of the sensitive nature of the information we were obtaining, we agreed not to identify the companies in our report and to treat any information they provided, including their standard contract forms, as proprietary.

To identify how federal agencies regulate and monitor the sharing and safeguarding of SSNs and other personal information between entities they oversee and their contractors, we interviewed agency officials and reviewed documents from the following agencies with jurisdiction over the four industry sectors in our review

- Federal Deposit Insurance Corporation,
- Federal Reserve System,
- Office of the Comptroller of the Currency,
- Federal Financial Institutions Examination Council,
- Federal Trade Commission,
- Federal Communications Commission,
- Internal Revenue Service, and
- Securities and Exchange Commission.

We also met with officials from self-regulatory agencies-—the New York Stock Exchange and the National Association of Securities Dealers—and reviewed documents they prepared.

Documents we obtained and reviewed included applicable statutes, regulations, guidance to regulated entities, examination manuals and related materials, examination reports and related workpapers, survey reports, and any other related materials. We limited our review to identifying steps and procedures the agencies follow in overseeing compliance with federal requirements for safeguarding personal

information. We did not assess the adequacy or effectiveness of their oversight and enforcement measures.

For bank examination reports, we limited our analysis to reviewing those for the three banks we met with. Our purpose was to, in general, identify what the examinations covered, if they followed OCC's examination procedures, and the types of issues they found. We reviewed only those reports relating to GLBA, information security, or contractor management that were issued since 2002. In addition, we reviewed the most recent examination report for 66 contractors. Most of the reports are maintained in the regional or field offices of the bank regulatory agency that had lead responsibility for the exam. Examination reports for 16 multi-regional service providers—which FFIEC classifies separately—are maintained in FFIEC headquarters. Because of this dispersion, we requested the reports for the 16 multi-regional service providers and any other reports that were available electronically—which were the remaining 50. As a result, our sample of both the bank and contractor examination reports is not representative, and our findings from them cannot be generalized.

In order to ensure we obtained complete information from the federal agencies, we also asked the companies we interviewed to tell us the federal requirements for protecting personal information they were responsible for complying with and compared their responses with what we obtained from the agencies.

Appendix II: Summary of Federal Bank Supervisory Agency Guidance on Contracting with Technology Service Providers

- **Conduct appropriate risk assessments**. When considering contracting out a particular activity, banks should evaluate factors such as the strategic goals, objectives, and business needs of the financial institution; the ability to evaluate and oversee contractual relationships; the importance and criticality of the services to the bank; defined requirements for the contracted activity; necessary controls and reporting processes; contractual obligations and requirements for the contractor; contingency plans, including availability of alternative contractors, costs and resources required to switch contractors; ongoing assessment of contractual arrangements to evaluate consistency with strategic objectives and contractor performance; and regulatory requirements and guidance for the business lines affected and technologies used.

- **Maintain adequate due diligence procedures**. Banks should evaluate prospective contractors to determine their ability, both operationally and financially, to meet the bank's needs, and should convey the bank's needs, objectives, and necessary controls to the prospective contractor. Some of the specific factors banks should consider in selecting contractors include their technology and industry expertise, financial condition, and operations and controls including the adequacy of their standards, policies and procedures relating to internal controls, security, privacy protections, and maintenance of records and also determining if contractors provide sufficient security precautions such as encryption and customer identity authentication.

- **Closely evaluate all contracts to ensure necessary provisions for assuring security and confidentiality are included**. Consideration should be given to including contract provisions that address control over operations. Contracts should address, among other matters, the scope of service, performance standards, security and confidentiality of the bank's information and other resources, controls, audit rights, frequency and type of reporting to the bank, and sub-contracting. Security and confidentiality provisions should include prohibiting the contractor and its agents or subcontractors from using or disclosing the bank's information except as needed to or be consistent with providing the contracted service, protecting against unauthorized use, and requiring the contractor to fully disclose security breaches that result in unauthorized intrusions that may materially affect the bank or its customers and report corrective actions taken.

- **Establish ongoing monitoring and oversight procedures.** Banks should implement an oversight program to monitor each contractor's financial conditions and operations, the quality of service and support

in fulfilling the contract, contract compliance and revision needs, and maintenance of business resumption contingency plans.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Barbara D. Bovbjerg, Director, (202) 512-7215

Staff Acknowledgments

The following team members made key contributions to this report: Margaret Armen, Pat Bernard, Richard Burkard, Tamara Cross, Amber Edwards, Michele Fejfar, Jason Holsclaw, Joel Marus, Sheila McCoy, Jonathan McMurray, and Amanda Miller.

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

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER