United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Information Policy, Census and National Archives, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, June 17, 2009

IDENTITY THEFT

Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain

Statement of Daniel Bertoni, Director
Education, Workforce, and Income Security Issues

June 17, 2009

IDENTITY THEFT

Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-09-759T, a testimony before the Subcommittee on Information Policy, Census, and National Archives, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

The loss of personally identifiable information, such as an individual's Social Security number, name, and date of birth can result in serious harm, including identity theft. Identity theft is a serious crime that impacts millions of individuals each year. Identity theft occurs when such information is used without authorization to commit fraud or other crimes. While progress has been made protecting personally identifiable information in the public and private sectors, challenges remain.

GAO was asked to testify on how the loss of personally identifiable information contributes to identity theft. This testimony summarizes (1) the problem of identity theft; (2) steps taken at the federal, state, and local level to prevent potential identity theft; and (3) vulnerabilities that remain to protecting personally identifiable information, including in federal information systems.

For this testimony, GAO relied primarily on information from prior reports and testimonies that address public and private sector use of personally identifiable information, as well as federal, state, and local efforts to protect the security of such information.

GAO and agency inspectors general have made numerous recommendations to agencies to resolve prior significant information control deficiencies and information security program shortfalls. The effective implementation of these recommendations will continue to strengthen the security posture at these agencies.

To view the full product, including the scope and methodology, click on GAO-09-759T
For more information, contact Daniel Bertoni at (202) 512-5988 or bertonid@gao.gov.

What GAO Found

Identity theft is a serious problem because, among other things, it can take a long period of time before a victim becomes aware that the crime has taken place and thus can cause substantial harm to the victim's credit rating. Moreover, while some identity theft victims can resolve their problems quickly, others face substantial costs and inconvenience repairing damage to their credit records. Some individuals have lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft. Millions of people become victims of identity theft each year. The Federal Trade Commission (FTC) estimates that in 1 year, as many as 10 million people—or 4.6 percent of the U.S. adult population—discover that they are victims of some form of identity theft, translating into reported losses exceeding $50 billion.

Several steps have been taken, both in terms of legislation and administrative actions to combat identity theft at the federal, state and local levels, although efforts to assist victims of the crime once it has occurred remain somewhat piecemeal. While there is no one law that regulates the overall use of personally identifiable information by all levels and branches of government, numerous federal laws place restrictions on public and private sector entities' use and disclosure of individuals' personal information in specific instances, including the use and disclosure of Social Security Numbers (SSN)—a key piece of information that is highly valuable to identity thieves. One intention of some of these laws is to prevent the misuse of personal information for purposes such as identity theft.

Despite efforts to prevent identity theft, vulnerabilities remain and can be grouped into several areas, including display and use of Social Security numbers, availability of personal information through information resellers, security weaknesses in federal agency information systems, and data security breaches. GAO's work indicates that persistent weaknesses appear in five major categories of information system controls, including access controls which ensure that only authorized agency personnel can read, alter, or delete data. As a result, federal systems and sensitive information are at increased risk of unauthorized access and disclosure, modification, or destruction, as well as inadvertent or deliberate disruption of system operations and services. GAO has reported that federal agencies continue to experience numerous security incidents that could leave sensitive personally identifiable information in federal records vulnerable to identity theft.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the role that personally identifiable information plays in identity theft, efforts taken by governments to prevent identity theft, and vulnerabilities that remain to protecting individuals' identities. Personally identifiable information includes information that can be used to locate or identify an individual, including names, date of birth, Social Security number (SSN), biometric records, or other information that can be linked to an individual. Identity theft occurs when individuals' personal identifying information is used without authorization in an attempt to commit fraud or other crimes. Identity thieves use personally identifiable information to open new financial accounts and incur charges (such as opening credit accounts in that individual's name), to take over an individual's existing accounts to make unauthorized charges or withdraw money, or to assume another person's identity. Accordingly, my remarks today will address (1) the problem of identity theft; (2) steps taken at the federal, state, and local level, to prevent potential identity theft and assist victims of this crime; and (3) vulnerabilities that remain to protecting personally identifiable information, particularly in federal information systems.

In summary, identity theft is a serious crime that affects millions of individuals each year with costs, according to a Federal Trade Commission estimate, that exceeded $50 billion in a single year. Victims of identity theft may not realize the crime has been committed for months or years, with potential serious consequences financially, civilly, and even criminally. Once victimized, individuals may have to deal with a complex array of public and private organizations to correct the damage, often at great expense to themselves both in terms of time and money. Steps have been taken in both the public and private sectors in an attempt to prevent or detect identity theft, and where possible, assist victims. These include federal and state laws, law enforcement activities, and guidance and other assistance provided to consumers. Despite these steps, vulnerabilities remain. In particular, recent security breaches of both federal and private data sources have highlighted the challenges that remain to preventing identity theft. We and agency inspectors general have made numerous recommendations in recent years to federal agencies to resolve significant control deficiencies and information security program shortfalls. In particular, we have noted that agencies also need to implement controls that reduce the chance of incidents involving data loss or theft, computer intrusions, and privacy breaches.

For this testimony, we primarily relied on information from our prior reports and testimonies that address public and private sector use of personally identifiable information, as well as federal, state and local efforts to protect the security of such information. These products were issued from 2002 to 2009 and are listed in the related GAO products section at the end of this statement. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The growth in information technology, networking, and electronic storage has made it ever easier to collect and maintain information about individuals. An accompanying growth in incidents of loss and unauthorized use of such information has led to increased concerns about protecting this information on federal systems as well as from private-sector sources, such as data resellers that specialize in amassing personal information from multiple sources. As a result, additional laws protecting personally identifiable information collected and maintained by both government and private-sector entities have been enacted since the Privacy Act of 1974, including measures that are particularly concerned with the protection of personal data maintained in automated information systems.

Protecting personally identifiable information in federal systems, such as names, date of birth and SSNs, is critical because its loss or unauthorized disclosure can lead to serious consequences for individuals. These consequences include identity theft or other fraudulent activity, which can result in substantial harm, embarrassment, and inconvenience.

Identity Theft Is a Serious Problem

Identity theft is a serious problem because, among other things, it may take a long period of time before a victim becomes aware that the crime has taken place, and thus can cause substantial harm to the victim's credit rating. Moreover, while some identity theft victims can resolve their problems quickly, others face substantial costs and inconvenience repairing damage to their credit records. Some individuals have lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft.

Millions of people become victims of identity theft each year. The Federal Trade Commission (FTC) estimates that in 1 year, as many as 10 million people—or 4.6 percent of the U.S. adult population—discover that they are victims of some form of identity theft, translating into reported losses exceeding $50 billion. In 2007, the FTC estimated that the median value of goods and services obtained by identity thieves was $500, with 10 percent of victims reporting the thief obtained $6,000 or more. Similarly, a more recent 2008 industry survey estimated that, 9.9 million adults in the United States were victims of identity fraud.[1] While available data suggest that identity theft remains a persistent and serious problem, the FTC found that most victims of identity theft do not report the crime. Therefore, the total of number of identity thefts is unknown.

Several examples we previously identified illustrate the magnitude of the losses that could occur from a single incident and how aggregated personal information can be vulnerable to misuse:

- A help desk employee at a New York-based software company, which provided software to its clients to access consumer credit reports, stole the identities of up to 30,000 individuals by using confidential passwords and subscriber codes of the company's customers. The former employee reportedly sold these identities for $60 each. Furthermore, given the explosion of Internet use and the ease with which personally identifiable information is accessible, individuals looking to steal someone's identity are increasingly able to do so. In our work, we identified a case where an individual obtained the names and SSNs of high-ranking U.S. military officers from a public Web site and used those identities to apply online for credit cards and bank credit.[2]

- In 2006, an Ohio woman pled guilty to conspiracy, bank fraud, and aggravated identity theft as the leader of a group that stole citizens' personal identifying information from a local public record keeper's Web site and other sources, resulting in over $450,000 in losses to individuals, financial institutions, and other businesses.[3]

[1]Javelin Strategy and Research, *2009 Identity Fraud Survey Report: Consumer Version* (Pleasanton, Calif., February 2009).

[2]GAO *Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain*. GAO-05-1016T. (Washington, D.C.: September 15, 2005)

[3]*Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain.* GAO-07-752. (Washington, D.C.: June 15, 2007).

- In February 2007, an individual was convicted of aggravated identity theft, access device fraud, and conspiracy to commit bank fraud in the Eastern District of Virginia. The individual, who went by the Internet nickname "John Dillinger," was involved in extensive illegal online "carding" activities, in which he received e-mails or instant messages containing hundreds of stolen credit card numbers, usually obtained through phishing[4] schemes or network intrusions, from "vendors" who were located in Russia and Romania. In his role as a "cashier" of these stolen credit card numbers, this individual would then electronically encode these numbers to plastic bank cards, make ATM withdrawals, and return a portion to the vendors. Computers seized by authorities revealed over 4,300 compromised account numbers and full identity information (i.e., name, address, date of birth, Social Security number, and mother's maiden name) for over 1,600 individual victims.[5]

Steps Have Been Taken at the Federal, State, and Local Level to Prevent Identity Theft, Although Gaps Remain in Efforts to Assist Victims

Several steps have been taken, both in terms of legislation and administrative actions to combat identity theft at the federal, state and local levels, although efforts to assist victims of the crime once it has occurred remain somewhat piecemeal. While there is no one law that regulates the overall use of personally identifiable information by all levels and branches of government, numerous federal laws place restrictions on public and private sector entities' use and disclosure of individuals' personal information in specific instances, including the use and disclosure of SSNs—a key piece of information that is highly valuable to identity thieves. One intention of some of these laws is to prevent the misuse of personal information for purposes such as identity theft.

Several Federal Laws Seek to Protect Personally Identifiable Information Including SSNs

Two primary laws (the Privacy Act of 1974 and the E-Government Act of 2002) give federal agencies responsibilities for protecting personal information, including ensuring its security. Additionally, the Federal Information Security Management Act of 2002 (FISMA) requires agencies to develop, document, and implement agency wide programs to provide security for their information and information systems (which include

[4]Phishing is a high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.

[5]*Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats.* GAO-07-705. (Washington, D.C.: June 22, 2007). Statement of Associate Deputy Attorney General before the Subcommittee on Terrorism, Technology and Homeland Security the Senate Committee on the Judiciary (Mar. 21, 2007)

personally identifiable information and the systems on which it resides). FISMA is the primary law governing information security in the federal government. The act also requires the National Institute of Standards and Technology (NIST) to develop technical guidance in specific areas, including minimum information security requirements for information and information systems.

Other laws which help protect personally identifiable information include the Identity Theft and Assumption Deterrence Act, the Identity Theft Penalty Enhancement Act of 1998, the Gramm-Leach-Bliley Act (GLBA), and the Fair and Accurate Credit Transactions Act (FACTA). (See app. I, table 1, for a more detailed description of these and other related laws.) For example, the Identity Theft and Assumption Deterrence Act, enacted in 1998, makes it a criminal offense for a person to "knowingly transfer, possess, or use without lawful authority," another person's means of identification, such as their SSN, with the intent to commit, or in connection with, any unlawful activity that constitutes a felony under state or local law.[6] This act also mandated a specific role for the FTC in combating identity theft. To fulfill the mandate, FTC is collecting identity theft complaints and assisting victims through a telephone hotline and a dedicated Web site; maintaining and promoting the Identity Theft Data Clearinghouse, a centralized database of victim complaints that serves as an investigative tool for law enforcement; and providing outreach and education to consumers, law enforcement, and industry. According to FTC, it receives roughly 15,000 to 20,000 contacts per week on the hotline, via its Web site, or through the mail from victims and consumers who want to avoid becoming victims. In addition, the Identity Theft Enforcement and Restitution Act of 2008 requires persons convicted of identity theft to compensate their victims for the value of the time spent by the victim in an attempt to remediate the intended or actual harm incurred.

Another law with some provisions to assist victims of identity theft is FACTA. This law has several provisions to help address the difficulties victims often encounter in trying to recover from identity theft, including (1) a requirement that the FTC develop a model summary of rights to be distributed to consumers who believe that they are victims of identity theft, (2) the right for consumers to place fraud alerts on their credit reports, (3) the right to obtain copies of business records involved in

[6]Under the act, an individual's name or Social Security number is considered a "means of identification."

transactions alleged to be the result of identity theft, and (4) the right to obtain all information about fraudulently incurred debts that have been turned over to a collection agency.

The Office of Management and Budget has also issued numerous memoranda to federal agencies on safeguarding personally identifiable information. These cover such matters as designating a senior privacy official with responsibility for safeguarding information, and developing and implementing a data breach notification plan. (See app. I, table 2, for a more comprehensive list of pertinent OMB memoranda).

Several Federal Agencies Are Involved in Identifying and Investigating Identity Theft

Numerous federal agencies can have a role in identifying and investigating identity theft. This is, in part, because identity theft is not a "stand alone" crime, but rather a component of one or more complex crimes, such as computer fraud, credit card fraud, or mail fraud. For example, with the theft of identity information, a perpetrator may commit computer fraud when using a stolen identity to fraudulently obtain credit on the Internet. Computer fraud may also be the primary vehicle used to obtain identity information when the offender obtains unauthorized access to another computer or Web site to obtain such information. As a result, if caught, the offender may be charged with both identity theft and computer fraud. Moreover, perpetrators usually prey on multiple victims in multiple jurisdictions. Consequently, a number of federal law enforcement agencies can have a role in investigating identity theft crimes. How the thief obtains and/or uses an individual's identity usually dictates which federal agency has jurisdiction in the case. For example, if an individual finds that an identity thief has stolen the individual's mail to obtain credit cards, bank statements, or tax information, the victim should report the crime to the U.S. Postal Inspection Service, the law enforcement arm of the U.S. Postal Service. In addition, violations are investigated by other federal agencies, such as the Social Security Administration Office of the Inspector General, the U.S. Secret Service, the Federal Bureau of Investigation (FBI), the U.S. Department of State, the U.S. Department of Education Office of Inspector General, and the Internal Revenue Service. The Department of Justice may also prosecute federal identity theft cases. (See app. I, table 3, which highlights some of the jurisdictional responsibilities of some key federal agencies.)

States and Localities Have Enacted Laws and Taken Other Measures to Prevent Identity Theft and Assist Potential Victims

Many states have laws prohibiting the theft of identity information. For example, New York law makes identity theft a crime.[7] In other states, identity theft statutes also address specific crimes committed under a false identity. For example, Arizona law prohibits any person from using deceptive means to alter certain computer functions or use software to collect bank information, take control of another person's computer, or prevent the operator from blocking the installation of specific software.[8] In addition, Idaho law makes it unlawful to impersonate any state official to seek, demand, or obtain personally identifiable information of another person.[9] Furthermore, some states have also included identity theft victim assistance provisions in their laws. For example, Washington state law requires police and sheriffs' departments to provide a police report or original incident report at the request of any consumer claiming to be a victim of identity theft.[10]

States have also enacted laws to protect victims or potential victims of identity theft. One organization that tracks trends in identity theft reported in April 2009 that 47 states and the District of Columbia have enacted so-called "credit" or "security freeze" laws.[11] These laws allow consumers to block unauthorized third parties from obtaining their credit report or score. A consumer who places a security freeze on his or her credit report or score receives a personal identification number to gain access to credit information or to authorize the dissemination of credit information. Some states permit consumers to place security freezes only if they have been victims of identity theft or attempted identity theft.[12] The same organization also reported that, as of January 2009, 43 states and the District of Columbia require notifications of data breaches to consumers in

[7]N.Y. Penal Law § 190.77-190.84 (2002).

[8]Ariz. Rev. Stat. § 44-7301 et seq. (2005).

[9]Idaho Code § 18-3126A (2005).

[10]Wash. Rev. Code § 19.182.160 (2005).

[11]See Consumers Union Web Site, http://www.consumersunion.org/campaigns//learn_more/003484indiv.html (accessed May 14, 2009).

[12]CRS, *Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills*, T. A. Rainson, Congressional Research Service, RL 34028 (Washington, D.C.: Aug. 6, 2007).

certain circumstances.[13] Recently, some county governments have also completed or begun redacting or truncating SSNs that are displayed in public records—that is removing the full SSN from display or showing only part of it. Some are responding to state laws requiring these measures, but others have acted on their own based on concerns about the potential vulnerability of SSNs to misuse.

Vulnerabilities Remain to Protecting Personally Identifiable Information

While steps have been taken at the federal, state, and local level to prevent identity theft, vulnerabilities remain in both the public and private sectors. These vulnerabilities can be grouped into different areas, including: (1) display and use of Social Security numbers; (2) availability of personal information through private information resellers; and (3) security weaknesses in federal agency information systems that may lead to data security breaches involving personally identifiable information; among others.[14]

SSNs Are a Key Piece of Information Used in Identity Theft

SSNs are a critical piece of information used to perpetrate identity theft. Although the SSN was created as a means to track workers' earnings and eligibility for Social Security benefits, it is now also a vital piece of information needed to function in American society. Because of its unique nature and broad applicability, the SSN has become the identifier of choice for public and private sector entities, and it is used for numerous non-Social Security purposes. Today, U.S. citizens generally need an SSN to pay taxes, obtain a driver's license, or open a bank account, among other things. SSNs, along with names and birth certificates, are among the three personal identifiers most often sought by identity thieves. SSNs play an important role in identity theft because they are used as breeder information to create additional false identification documents, such as drivers' licenses. Most often, identity thieves use SSNs belonging to real people rather than making one up; however, on the basis of a review of identity theft reports, victims usually (65 percent of the time) did not know

[13]See Consumers Union Web Site, http://www.consumersunion.org/campaigns//financialprivacynow/002215indiv.html (accessed May 14, 2009).

[14]Our work has also identified other potential vulnerabilities to personally identifiable information in the public and private sectors, including security of personal information when it is outsourced to third party service providers, vulnerabilities in identification cards, and availability of personal information in public records.

where or how the thieves got their personal information.[15] In those instances when the source was known, the personal information, including SSNs, usually was obtained illegally. In these cases, identity thieves most often gained access to this personal information by taking advantage of an existing relationship with the victim. The next most common means of gaining access were by stealing information from purses, wallets, or the mail. Finally, while documents such as public records were traditionally accessed by visiting government records centers, a growing source of identity theft may be via the Internet. This is because some record keepers sell records containing SSNs in bulk to private companies and provide access to records on their own government Web sites. When records are sold in bulk or made available on the Internet, it is unknown how and by whom the records, and the personal identifying information contained in them, are used. Because the sources of identity theft cannot be more accurately pinpointed, it is not possible at this time to determine whether SSNs that are used improperly are obtained most frequently from the private or public sector.

Our prior work has documented several areas where potential vulnerabilities exist with respect to protecting the security of SSNs in both the public and private sectors. For example:

- **SSNs are displayed on some government-issued identification cards**: We have reported that an estimated 42 million Medicare cards, 8 million Department of Defense (DOD) insurance cards, and 7 million Department of Veterans Affairs (VA) beneficiary cards displayed entire 9-digit SSNs. VA and DOD have begun taking action to remove SSNs from cards. For example, VA is eliminating SSNs from 7 million VA identification cards and will replace cards with SSNs or issue new cards without SSNs until all such cards have been replaced. However, the Centers for Medicare and Medicaid Services, with the largest number of cards displaying the entire 9-digit SSN, has no plans to remove the SSN from Medicare identification cards.

- **Complete SSNs Could be Constructed Using Various Sources**: We also found a gap in a common practice for protecting SSNs: truncation—the practice of only displaying a partial number, such as the first 5 digits of an SSN. While we found that this practice would improve SSN protection if standardized, vulnerabilities remain. For example, in a recent review

[15]Javelin Strategy and Research, *2009 Identity Fraud Survey Report: Consumer Version* (Pleasanton, Calif., February 2009).

examining the availability of SSNs in public records, we found that it is possible to reconstruct an individual's full nine-digit SSN by combining a truncated SSN from a federally generated lien record with a truncated SSN from an information reseller.[16] These records typically contain an individual's SSN, name, and address. As a result of these findings, we advised Congress to consider enacting legislation to develop a standardized method of truncating SSNs. Such legislation was introduced in the 110th Congress.

Federal Law Does Not Cover all Data or Services Provided by Information Resellers

Federal law does not currently cover all data or services provided by information resellers, and the personally identifiable information these entities use in the course of their business operations could create potential vulnerability for identity theft, particularly when the information is available on the Internet. For example, information resellers, sometimes referred to as information brokers, are businesses that specialize in amassing personal information from multiple sources and offering informational services, including data on individuals. These entities may provide their services to a variety of prospective buyers, either to specific business clients or to the general public through the Internet. More prominent information resellers such as consumer reporting agencies and entities like LexisNexis provide information to their customers for various purposes, such as building consumer credit reports, verifying an individual's identity, differentiating records, marketing their products, and preventing financial fraud. These information resellers limit their services to businesses and government entities that establish accounts with them and have a legitimate purpose for obtaining an individual's personal information. For example, law firms and collection agencies may request information on an individual's bank accounts and real estate holdings for use in civil proceedings, such as a divorce. Information resellers that offer their services through the Internet (Internet resellers) will generally advertise their services to the general public for a fee. Resellers, whether well-known or Internet-based, collect information from three sources: public records, publicly available information, and nonpublic information. The aggregation of the general public's personal information, such as SSNs, in large corporate databases and the increased availability of information via the Internet may provide unscrupulous individuals a means to acquire SSNs and other personal information and use them for illegal purposes including identity theft.

[16] GAO-07-752

However, no federal law explicitly requires all information resellers to safeguard all of the sensitive personal information they may hold. For example, the Fair Credit and Reporting Act (FCRA) applies only to consumer information used or intended to be used to help determine eligibility for credit, and GLBA's safeguarding requirements apply only to customer data held by GLBA-defined financial institutions. Unfortunately, much of the personal information maintained by information resellers that does not fall under FCRA or GLBA is not necessarily required by federal law to be safeguarded, even when the information is sensitive and subject to misuse by identity thieves.

Federal Agencies Rely on Information Systems to Carry out Their Missions but Security Weaknesses Leave them Vulnerable to Data Breaches

Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. However, it is important for agencies to safeguard their systems against risks such as loss or theft of resources (such as federal payments and collections), modification or destruction of data, and unauthorized uses of computer resources or to launch attacks on other computer systems. Without such safeguards, sensitive information, such as taxpayer data, Social Security records, medical records, and proprietary business information could be inappropriately disclosed, browsed, or copied for improper or criminal purposes including identity theft.

Our work indicates that persistent weaknesses appear in five major categories of information system controls.[17] As a result, federal systems and sensitive information are at increased risk of unauthorized access and disclosure, modification, or destruction, as well as inadvertent or deliberate disruption of system operations and services. GAO has found that federal agencies continue to experience numerous security incidents that could leave sensitive personally identifiable information in federal records vulnerable to identity theft. Such risks are illustrated by the following examples:

[17]These weaknesses include (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and (5) an agency-wide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.

- In February 2009, the Federal Aviation Administration (FAA) notified employees that an agency computer was illegally accessed and employee personal identity information had been stolen electronically. Two of the 48 files on the breached computer server contained personal information about more than 45,000 FAA employees and retirees who were on the FAA's rolls as of the first week of February 2006. Law enforcement agencies were notified and are investigating the data theft.

- In June 2008, the Walter Reed Army Medical Center reported that officials were investigating the possible disclosure of personally identifiable information through unauthorized sharing of a data file containing the names of approximately 1,000 Military Health System beneficiaries. Walter Reed officials were notified of the possible exposure on May 21 by an outside company. Preliminary results of an ongoing investigation identified a computer from which the data had apparently been compromised. Data security personnel from Walter Reed and the Department of the Army think it is possible that individuals named in the file could become victims of identity theft. The compromised data file did not include protected health information such as medical records, diagnosis, or prognosis for patients.

- During fiscal year 2008, federal agencies reported 16, 843 incidents to the U.S. Computer Emergency Readiness Team (US-CERT)—a 206 percent increase over the 5,503 incidents reported in 2006.

Thus, significant weaknesses continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies.

The extent to which data breaches result in identity theft is not well known, in large part because it can be difficult to determine the source of the information used to commit identity theft. Available data and interviews with researchers, law enforcement officials, and industry representatives indicate that most breaches have not resulted in detected incidents of identity theft. In 2007, we reported on data breaches in selected sectors of the economy and the potential benefits of breach notifications.[18] As part of this review of the issue, we examined the 24 largest breaches that appeared in the news media from January 2000

[18]GAO, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent is Unknown*, GAO-07-737 (Washington, D.C.: June 4, 2007).

through June 2005 and found that 3 breaches appeared to have resulted in fraud on existing accounts, and 1 breach appeared to have resulted in the unauthorized creation of new accounts.[19]

When data breaches do occur, notification to the individuals affected and/or the public has clear benefits, allowing individuals the opportunity to take steps to protect themselves against the dangers of identity theft. Moreover, although existing laws do not require agencies to notify the public when data breaches occur, such notification is consistent with federal agencies' responsibility to inform individuals about how their information is being accessed and used, and promotes accountability for privacy protection. Similarly, in the private sector, representatives of federal banking regulators, industry associations, and other affected parties told us that breach notification requirements have encouraged companies and other entities to improve their data security practices to minimize legal liability or avoid public relations risks that may result from a publicized breach of customer data. Further, notifying affected consumers of a breach gives individuals the opportunity to mitigate potential risk—for example, by reviewing their credit card statements and credit reports, or placing a fraud alert on their credit files. Requiring consumer notification of data breaches may encourage better data security practices and help deter or mitigate harm from identity theft; however, such practices also involve monetary costs and other challenges such as determining an appropriate notification standard.

Based on the experience of various federal agencies and private sector organizations in responding to data breaches, we identified the following lessons learned regarding how and when to notify government officials, affected individuals, and the public of a data breach. In particular:

- Rapid internal notification of key government officials is critical.
- A core group of senior officials should be designated to make decisions regarding an agency's response.
- Mechanisms must be in place to obtain contact information for affected individuals.

[19] GAO-07-737.

- Determining when to offer credit monitoring to affected individuals requires risk-based management decisions.
- Interaction with the public requires careful coordination and can be resource-intensive.
- Internal training and awareness are critical to timely breach response, including notification.
- Contractor responsibilities for data breaches should be clearly defined.

OMB issued guidance in 2006 and 2007 reiterating agency responsibilities under the Privacy Act and FISMA, as well as technical guidance, drawing particular attention to the requirements associated with personally identifiable information. In this guidance, OMB directed, among other things, that agencies encrypt data on mobile computers or devices and follow NIST security guidelines regarding personally identifiable information.

However, guidance to assist agency officials in making consistent risk-based determinations about when to offer credit monitoring or other protection services has not been developed. Without such guidance, agencies are likely to continue to make inconsistent decisions about what protections to offer affected individuals, potentially leaving some people more vulnerable than others.

We and various agency inspectors general have made numerous recommendations to federal agencies to resolve prior significant control deficiencies and information security program shortfalls. In particular, we have noted that agencies also need to implement controls that reduce the chance of incidents involving data loss or theft, computer intrusions, and privacy breaches. For example, we recommended that the Director of OMB develop guidance for federal agencies on conducting risk analyses to determine when to offer credit monitoring and when to contract for an alternative form of monitoring, such as data breach monitoring, to assist individuals at risk of identity theft as a result of a federal data breach.[20] Other recommendations to agencies include that they need to implement controls that prevent, limit, or detect access to computer resources, and

[20]GAO *Privacy: Lessons Learned about Data Breach Notification*, GAO-07-657. (Washington, D.C.: April 30, 2007).

should manage the configuration of network devices to prevent unauthorized access and ensure system integrity. In addition, opportunities also exist to enhance policies and practices necessary for implementing sound information security programs. To implement these programs, agencies must create and maintain inventories of major systems, implement common security configurations, ensure staff receive information security training, test and evaluate controls, take remedial actions for known deficiencies, and certify and accredit systems for operation. While these recommendations are intended to broadly strengthen the integrity of federal information systems, they will also help address many of the vulnerabilities that can contribute to identity theft.

Concluding Observations

Efforts at the federal, state, and local level to protect personally identifiable information and help prevent identity theft are positive steps, but challenges remain. In particular, the use of SSNs by both public and private sector entities is likely to continue given that it is the key identifier used by these entities, and there is currently no widely accepted alternative. Personally identifiable information including an individual's name, date of birth, and SSN are important pieces of information used to perpetrate identify theft and fraud, and it is critical that steps be taken to protect such information. Without proper safeguards in place, such information will remain vulnerable to misuse, thus adding to the growing number of identity theft victims. As Congress moves forward in pursuing legislation to address the problem of identity theft, focusing the debate on vulnerabilities that have already been documented may help target efforts and policy directly toward new solutions. We look forward to supporting congressional consideration of these important policy issues.

Mr. Chairman, this concludes my prepared testimony. I would be pleased to respond to any questions you or other Members of the Subcommittee may have.

GAO Contacts

For further information regarding this testimony, please contact me at bertonid@gao.gov or (202) 512-7215. In addition, contact points for our Offices of Congressional Relations and Public Affairs can be found on the last page of this statement. Individuals making key contributions to this testimony include Jeremy Cox, John De Ferrari, Doreen Feldman, Christopher Lyons, and Joel Marus.

APPENDIX I: Additional Information on Federal Laws, OMB Memorandums, and Federal Agency Investigation Jurisdiction Relating to Protection of Personal Information and Identity Theft

Table 1: Selected Federal Laws Affecting Public and Private Sector Disclosure of Personal Information

Federal laws	Restrictions on disclosure	Entities affected
Gramm-Leach-Bliley Act (GLBA)	Creates a new definition of nonpublic personal information that includes SSNs and gives consumers the right to limit some, but not all, sharing of their nonpublic personal information. Financial institutions can disclose consumers' nonpublic information without offering them an opt-out right under certain circumstances permissible under the law, such as to protect the confidentiality or security of the consumer's record and to prevent actual or potential fraud.	Financial institutions such as credit bureaus and entities that receive data from financial institutions
Fair Credit Reporting Act (FCRA)	Limits access to consumer reports, which generally include SSNs, to those who have a permissible purpose under the law, such as state or local officials involved in the enforcement of child support cases or determining eligibility for employment.	Consumer reporting agencies and users of consumer reports
Fair and Accurate Credit Transactions Act (FACTA)	Amends FCRA to allow, among other things, consumers who request a copy of their credit report to also request that the first five digits of their SSN (or similar identification number) not be displayed; requires consumer reporting agencies and any business that uses consumer reports to adopt procedures for proper disposal of such reports.	Consumer reporting agencies and users of consumer reports
Driver's Privacy Protection Act (DPPA)	Prohibits disclosing personal information from a motor vehicle record, including SSNs, except for purposes permissible under the law.	State departments of motor vehicles, department of motor vehicle employees or contractors, and recipients of personal information from motor vehicle records
Health Insurance Portability and Accountability Act (HIPAA)	Protects the privacy of health information that identifies an individual (including by SSNs) and restricts health care organizations from disclosing such information to others without the patient's consent.	Health care providers, plans, and clearinghouses
The Privacy Act of 1974	Regulates certain types of federal recordkeeping; generally prohibits disclosure of personal information collected and maintained by federal agencies, such as SSNs, with exceptions.	Federal agencies
Social Security Act Amendments of 1990	Bars disclosure of SSNs collected pursuant to laws enacted on or after October 1, 1990.	Federal, state, and local government agencies
E-Government Act of 2002	Requires agencies to conduct privacy impact assessments (PIA) of how personal information is collected, stored, shared, and managed in a federal information system.	Federal agencies
Federal Information Security Management Act of 2002 (FISMA)	Defines federal requirements for securing information and information systems that support federal agency operations and assets including controls necessary to preserve authorized restrictions on access and disclosure to protect personal privacy.	Federal agencies

Source: GAO-02-352, GAO-06-495, GAO-06-676, GAO-06-833T, GAO-07-1023T

Table 2: Major OMB Memorandums Related to Protection of Personally Identifiable Information

Memorandum, date	Title	Major personally identifiable information requirement or recommendation
M-05-08, Feb. 11, 2005	Designation of Senior Agency Officials for Privacy	Directs agencies to designate a senior official with overall responsibility for information privacy issues who • is accountable for ensuring agency implementation of information privacy protection; and • must take appropriate steps to protect personally identifiable information from unauthorized use, access, disclosure, or sharing, and to protect related information systems from unauthorized access, modification, disruption, or destruction.
M-06-15, May 22, 2006	Safeguarding Personally Identifiable information	Re-emphasizes agency responsibilities to safeguard personally identifiable information and to appropriately train employees in this regard. Requires agency Senior Official for Privacy to conduct a review of policies and processes, and take necessary corrective actions to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information.
M-06-16, June 23, 2006	Protection of Sensitive Agency Information	Recommends that all agencies • encrypt all data on mobile computers/devices that carry agency data unless the data are determined to be nonsensitive; • allow remote access only with two-factor authentication, where one factor is provided by a device separate from the computer gaining access; • use a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity; and • log all computer-readable data extracts from databases holding sensitive information and verify that each extract including sensitive data has been erased within 90 days. Recommends that agencies use a NIST security checklist, included in the memo, that provides specific actions to be taken by agencies to protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter.
M-06-19, July 12, 2006	Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments	Requires agencies to report all incidents involving personally identifiable information to US-CERT within 1 hour of discovering the incident (this revises previous guidelines for reporting security incidents).
M-06-20, July 17, 2006	FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management	Requires agencies to identify in their yearly FISMA reports any physical or electronic incidents involving the loss of or unauthorized access to personally identifiable information.

Memorandum, date	Title	Major personally identifiable information requirement or recommendation
M-07-16, May 22, 2007	Safeguarding Against and Responding to the Breach of Personally Identifiable Information	Requires agencies to develop and implement a breach notification policy and plan, including policy for the notification of the public, and provides the elements that must be included in the policies, including the incident reporting requirements of M-06-19. Restates recommendations of M-06-16 as requirements. Requires agencies to establish an agency response team to ensure adequate coverage and implementation of the plan. Requires agencies to review and reduce the volume of personally identifiable information to the minimum necessary and reduce the use of Social Security numbers. Updates incident reporting and handling requirements. Requires agencies' breach notification policy and plan to lay out employees' roles and responsibilities for handling breaches of personally identifiable information, as well as relationships with contractors or partners.

Source: GAO-08-343

Table 3: List of Federal Agencies with Some Identity Theft Jurisdiction

Federal agency	Jurisdictional identity theft highlights
Social Security Administration's Office of the Inspector General	Investigates SSN misuse involving the buying and selling of SSN cards.
U.S. Secret Service	Investigates crimes associated with financial institutions; investigations include bank fraud, access device fraud involving credit and debit cards, telecommunications and computer crimes, fraudulent identification, fraudulent government and commercial securities, and electronic funds transfer fraud.
Federal Bureau of Investigation	Investigates cases of identity theft; investigations can include bank fraud, mail fraud, wire fraud, bankruptcy fraud, insurance fraud, and fraud against the government. In addition, FBI sponsors a national Identity Theft Working Group, where participants from law enforcement, federal regulatory bodies, and the financial services industry meet regularly to discuss identity theft related issues.
U.S. Securities and Exchange Commission	Investigates investment fraud in instances where an identity thief has tampered with securities investments or brokerage accounts.
U.S. Department of State	Investigates passport fraud in instances where a passport is used fraudulently.
U.S. Department of Education, Office of Inspector General	Investigates fraudulent student loan activity.
Internal Revenue Service	Investigates tax fraud where identity theft may relate directly to tax records.

Source: GAO-05-1016T

Related GAO Products

Information Security: Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist. GAO-09-701T. Washington, D.C.: May 19, 2009.

Social Security Numbers Are Widely Available in Bulk and Online Records, but Changes to Enhance Security Are Occurring. GAO-08-1009R. Washington, D.C.: September 19, 2008.

Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains. GAO-08-525. Washington, D.C.: June 27, 2008.

Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist. GAO-08-571T. Washington, D.C.: March 12, 2008.

Information Security: Protecting Personally Identifiable Information. GAO-08-343. Washington, D.C.: January 25, 2008.

Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses. GAO-07-837. Washington, D.C.: July 27, 2007.

Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats. GAO-07-705. Washington, D.C.: June 22, 2007.

Social Security Numbers: Use is Widespread and Protection Could Be Improved. GAO-07-1023T. Washington, D.C.: June 21, 2007.

Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain. GAO-07-752. Washington, D.C.: June 15, 2007.

Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown. GAO-07-737. Washington, D.C.: June 4, 2007.

Privacy: Lessons Learned about Data Breach Notification. GAO-07-657. Washington, D.C.: April 30, 2007.

Privacy: Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid, and TRICARE. GAO-06-676. Washington, D.C.: September 5, 2006

Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data. GAO-06-674. Washington, D.C.: June 26, 2006.

Privacy: Preventing and Responding to Improper Disclosures of Personal Information. GAO-06-833T. Washington, D.C.: June 8, 2006.

Social Security Numbers: Internet Resellers Provide Few Full SSNs, but Congress Should Consider Enacting Standards for Truncating SSNs. GAO-06-495. Washington, D.C.: May 17, 2006.

Social Security Numbers: More Could Be Done to Protect SSNs. GAO-06-586T. Washington, D.C.: March 30, 2006.

Social Security Numbers: Stronger Protections Needed When Contractors Have Access to SSNs. GAO-06-238. Washington, D.C.: January 23, 2006.

Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain. GAO-05-1016T. Washington, D.C.: September 15, 2005.

Identity Theft: Some Outreach Efforts to Promote Awareness of New Consumer Rights Are Underway. GAO-05-710. Washington, D.C.: June 30, 2005.

Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems. GAO-05-231. Washington, D.C.: May 13, 2005.

Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards. GAO-05-59. Washington, D.C.: November 9, 2004.

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

Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards. GAO-02-352. Washington, D.C.: May 31, 2002.

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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

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

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548