

GAO

Report to the Chairman, Subcommittee
on Administrative Oversight and the
Courts, Committee on the Judiciary,
U.S. Senate

June 2007

SOCIAL SECURITY NUMBERS

Federal Actions Could
Further Decrease
Availability in Public
Records, though Other
Vulnerabilities Remain



Contents

Letter		1
	Conclusions	3
	Recommendations for Executive Action	4
	Agency Comments	4
Appendix I	Briefing Slides	6
Appendix II	Comments from the Office of Management and Budget	40
Appendix III	Comments from the Internal Revenue Service	42
Related GAO Products		44

Abbreviations

DOJ	Department of Justice
IRS	Internal Revenue Service
OMB	Office of Management and Budget
SSA	Social Security Administration
SSN	Social Security number

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



United States Government Accountability Office
Washington, DC 20548

June 15, 2007

The Honorable Charles Schumer
Chairman
Subcommittee on Administrative Oversight and the Courts
Committee on the Judiciary
United States Senate

Various public records in the United States, including some generated by the federal government, contain Social Security numbers (SSN) and other personal identifying information that could be used to commit fraud and identity theft. Public records are generally defined as government agency-held records made available to the public in their entirety for inspection, such as property records and court records. Although public records were traditionally accessed locally in county courthouses and government record centers, in recent years, some state and local public record keepers have begun to make these records available to the public through the Internet. While it is important for the public to have access to these records, concerns about the use of information in these records for criminal purposes have been raised. In 2006, these concerns were heightened when 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.

Although we previously reported on the types of public records that contain SSNs and access to those records, less is known about the federal government's direct provision of records with SSNs to state and local public record keepers. Because of your interest in information on these issues, we agreed to answer the following questions: (1) Which federal agencies commonly provide records containing SSNs to state and local public record keepers, and what actions have been taken to protect SSNs in these records? (2) What significant vulnerabilities, if any, remain to protecting SSNs in public records?

To answer these questions, we gathered information from a variety of sources. Specifically, we interviewed cognizant officials from the Social Security Administration (SSA), Office of Management and Budget (OMB), Internal Revenue Service (IRS), and Department of Justice (DOJ). We interviewed these agencies because they are responsible for overseeing

federal use of the SSN or they were identified through our research as commonly providing records containing SSNs to state and local public record keepers. We also conducted interviews with public record keepers, their national associations, and stakeholder groups focused on privacy rights, open government, and the title insurance industry. To gather information on records access, we visited local public record keepers' offices in the District of Columbia, Maryland, and Virginia; reviewed several Web sites that provide information on state and local public records access; and used this work to guide our selection of state and local public record keepers' Web sites nationwide for additional review. In total, we reviewed at least one public record keeper's Web site per state. We also interviewed public record keepers in five Florida counties to examine implementation of recently enacted Florida statutes requiring Internet access to public records and the removal of SSNs and other information in those records. We conducted our work from November 2006 through May 2007 in accordance with generally accepted government auditing standards.

On May 10, 2007, we briefed your staff on the results of our analysis. This report formally conveys the information provided during that briefing (see app. I). In summary, we found:

- IRS and DOJ are the only federal agencies that commonly provide records containing SSNs to state and local public record keepers, and in recent years, both have taken steps to truncate or remove SSNs in those records. These agencies provide property lien records to public record keepers, on which they traditionally included full SSNs for identity verification purposes. However, both agencies have recently taken steps to better protect SSNs in these records. Currently, IRS mandates the use of a truncated version of SSNs on tax lien notices, which displays only the last four digits of the SSN. However, the agency does not mandate SSN truncation on all lien releases it issues. In addition, many of DOJ's districts have begun to truncate or fully remove SSNs on the lien records they provide to public record keepers. However, because DOJ's districts act independently to issue lien notices, some continue to display full SSNs in these records. Independent of IRS and DOJ efforts in this area, some states have begun to remove SSNs in all public records they maintain, though this approach can be costly and may not be fully effective at protecting SSNs.
- Both full and truncated SSNs in federally generated public records remain vulnerable to potential misuse, in part because different

truncation methods used by the public and private sectors may enable the reconstruction of full SSNs. While the display of truncated SSNs in federally generated public records is a step toward improved SSN protection, we previously reported that information resellers—companies that specialize in amassing personal information—sometimes provide truncated SSNs to customers that show the first five digits. Consequently, 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. In addition, while IRS and DOJ have recently taken actions to limit disclosure of full SSNs in records they generate going forward, full SSNs remain in the millions of lien records provided to public record keepers before the agencies implemented these changes. Increased access to these records through bulk sales to private companies and Internet access also creates the potential for identity theft. For example, public record keepers in some states have been selling complete copies of their records to private companies, such as title companies and information resellers, for many years. Because of this practice, current efforts to remove SSNs in records maintained by public record keepers do not apply to all copies of the record already made available. In addition, some public record keepers now provide potentially unlimited Web site access to personal identifying information in the records they maintain.

Conclusions

Federal agencies have taken actions to mitigate the availability of SSNs in public records by implementing the use of truncation for documents provided to state and local record keepers. While these actions provide some additional protection against using these records to perpetrate identity theft, our review demonstrates that identity thieves may still be able to reconstruct full SSNs by combining different truncated versions of the SSN available from public and private sources. Thus, truncation does not provide complete protection against identity theft. Yet despite this limitation, our analysis suggests that truncation provides better protection compared with records that display full SSNs. In this regard, as we noted in our May 2006 report, Congress may wish to further improve SSN protection by enacting truncation standards or assigning an agency to do so. In addition, Congress may wish to solicit input on promising truncation practices from the Commissioner of Social Security as part of this process. However, in the absence of such standards, federal agencies can still take steps to protect SSNs by further reducing their exposure in records they generate and provide to record keepers.

Recommendations for Executive Action

To the extent that truncation provides an added level of protection from identity theft, we are recommending that

- The Commissioner of IRS should implement a policy requiring the truncation of all SSNs in lien releases the agency generates.
- The Attorney General should implement a policy requiring, at a minimum, SSN truncation in all lien records generated by its judicial districts. Truncation should be in the same format as is currently used by IRS on lien notices.

Agency Comments

We provided a draft of this report to SSA, OMB, IRS, and DOJ for review and comment. SSA, IRS, and DOJ provided technical comments, which we incorporated as appropriate. We received written comments from OMB and IRS, which are reproduced in appendixes II and III. In its comments, OMB indicated its appreciation for the report's analysis of SSN use and vulnerability, in both full and truncated forms, and provided information on OMB's recent actions that require federal agencies to reduce the volume of sensitive information, including SSNs, they maintain.

Concerning our recommendations, SSA indicated that the agency fully supports our recommendations to IRS and DOJ because it believes that SSN truncation will greatly improve protection of the SSN. DOJ also agreed with our recommendation and subsequently issued a policy guidance memo that restricts all U.S. Attorneys' Offices from using full SSNs in any record submitted to state or local public record keepers. The memo requires offices to either remove the SSN entirely from these records or use a truncated version of the SSN, showing only the last four digits. While IRS generally agreed that the use of truncated SSNs on records submitted to state and local public record keepers provides an added level of protection against identity theft, the agency does not currently plan to implement our recommendation to truncate SSNs in all lien releases it generates, specifically those relating to pre-2006 lien notices. IRS indicated that truncating SSNs on lien releases for which the original lien notices show full SSNs may place a hardship on IRS's lien processing capabilities because it requires a change in how the agency's centralized Lien Processing Unit formats those lien releases. While we recognize that this change could potentially cause an administrative burden for IRS, we believe that the added level of protection against identity theft accomplished by truncating SSNs on lien releases outweighs these costs. IRS also indicated that truncating SSNs on lien releases for which the original lien notices show full SSNs may prove problematic for

record keepers. However, we do not believe that truncating SSNs on lien releases would prove problematic for most record keepers. Specifically, IRS includes key identifying information that corresponds to the original lien notice on most of the lien releases they submit to record keepers. Therefore, this identifying information can be used by record keepers to determine which lien notice corresponds to the newly submitted release, and IRS should not need to include a person's full SSN on the lien release for this purpose.

As we agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its issue date. At that time, we will send copies of this report to relevant congressional committees, the Commissioner of SSA, the Director of OMB, the Commissioner of IRS, the Attorney General, and other interested parties and will make copies available to others upon request. In addition, this report will be available on GAO's Web site at <http://www.gao.gov>. If you or your staff have any questions about this report, please contact me at 202-512-7215 or bertonid@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report include Jeremy Cox (Assistant Director), Rachel Frisk (Analyst-in-Charge), and Ayeke Messam. In addition, Dan Schwimer provided legal assistance.



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

Appendix I: Briefing Slides



SOCIAL SECURITY NUMBERS: Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain

**Briefing for Senator Charles Schumer
Chairman of the Subcommittee on Administrative
Oversight and the Courts
Committee on the Judiciary**

May 10, 2007



Overview

- Key Objectives
 - Scope and Methodology
 - Summary of Results
 - Background
 - Findings
 - Conclusions
 - Recommendations for Executive Action
-



Key Objectives

We agreed to determine:

1. Which federal agencies commonly provide records containing Social Security numbers (SSN) to state and local public record keepers, and what actions have been taken to protect SSNs in these records?
2. What significant vulnerabilities, if any, remain to protecting SSNs in public records?



Scope and Methodology

To answer these questions, we:

- Gathered information from the Social Security Administration (SSA), Office of Management and Budget (OMB), Internal Revenue Service (IRS), and Department of Justice (DOJ);
 - Interviewed public record keepers, their national associations, and stakeholder groups focused on privacy rights, open government, and the title insurance industry;
 - Visited local record keepers' offices in the District of Columbia (D.C.), Maryland, and Virginia, reviewed several Web sites that provide information on public records access, and examined selected record keepers' Web sites nationwide; and,
 - Interviewed record keepers in five Florida counties to discuss recently enacted state statutes related to public records access and the removal of certain personal-identifying information in those records.
-



Summary of Results

- IRS and DOJ commonly provide lien records containing SSNs to state and local public record keepers, and they have recently begun to truncate or remove SSNs in those records. While IRS mandates SSN truncation in all lien notices, it does not mandate truncation in all lien releases.¹ Because DOJ's districts act independently to issue lien notices, some truncate or remove SSNs in these records, while others continue to display full SSNs. Independent of these efforts, some states have begun to remove SSNs in all public records. However, this approach can be costly and may not fully protect SSNs.

¹ Lien notices are issued by government agencies to inform the public and creditors of a lien against a debtor's property. Lien releases are issued by agencies when a debt has been paid.



Summary of Results (continued)

- Both full and truncated SSNs in federally generated public records remain vulnerable to potential misuse, in part because different truncation methods used by the public and private sectors enable the reconstruction of full SSNs. In addition, the continued availability of SSNs in public records, as well as increased access to these records through bulk sales and Internet access, create the potential for identity theft.

Background



SSNs: Use and Federal Regulation

- Although originally created to track workers' earnings and Social Security benefits, SSNs have become the identifier of choice for government agencies and private businesses and are currently used for myriad non-Social Security purposes.

Background



SSNs: Use and Federal Regulation (continued)

-
- No single federal law regulates the overall use or restricts the disclosure of SSNs by governments. However, certain laws limit SSN use in specific circumstances.
 - For example, the Privacy Act of 1974 generally prohibits federal agencies from disclosing records containing SSNs without the consent of the individual whose records are being sought.
 - Exceptions authorized under the act include routine uses that are compatible with the purpose for which the SSN was collected, such as activities related to tax and debt collection.

Background



SSNs: Use in Identity Theft

- While the use of SSNs can be beneficial for identity verification and other purposes, SSNs are also a key piece of information used to create false identities for financial misuse or assume another individual's identity.
- Most often, identity thieves use SSNs belonging to real people. However, only 30 percent of identity theft victims know how thieves obtained their personal information.¹
- The Federal Trade Commission (FTC) estimated that over a 1-year period, nearly 10 million people discovered they were victims of identity theft, translating into estimated losses of billions of dollars.
- In response to this issue, the federal government and several state governments have passed identity theft legislation in recent years.

¹ This estimate is based on the FTC's identity theft victim complaint data. These data are self-reported and only represent crimes reported to FTC.

Background



Public Records: Definition and Types

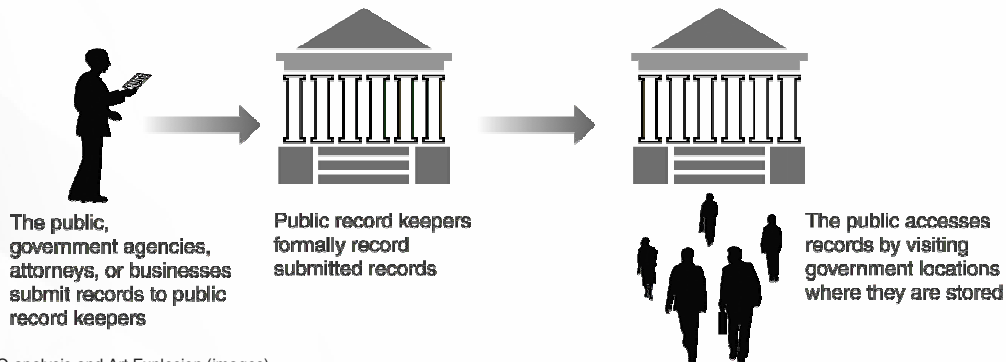
- Public records can generally be defined as records or documents that are routinely made available to the public by a government agency or the courts.
 - For example, local record keepers maintain public records that assist in the conduct of business, legal, or personal affairs.
- There are many types of public records, including birth, death, and marriage records; criminal and civil court case files; and records that concern property ownership, such as property liens.
 - Some documents in these records are created by government agencies, while others are submitted by private entities.
 - Some records contain personal identifying information, such as SSNs, dates of birth, credit card or bank account numbers, and children's names or mothers' maiden names.

Background



Public Records: Storage and Access

- Record keepers store records in several formats, including paper copy, microfiche or microfilm, and electronic image.
- Traditionally, individuals accessed public records by visiting the government offices that maintained them, which provided practical limits on the volume of personal identifying information that could be disclosed.



Source: GAO analysis and Art Explosion (images).

Objective 1: Federal Provision of Records with SSNs



IRS and DOJ Commonly Provide Records Containing SSNs to Record Keepers, and They Have Recently Begun to Truncate or Remove SSNs in Those Records

- IRS and DOJ commonly provide lien notices and releases containing SSNs to state and local public record keepers.
- IRS mandates SSN truncation in all lien notices but not all releases.
- DOJ's judicial districts act independently to truncate, remove, or include SSNs in lien notices.
- Some states are independently taking actions to remove SSNs from public records, but these approaches can be costly and may have a limited effect on protecting SSNs.

Objective 1: Federal Provision of Records with SSNs



IRS and DOJ Commonly Provide Lien Notices and Releases Containing SSNs to State and Local Public Record Keepers

- We found that IRS and DOJ are the only federal agencies that commonly provide records containing SSNs to state and local public record keepers.
- Annually, IRS generates approximately 900,000 lien notices and releases for tax-related debts owed to the federal government.
 - IRS files lien notices and releases with state and local public record keepers through its centralized Lien Processing Unit.
- Annually, DOJ issues approximately 11,000 lien notices for criminal or civil court-related debts owed to the federal government.
 - DOJ lien notices are not generated through a centralized processing system. Instead, debt collection units for each judicial district file liens individually with the relevant public record keeper.¹

¹ While there are 94 districts, there are 93 debt collection units. These units also generate lien releases, but releases are typically provided directly to debtors rather than public record keepers.

Objective 1: Federal Provision of Records with SSNs



IRS and DOJ Commonly Provide Lien Notices and Releases Containing SSNs to State and Local Public Record Keepers (continued)

- IRS- and DOJ-issued liens serve as federal government liens against property and are generally filed in the same manner.
- Neither federal statute nor regulations require that the SSN be included on notices or releases of liens. However, current federal law also does not prohibit SSNs from being included on these records. A lien record typically contains an SSN, name, address, and amount owed.
 - IRS and DOJ officials reported that SSNs traditionally have been included on lien records for identity verification purposes.

Objective 1: Federal Provision of Records with SSNs



IRS and DOJ Commonly Provide Lien Notices and Releases Containing SSNs to State and Local Public Record Keepers (continued)

- While a significant number of federal lien records are generated annually, because they are distributed throughout the country, they do not always make up a significant portion of local record keepers' official records.¹
 - For example, the Palm Beach County, Florida, Clerk and Comptroller's Office reported that federally generated records account for only 3 percent of the county's official records.

¹ Official public records, or property records, generally include records related to property sale, ownership, or encumbrance, rather than vital records or court records unrelated to property.

Objective 1: Federal Provision of Records with SSNs



IRS Partially Mandates SSN Truncation, while DOJ's Districts Act Independently to Truncate or Remove SSNs in Lien Records

- In recent years, IRS and DOJ have taken steps to better protect SSNs in lien records they file with state and local public record keepers.
 - As of January 1, 2006, IRS mandates the use of a truncated version of the SSN on all tax lien notices. This truncated SSN displays only the last four digits of the nine-digit number.
 - Before implementing this change in policy, IRS conducted a survey of recording officials in 12 states who agreed that SSN truncation would be helpful in addressing privacy and identity theft concerns.
 - IRS stated that its SSN truncation policy still ensures identity verification with a high degree of certainty.

Objective 1: Federal Provision of Records with SSNs



IRS Partially Mandates SSN Truncation, while DOJ's Districts Act Independently to Truncate or Remove SSNs in Lien Records (continued)

- IRS's change in its SSN policy for lien notices does not apply to lien releases.
- Because the release is generated to match the original lien notice, lien releases sometimes still contain full SSNs.
 - For example, a lien release recorded in 2007 will show a full SSN if the corresponding lien notice was recorded before January 1, 2006.
 - However, lien releases recorded for notices generated after January 1, 2006, will contain truncated SSNs, like the corresponding notices.

Objective 1: Federal Provision of Records with SSNs



IRS Partially Mandates SSN Truncation, while DOJ's Districts Act Independently to Truncate or Remove SSNs in Lien Records (continued)

- Unlike IRS, DOJ has not issued a central policy regarding disclosure of SSNs in lien notices.
- Consequently, the 93 debt collection units for DOJ districts individually decide how to display SSNs in the lien notices they record with record keepers.
 - DOJ officials reported that 80 debt collection units currently include either a truncated SSN or no SSN in lien notices. Most include a truncated SSN showing the last four digits.¹
 - According to DOJ, the remaining 13 debt collection units currently include a full SSN on liens. However, several of these units told DOJ officials that they are considering removing SSNs on future liens.

¹ While DOJ could not confirm that all districts displaying truncated SSNs on lien notices show the last four digits, this is likely, due to similar changes in SSNs displayed in federal court records. 18

Objective 1: Federal Provision of Records with SSNs



Some States Are Taking Actions to Remove SSNs from Public Records, but These Approaches Can Be Costly and May Have Limited Effect

- Independent of IRS and DOJ actions, some states have recently considered removing SSNs in public records in order to better protect this information.
 - Florida and Nevada both passed legislation in 2005 requiring the removal of SSNs in public records. Record keepers have until January 1, 2008, to comply with the Florida law and January 1, 2017, to comply with the Nevada law.
 - Texas also passed legislation in 2005 that was interpreted by the Attorney General as prohibiting the disclosure of SSNs in public records. However, in response to that ruling, the Texas legislature enacted legislation that permits the disclosure of SSNs in public records and states that the SSN of a living person in Texas is not considered confidential in these records.

Objective 1: Federal Provision of Records with SSNs



Some States Are Taking Actions to Remove SSNs from Public Records, but These Approaches Can Be Costly and May Have Limited Effect (continued)

- Due to the 2008 deadline, public record keepers in Florida are currently taking actions to remove SSNs and several other personal identifiers from records. Officials in the five counties we spoke with are using a two-step process utilizing software that searches for and removes SSNs and a manual review of records by county or contractor staff.
- Florida record keepers reported that this approach is costly, with some funding provided by each county's trust fund for public records modernization.¹
 - For example, Palm Beach County, Florida's third largest county, paid over \$2 million to complete software and manual review and removal of SSNs and other personal identifiers in approximately 40 million pages of records.
- Due to software limitations and the potential for human error, this process may still not remove 100 percent of SSNs in these records.

¹ Recording fees have been accruing in county trust funds since Florida statute created these funds in 1987.

Objective 2: Remaining Vulnerabilities



The Continued Availability of SSNs in Public Records, as well as Increased Access to These Records, Create the Potential for Identity Theft

- Both full and truncated SSNs can potentially be used to commit identity theft.
- Although IRS and DOJ have taken actions to better protect SSNs in the public records they commonly generate going forward, records they generated prior to these actions still contain SSNs.
- Some public record keepers provide potentially unlimited access to records and their content through bulk sales to private companies and online access.

Objective 2: Remaining Vulnerabilities



Both Full SSNs and Truncated SSNs Can Potentially Be Used to Commit Identity Theft

- Full nine-digit SSNs are key to the commission of identity theft.
 - For example, SSNs can be used as breeder information to create false identification documents, such as driver's licenses.
 - In addition, SSNs and other personal identifying information are used to fraudulently obtain credit cards, open utility accounts, commit bank fraud, file false tax returns, and falsely obtain employment and government benefits.
- Identity theft has been traced to personal identifying information accessed in public records.
 - For example, in recent years, criminals used personal identifying information contained in public records found on record keepers' Web sites in Hamilton County, Ohio, and Maricopa County, Arizona, to commit identity theft.
- However, the extent to which SSNs in public records have been used for this purpose is largely unknown.

Objective 2: Remaining Vulnerabilities



Both Full SSNs and Truncated SSNs Can Potentially Be Used to Commit Identity Theft (continued)

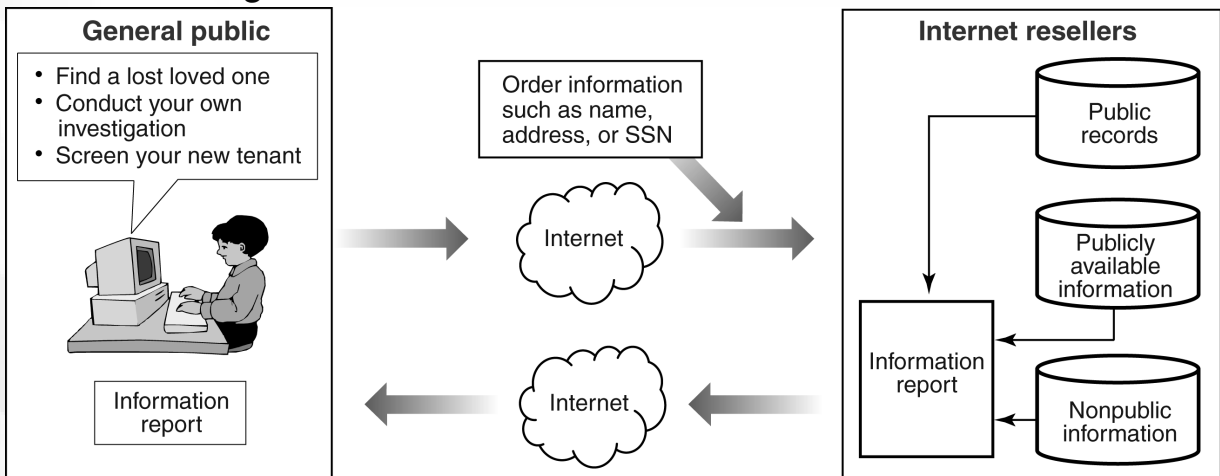
- While the display of truncated SSNs—showing only the last four digits—in federally generated public records is a step toward improved SSN protection, this method of truncation does not fully protect SSNs because other sources may provide the first five digits of a person’s SSN.
- In our prior work, we found that information resellers—private companies that specialize in amassing personal information—sometimes provide truncated SSNs showing the first five digits to customers with which they have accounts or to the public over the Internet.¹
 - For example, most customers of a prominent information reseller are able to access information containing truncated SSNs that show the first five digits.
 - Similarly, in our prior work on Internet-based information resellers, four resellers that gave our investigators truncated SSNs provided them in a form that showed the first five digits.

¹ See GAO-04-11 and GAO-06-495.

Objective 2: Remaining Vulnerabilities

Both Full SSNs and Truncated SSNs Can Potentially Be Used to Commit Identity Theft (continued)

The general public can purchase personal information, which may include truncated SSNs, from information resellers that provide services through the Internet.



Source: GAO analysis.

Objective 2: Remaining Vulnerabilities



Both Full SSNs and Truncated SSNs Can Potentially Be Used to Commit Identity Theft (continued)

- Consequently, by combining a person’s truncated SSN on an IRS- or DOJ-generated lien notice with that same person’s truncated SSN obtained from an information reseller, it may be possible to determine an individual’s full nine-digit SSN.
 - We tested this method and found that it can potentially be used by identity thieves to reconstruct full SSNs.

Objective 2: Remaining Vulnerabilities



Although Federal Agencies Have Taken Actions to Better Protect SSNs in Records, Some Still Contain SSNs

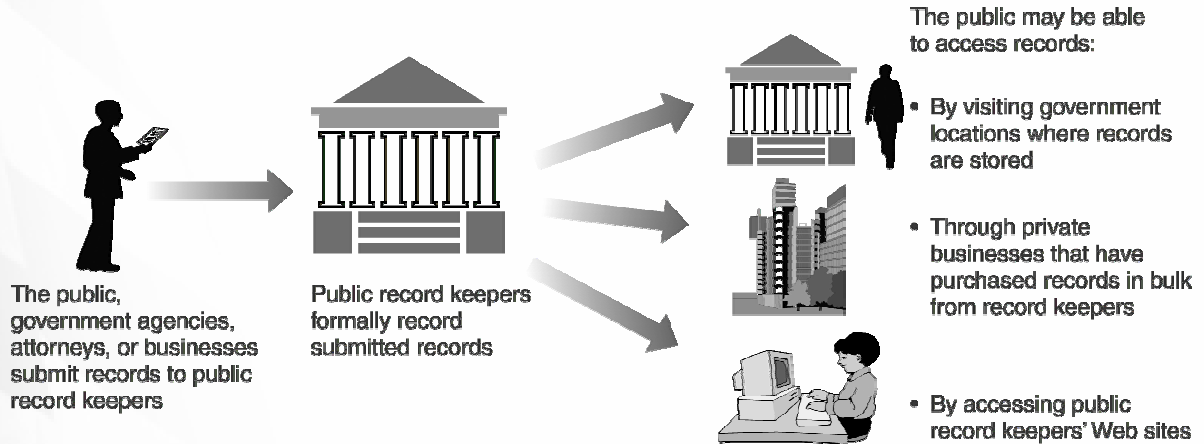
- IRS and DOJ actions will generally limit disclosure of full nine-digit SSNs in records they generate going forward, but full SSNs remain in the millions of records these agencies provided to public record keepers before they began truncating and removing SSNs.
 - For example, in the 10 years prior to IRS enacting its policy requiring truncated SSNs on lien notices, IRS generated almost 9 million lien records containing full SSNs,¹ all of which currently remain in the public record.
- Once a record is officially recorded, the public record keeper is responsible for maintaining it in perpetuity. Therefore, although an IRS tax lien expires after 10 years, the lien notice remains in the public record even after expiration.

¹ The 9 million lien records include lien notices and releases.

Objective 2: Remaining Vulnerabilities

Some Record Keepers Provide Potentially Unlimited Access to Records and Their Content through Sales to Private Companies and Online Access

Public records were traditionally accessed by visiting government record centers. However, some record keepers currently sell records in bulk to private companies, and some provide access to records on their own government Web sites.

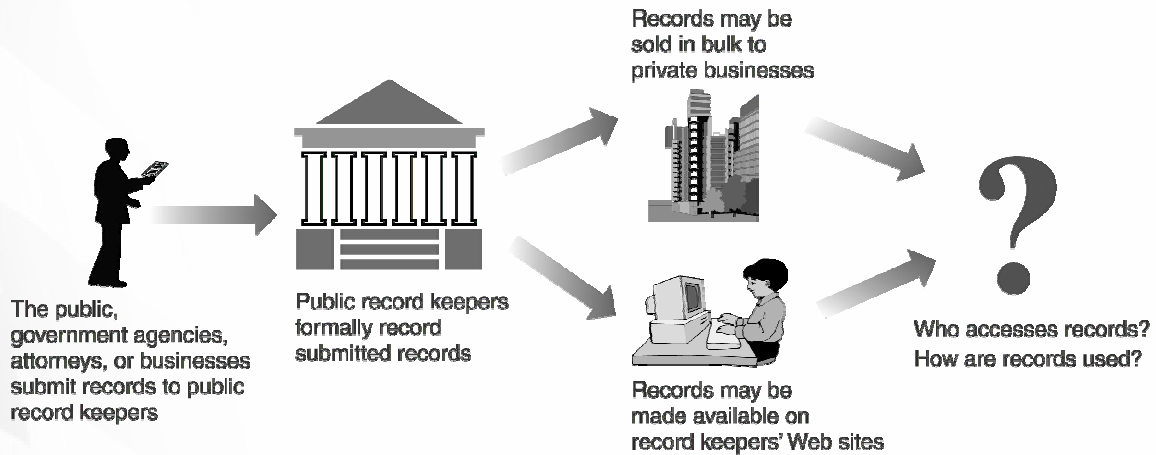


Source: GAO analysis and Art Explosion (images).

Objective 2: Remaining Vulnerabilities

Some Record Keepers Provide Potentially Unlimited Access to Records and Their Content through Sales to Private Companies and Online Access (continued)

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.



Source: GAO analysis and Art Explosion (images).

Objective 2: Remaining Vulnerabilities



The Extent of Bulk Record Sales to Private Companies, as well as How Companies Use and Provide Access to Records, Are Unknown

- Record keepers and others report that private businesses have been purchasing public records in bulk for years.¹ However, the extent of this practice and the ways in which private businesses use and provide access to these records are largely unknown.
 - For example, while title insurance companies may primarily use copies of property records to conduct related business, information resellers may use records for a variety of purposes. These purposes may include the provision of records that contain SSNs to customers and the general public.
 - In addition, the extent to which businesses provide access to these records, and their content, is unknown. Because some businesses use companies located outside of the United States for data entry and other purposes, records and the personal identifying information they contain may be accessible overseas. In these instances, it is unclear whether U.S. law would protect SSNs from potential misuse.

¹ This practice varies by state and locality. For example, some states require record keepers to sell records in bulk and only charge to recover the costs associated with record reproduction.

Objective 2: Remaining Vulnerabilities



Online Access to Records Is Increasing, and May Result in Potentially Unlimited Access to Records and Their Content

- Many record keepers and representatives of stakeholder groups we interviewed indicated that public records have become more available on the Internet in recent years.
- Across the country, record keepers provide different types of access to public records on their Web sites.
 - Some provide free access to a records index that includes information such as record type, person associated with the record, and recording date.
 - Others provide either free or paid access to both a records index and electronic record images. An electronic record image is typically a complete copy of the record and its contents.
- One organization that publishes public records information estimated that from 2004 to 2006, the proportion of all record keepers providing Internet access to a records index or electronic record images increased from 40 to 57 percent.¹

¹ This organization conducts research nationwide on entities that maintain public records and access to records. This estimate does not include public record keepers that maintain court records.³⁰



Objective 2: Remaining Vulnerabilities

Online Access to Records Is Increasing, and May Result in Potentially Unlimited Access to Records and Their Content (continued)

- Online access to electronic record images provides potentially unlimited access to the content of records, including SSNs and other personal identifying information, unless this information has been removed by the record keeper.
 - In our own review of record keepers' Web sites across the country, we found that at least 1 record keeper in 40 of the 50 states and D.C. (78 percent) provided free or paid online access to electronic record images.¹

¹ We reviewed the Web sites of state and local record keepers that maintain property records. Therefore, this figure does not include record keepers that maintain court or other public records.



Conclusions

-
- Federal agencies have taken actions to mitigate the availability of SSNs in public records by implementing the use of truncation for documents provided to state and local record keepers.
 - While these actions provide some additional protection against using these records to perpetrate identity theft, our review demonstrates that identity thieves may still be able to reconstruct full SSNs by combining different truncated versions of the SSN available from public and private sources.
 - Thus, truncation does not provide complete protection against identity theft.
-



Conclusions (continued)

- Yet despite this limitation, our analysis suggests that truncation provides better protection compared with records that display full SSNs.
- In this regard, as we noted in our May 2006 report, Congress may wish to further improve SSN protection by enacting truncation standards or assigning an agency to do so.¹ In addition, Congress may wish to solicit input on promising truncation practices from the Commissioner of Social Security as part of this process.
- However, in the absence of such standards, federal agencies can still take steps to protect SSNs by further reducing their exposure in records they generate and provide to record keepers.

¹ See GAO-06-495.



Recommendations for Executive Action

- To the extent that truncation provides an added level of protection from identity theft, we are recommending that
 - The Commissioner of IRS should implement a policy requiring the truncation of all SSNs in lien releases the agency generates.
 - The Attorney General should implement a policy requiring, at a minimum, SSN truncation in all lien records generated by its judicial districts. Truncation should be in the same format as is currently used by IRS on lien notices.

Appendix II: Comments from the Office of Management and Budget



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D. C. 20503

June 8, 2007

Mr. Daniel Bertoni
Director, Education, Workforce, and
Income Security Issues
Government Accountability Office
441 G Street, SW
Washington, DC 20548

Dear Mr. Bertoni:

Thank you for the opportunity to comment on the draft Government Accountability Office (GAO) report, "Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records, Though Other Vulnerabilities Remain," (GAO-07-752), which addresses the federal government's role in providing records with Social Security numbers (SSNs) and other personal identifying information to state and local public recordkeepers.

While this report does not provide recommendations for the Office of Management and Budget (OMB), we would like to comment on the issue of truncated (partial) SSNs which was discussed in the report. OMB appreciates the careful analysis that GAO provides in its report. In its report, GAO notes SSN, in both full and truncated form, remain vulnerable to misuse by identity thieves. Your report states that this is attributed in part due to external factors such as differing methods of truncation used by the public and private sectors, the availability of the SSN in public records and through the Internet, and the relative ease with which a partial SSN can be used to reconstruct a full SSN. The report further notes that, although an improvement over full SSN, truncation does not provide complete protection against identity theft and advises agencies the best protection is to reduce exposure.

On May 23, 2007, our Deputy Director for Management issued Memorandum M-07-16 to Federal agencies titled, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." (www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf) The Memorandum and its attachments require agencies to take actions which address the issue of data breaches including, among other things:

- develop and implement a risk-based breach notification policy within the required framework presented through the attachments;
- protect Federal information accessed remotely; and
- develop and implement a policy outlining the rules of behavior and identifying consequences and potential corrective actions for failure to follow these rules.

Additionally, this Memorandum requires agencies to reduce the volume of sensitive information maintained by agencies, including SSNs, to the minimum necessary. OMB further recognizes the path forward is for the Federal government to reduce its reliance on use of SSN. In this light, the Memorandum requires agencies to participate in government-wide efforts to explore alternatives to the use of SSNs as a personal identifier for both Federal employees and in Federal programs (e.g., surveys, data calls, etc.). The Memorandum goes a step further to require agencies to establish a plan within 120 days to eliminate unnecessary use of SSNs and implement the plan within 18 months.

The Memorandum does not distinguish between full and truncated SSNs. OMB has been providing informal advice to the agencies that the policy applies to both the full and truncated SSN. Specifically, agencies are required to safeguard SSN in any form with equal diligence. We will be providing more formal guidance to the agencies on this issue.

Thank you for the opportunity to review and comment on the draft report on this important issue.

Sincerely,



Karen Evans
Administrator
Office of E-Government and
Information Technology
Office of Management and Budget

Appendix III: Comments from the Internal Revenue Service



COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

May 24, 2007

Mr. Daniel Bertoni
Director, Education, Workforce, and
Income Security Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Bertoni:

I have reviewed the draft Government Accountability Office (GAO) briefing document titled: "Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records though Other Vulnerabilities Remain" (GAO 07-752).

The Internal Revenue Service (IRS) recognizes the importance of preventing identity theft and agrees that truncation of Social Security Numbers (SSNs) on documents provided to public record keepers provides an added level of protection against identity theft. In January 2006, the Service implemented truncation of SSNs on Notices of Federal Tax Liens (NFTLs) issued after that date. IRS will also truncate SSNs on certificates of release related to those filings. During fiscal year 2006, SSNs were truncated on over 600,000 NFTLs.

If you have any questions, or if you would like to discuss this response in more detail, please contact Fredrick W. Schindler, Director, Collection Policy at (202) 283-7650.

Sincerely,

A handwritten signature in black ink, appearing to read "Kevin Brown".

Kevin Brown
Acting Commissioner

Enclosure

Enclosure

Recommendation:

To the extent that truncation provides an added level of protection from identity theft, we are recommending that the Commissioner of IRS should implement a policy requiring the truncation of all SSNs in lien releases the agency generates.

Response:

The IRS agrees that truncating SSNs on documents filed with public record keepers adds a level of protection against identity theft. A multi-functional IRS task group contacted state and local recording officials, financial institutions, title and mortgage companies and credit reporting agencies, as well as attorneys and practitioners, and gathered data regarding truncation of SSNs. The group identified the most used truncation method as redaction of the first 5 digits of the SSN (i.e. xxx-xx-1234), the same method used by most recording officials and financial institutions. However, the data shows that truncating SSNs on lien releases, when original liens show full SSNs, may prove problematic for recording offices and may place an extreme hardship on lien processing capabilities. Based on the assembled data, IRS implemented changes to its automated lien system and provided guidance for manually prepared lien documents.

Effective January 1, 2006, in an effort to prevent identity theft and in recognition of the growing number of states requiring truncation, we began truncating SSNs on NFTLs. We will also truncate SSNs on lien documents that impact these filings (generated after 1/1/2006), such as certificates of release, withdrawal, and revocation.

Related GAO Products

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: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain. [GAO-05-1016T](#). Washington, D.C.: September 15, 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: Use Is Widespread and Protections Vary in Private and Public Sectors. [GAO-04-1099T](#). Washington, D.C.: September 28, 2004.

Social Security Numbers: Use Is Widespread and Protections Vary. [GAO-04-768T](#). Washington, D.C.: June 15, 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: Ensuring the Integrity of the SSN. [GAO-03-941T](#). Washington, D.C.: July 10, 2003.

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

Social Security Numbers: SSNs Are Widely Used by Government and Could Be Better Protected. [GAO-02-691T](#). Washington, D.C.: April 29, 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, 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