United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives

For Release on Delivery
Expected at 1:00 p.m. EST
Thursday, July 10, 2003

SOCIAL SECURITY NUMBERS

Ensuring the Integrity of the SSN

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

G A O

Accountability * Integrity * Reliability

GAO-03-941T

July 10, 2003

SOCIAL SECURITY NUMBERS

Ensuring the Integrity of the SSN

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-941T, a report to the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives

Why GAO Did This Study

In 1936, the Social Security Administration (SSA) established the Social Security Number (SSN) to track worker's earnings for social security benefit purposes. However, the SSN is also used for a myriad of non-Social Security purposes. Today, the SSN is used, in part, as a verification tool for services such as child support collection, law enforcement enhancements, and issuing credit to individuals. Although these uses of SSNs are beneficial to the public, SSNs are also a key piece of information in creating false identities. Moreover, the aggregation of personal information, such as SSNs, in large corporate databases, as well as the public display of SSNs in various public records, may provide criminals the opportunity to commit identity crimes. SSA, the originator of the SSN, is responsible for ensuring SSN integrity and verifying the authenticity of identification documents used to obtain SSNs.

Although Congress has passed a number of laws to protect an individual's privacy, the continued use and reliance on SSNs by private and public sector entities and the potential for misuse underscores the importance of identifying areas that can be strengthened. Accordingly, this testimony focuses on describing (1) public and private sector use and display of SSNs, and (2) SSA's role in preventing the proliferation of false identities.

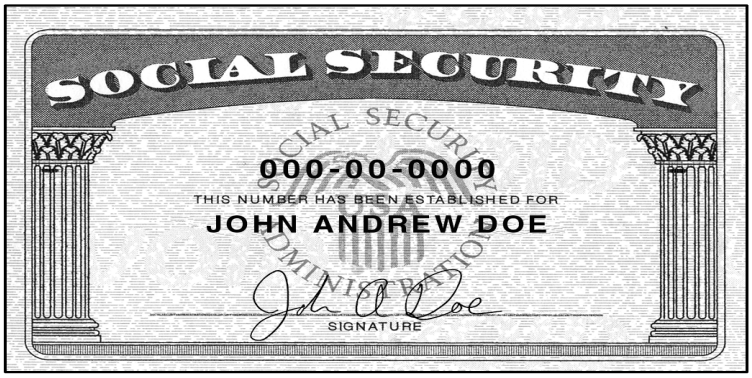
www.gao.gov/cgi-bin/getrpt?GAO-03-941T.

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

What GAO Found

Public and some private sector entities rely extensively on SSNs. We reported last year that federal, state and county government agencies rely on the SSN to manage records, verify eligibility of benefit applicants, and collect outstanding debt. SSNs are also displayed on a number of public record documents that are routinely made available to the public. To improve customer service, some state and local government entities are considering placing more public records on the Internet. In addition, some private sector entities have come to rely on the SSN as an identifier, using it and other information to accumulate information about individuals. This is particularly true of entities that amass public and private data, including SSNs, for resale. Certain laws have helped to restrict the use of SSN and other information by these private sector entities to specific purposes. However, as a result of the increased use and availability of SSN information and other data, more and more personal information is being centralized into various corporate and public databases. Because SSNs are often the identifier of choice among individuals seeking to create false identities, to the extent that personal information is aggregated in public and private sector databases it becomes vulnerable to misuse.

As the agency responsible for issuing SSNs and maintaining the earnings records for millions of SSN holders, SSA plays a unique role in helping to prevent the proliferation of false identities. Following the events of September 11, 2001, SSA formed a task force to address weaknesses in the enumeration process and developed major new initiatives to prevent the inappropriate assignment of SSNs to non-citizens, who represent the bulk of new SSNs issued by SSA's 1,333 field offices. SSA now requires field staff to verify the identity information and immigration status of all non-citizen applicants with the Department of Homeland Security (DHS), prior to issuing an SSN. However, other areas remain vulnerable and could be targeted by those seeking fraudulent SSNs. These include SSA's process for assigning social security numbers for children under age one and issuing replacement social security cards. SSA also provides a service to states to verify the SSNs of driver license applicants. Fewer than half the states have used SSA's service and the extent to which they regularly use it varies. Factors such as cost, problems with system reliability, and state priorities and policies affect states' use SSA's service. We also identified a weakness in SSA's verification service that exposes some states to fraud by those using the SSNs of deceased persons.



Source: GAO, Social Security Administration.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss ways to better protect Social Security Numbers (SSN) to help prevent the proliferation of false identities whether for financial misuse or for assuming an individual's identity. Although the Social Security Administration (SSA) originally created SSNs as a means to track worker's earnings and eligibility for Social Security benefits, over time the SSN has come to be used for a myriad of purposes. As you know, SSNs are a key piece of information in creating false identities. Allegations of SSN misuse include, for example, incidents where a criminal uses the SSN of another individual for the purpose of fraudulently obtaining credit, acquiring goods, violating immigration laws, or fleeing the criminal justice system.

Although Congress has passed a number of laws to protect the security of personal information, the continued use of and reliance on SSNs by private and public sector entities and the potential for misuse underscores the importance of identifying areas that can be further strengthened. Accordingly, you asked us to talk about the uses of SSNs and ways that the integrity of the SSN may be preserved. My remarks today will focus on describing (1) public and private sector use and display of SSNs and (2) SSA's role in preventing the proliferation of false identities. My testimony is based on a report we did for this Subcommittee on government uses of the SSN,[1] ongoing work that focuses on private sector SSN uses, and work we are completing on SSA's enumeration process and the agency's verification of SSNs for state driver licensing.

In summary, public and some private sector entities rely extensively on SSNs. We reported last year that federal, state, and county government agencies rely extensively on the SSN to manage records, verify eligibility of benefit applicants, collect outstanding debt, and conduct research and program evaluations. SSNs are also displayed on a number of public record documents that are routinely made available to the public. To improve customer service, some state and local government entities are considering placing more public records on the Internet. In addition, some private sector entities have come to rely on the SSN as an identifier, using it and other information to accumulate information about individuals. This

[1]U.S. General Accounting Office, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352 (Washington D.C.: May 31, 2002).

is particularly true of entities that amass public and private data, including SSNs, for resale. Certain laws have helped to restrict the use of SSNs and other information by these private sector entities to specific purposes. However, as a result of the increased use and availability of SSN information and other data, more and more personal information is being centralized into various corporate and public databases. Because SSNs are often the identifier of choice among individuals seeking to create false identities, to the extent that personal information is aggregated in public and private sector databases, it becomes vulnerable to misuse.

As the agency responsible for issuing SSNs and maintaining the earnings records and other personal information for millions of SSN holders, SSA plays a unique role in helping to prevent the proliferation of false identities. Following the events of September 11, 2001, SSA formed a task force to address weaknesses in the enumeration process and developed major new initiatives to prevent the inappropriate assignment of SSNs to noncitizens, who represent the bulk of new SSNs issued by SSA's 1,333 field offices. For example, SSA now requires field staff to independently verify the identity information and immigration status of all noncitizen applicants with the Department of Homeland Security (DHS), prior to issuing an SSN. However, some SSA field staff are relying exclusively on the DHS verification system, while neglecting other standard practices for visually inspecting documents. SSA's automated system for assigning SSNs also does not prevent the issuance of a SSN if staff by-pass required verification steps. Other areas remain vulnerable and could be targeted by those seeking fraudulent SSNs. These include SSA's process for assigning SSNs for children under age one and issuing replacement social security cards. In addition to its enumeration process, SSA provides a service to states to verify the SSNs of individuals seeking driver's licenses. We found that fewer than half the states have used SSA's service and the extent to which they regularly use the service varies widely across states. Factors such as cost, problems with system reliability, and state priorities and policies determine whether or not states use SSA's service. We also identified a weakness in SSA's verification service that exposes some states to fraud by those who would use the SSN of a deceased individual.

Background

The Social Security Act of 1935 authorized the SSA to establish a recordkeeping system to help manage the Social Security program, and resulted in the creation of the SSN. Through a process known as "enumeration," unique numbers are created for every person as a work and retirement benefit record for the Social Security program. Today, SSNs are generally issued to most U.S. citizens and are also available to

noncitizens lawfully admitted to the United States with permission to work. Lawfully admitted noncitizens may also qualify for a SSN for nonwork purposes when a federal, state, or local law requires a SSN to obtain a particular welfare benefit or service. SSA staff collect and verify information from such applicants regarding their age, identity, citizenship, and immigration status. Most of the agency's enumeration workload involves U.S. citizens who generally receive SSNs via SSA's birth registration process handled by hospitals. However, individuals seeking SSNs can also apply in person at any of SSA's field locations, through the mail, or via the Internet.

The uniqueness and broad applicability of the SSN have made it the identifier of choice for government agencies and private businesses, both for compliance with federal requirements and for the agencies' and businesses' own purposes. In addition, the boom in computer technology over the past decades has prompted private businesses and government agencies to rely on SSNs as a way to accumulate and identify information for their databases. As such, SSNs are often the identifier of choice among individuals seeking to create false identities. Law enforcement officials and others consider the proliferation of false identities to be one of the fastest growing crimes today. In 2002, the Federal Trade Commission received 380,103 consumer fraud and identity theft complaints, up from 139,007 in 2000.[2] In 2002, consumers also reported losses from fraud of more than $343 million. In addition, identity crime accounts for over 80 percent of social security number misuse allegations according to the SSA.

Public and Private Sector Uses and Display of SSNs

As we reported to you last year, federal, state, and county government agencies use SSNs.[3] When these entities administer programs that deliver services and benefits to the public, they rely extensively on the SSNs of those receiving the benefits and services. Because SSNs are unique identifiers and do not change, the numbers provide a convenient and efficient means of managing records. They are also particularly useful for data sharing and data matching because agencies can use them to check or compare their information quickly and accurately with that from other agencies. In so doing, these agencies can better ensure that they pay benefits or provide services only to eligible individuals and can more

[2]Identity theft records broken out of consumer fraud totaled per year: 31,117 (2000), 86,198 (2001), and 161,819 (2002).

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

readily recover delinquent debts individuals may owe. In addition to using SSNs to deliver services or benefits, agencies also use or share SSNs to conduct statistical research and program evaluations. Moreover, most of the government departments or agencies we surveyed use SSNs to varying extents to perform some of their responsibilities as employers, such as paying their employees and providing health and other insurance benefits.

Many of the government agencies we surveyed in our work last year reported maintaining public records that contain SSNs. This is particularly true at the state and county level where certain offices such as state professional licensing agencies and county recorders' offices have traditionally been repositories for public records that may contain SSNs. These records chronicle the various life events and other activities of individuals as they interact with the government, such as birth certificates, professional licenses, and property title transfers. Generally, state law governs whether and under what circumstances these records are made available to the public, and they vary from state to state. They may be made available for a number of reasons, including the presumption that citizens need key information to ensure that government is accountable to the people. Certain records maintained by federal, state, and county courts are also routinely made available to the public. In principle, these records are open to aid in preserving the integrity of the judicial process and to enhance public trust and confidence in the judicial process. At the federal level, access to court documents generally has its grounding in common law and constitutional principles. In some cases, public access is also required by statute, as is the case for papers filed in a bankruptcy proceeding. As with federal courts, requirements regarding access to state and local court records may have a state common law or constitutional basis or may be based on state laws.

Although public records have traditionally been housed in government offices and court buildings, to improve customer service, some state and local government entities are considering placing more public records on the Internet. Because such actions would create new opportunities for gathering SSNs from public records on a broad scale, we are beginning work for this Subcommittee to examine the extent to which SSNs in public records are already accessible via the Internet.

In our current work, we found that some private sector entities also rely extensively on the SSN. Businesses often request an individual's SSN in exchange for goods or services. For example, some businesses use the SSN as a key identifier to assess credit risk, track patient care among multiple providers, locate bankruptcy assets, and provide background

checks on new employees. In some cases, businesses require individuals to submit their SSNs to comply with federal laws such as the tax code. Currently, there is no federal law that generally prohibits businesses from requiring a person's SSN as a condition of providing goods and services. If an individual refuses to give his or her SSN to a company or organization, they can be refused goods and services unless the SSN is provided.

To build on previous work we did to determine certain private sector entities use of SSNs, we have focused our initial private sector work on information resellers and consumer reporting agencies (CRAs).[4] Some of these entities have come to rely on the SSN as an identifier to accumulate information about individuals, which helps them determine the identity of an individual for purposes such as employment screening, credit information, and criminal histories. This is particularly true of entities, known as information resellers, who amass personal information, including SSNs. Information resellers often compile information from various public and private sources.[5] These entities provide their products and services to a variety of customers, although the larger ones generally limit their services to customers that establish accounts with them, such as entities like law firms and financial institutions. Other information resellers often make their information available through the Internet to persons paying a fee to access it.

CRAs are also large private sector users of SSNs. These entities often rely on SSNs, as well as individuals' names and addresses to build and maintain credit histories. Businesses routinely report consumers' financial transactions, such as charges, loans, and credit repayments to CRAs. CRAs use SSNs to determine consumers' identities and ensure that incoming consumer account data is matched correctly with information already on file.

Certain laws such as the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Driver's Privacy Protection Act have helped to limit the use of personal information, including SSNs, by information resellers and

[4]U.S. General Accounting Office, *Social Security: Government and Commercial Use of the Social Security Number is Widespread*, GAO/HEHS-99-28 (Washington, D.C.: Feb. 16, 1999).

[5]The information compiled may include public records of bankruptcy, tax liens, civil judgments, criminal histories, deaths, real estate ownership, driving histories, voter registration, and professional licenses. Private data sources include information from telephone directories and copyrighted publications.

CRAs. These laws limit the disclosure of information by these entities to specific circumstances. In our discussion with some of the larger information resellers and CRAs, we were told that they take specific actions to adhere to these laws, such as establishing contracts with their clients specifying that the information obtained will be used only for accepted purposes under the law.

The extensive public and private sector uses of SSNs and availability of public records and other information, especially via the Internet, has allowed individuals' personal information to be aggregated into multiple databases or centralized locations. In the course of our work, we have identified numerous examples where public and private databases has been compromised and personal data, including SSNs, has been stolen. In some instances, the display of SSNs in public records and easily accessible Web sites provided the opportunity for identity thieves. In other instances, databases not readily available to outsiders have had their security breached by employees with access to key information. For example, in our current work, we identified a case where two individuals obtained the names and SSNs of 325 high-ranking U.S. military officers from a public Web site, then used those names and identities to apply for instant credit at a leading computer company. Although criminals have not accessed all public and private databases, such cases illustrate that these databases are vulnerable to criminal misuse.

SSA Has a Role in Preventing SSNs from Being Used to Create False Identities but Some Areas Remain Vulnerable

Because SSA is the issuer and custodian of SSN data, SSA has a unique role in helping to prevent the proliferation of false identities. Following the events of September 11, 2001, SSA began taking steps to increase management attention on enumeration and formed a task force to address weaknesses in the enumeration process. As a result of this effort, SSA has developed major new initiatives to prevent the inappropriate assignment of SSNs to noncitizens. However, our preliminary findings to date identified some continued vulnerabilities in the enumeration process, including SSA's process for issuing replacement Social Security cards and assigning SSNs to children under age one. SSA is also increasingly called upon by states to verify the identity of individuals seeking driver licenses. We found that fewer than half the states have used SSA's service and the extent to which they regularly use the service varies widely. Factors such as costs, problems with system reliability, and state priorities have affected states' use of SSA's verification service. We also identified a key weakness in the service that exposes some states to inadvertently issuing licenses to individuals using the SSNs of deceased individuals. We plan to issue reports on these issues in September that will likely contain

recommendations to improve SSA's enumeration process and its SSN verification service.

SSA's Enumeration Process Helps Prevent the Proliferation of False Identities, but Additional Actions are Needed to Safeguard the Issuance of SSNs

SSA has increased document verifications and developed new initiatives to prevent the inappropriate assignment of SSNs to noncitizens who represent the bulk of all initial SSNs issued by SSA's 1,333 field offices. Despite SSA's progress, some weaknesses remain. SSA has increased document verifications by requiring independent verification of the documents and immigration status of all noncitizen applicants with the issuing agency—namely DHS and the Department of State (State Department) prior to issuing the SSN. However, many field office staff we interviewed are relying heavily on DHS's verification service, while neglecting standard, in-house practices for visually inspecting and verifying identity documents. We also found that while SSA has made improvements to its automated system for assigning SSNs, the system is not designed to prevent the issuance of a SSN if field staff by-pass essential verification steps. SSA also has begun requiring foreign students to show proof of their full-time enrollment, and a number of field office staff told us they may verify this information if the documentation appears suspect. However, SSA does not require this verification step, nor does the agency have access to a systematic means to independently verify students' status. Consequently, SSNs for noncitizen students may still be improperly issued.

SSA has also undertaken other new initiatives to shift the burden of processing noncitizen applications from its field offices. SSA recently piloted a specialized center in Brooklyn, New York, which focuses exclusively on enumeration and utilizes the expertise of DHS document examiners and SSA Office of Inspector General's (OIG) investigators. However, the future of this pilot project and DHS' participation has not yet been determined. Meanwhile, in late 2002, SSA began a phased implementation of a long-term process to issue SSNs to noncitizens at the point of entry into the United States, called "Enumeration at Entry" (EAE). EAE offers the advantage of using State Department and DHS expertise to authenticate information provided by applicants for subsequent transmission to SSA who then issues the SSN. Currently, EAE is limited to immigrants age 18 and older who have the option of applying for a SSN at one of the 127 State Department posts worldwide that issue immigrant visas. SSA has experienced problems with obtaining clean records from both the State Department and DHS, but plans to continue expanding the program over time to include other noncitizen groups, such as students

and temporary visitors. SSA also intends to evaluate the initial phase of EAE in conjunction with the State Department and DHS.

While SSA has embarked on these new initiatives, it has not tightened controls in two key areas of its enumeration process that could be exploited by individuals seeking fraudulent SSNs. One area is the assignment of SSNs to children under age one. Prior work by SSA's Inspector General identified the assignment of SSNs to children as an area prone to fraud because SSA did not independently verify the authenticity of various state birth certificates. Despite the training and guidance provided to field office employees, the OIG found that the quality of many counterfeit documents was often too good to detect simply by visual inspection. Last year, SSA revised its policies to require that field staff obtain independent third party verification of the birth records for U.S. born individuals age one and older from the state or local bureau of vital statistics prior to issuing a SSN card.[6] However, SSA left in place its policy for children under age one and continues to require only a visual inspection of documents, such as birth records.

SSA's policies relating to enumerating children under age one expose the agency to fraud. During our fieldwork, we found an example of a noncitizen who submitted a counterfeit birth certificate in support of a SSN application for a fictitious U.S. born child under age one. In this case, the SSA field office employee identified the counterfeit state birth certificate by comparing it with an authentic one. However, SSA staff acknowledged that if a counterfeit out-of-state birth certificate had been used, SSA would likely have issued the SSN because of staff unfamiliarity with the specific features of the numerous state birth certificates. Further, we were able to prove the ease with which individuals can obtain SSNs by exploiting SSA's current processes. Working in an undercover capacity our investigators were able to obtain two SSNs. By posing as parents of newborns, they obtained the first SSN by applying in person at a SSA field office using a counterfeit birth certificate and baptismal certificate. Using

[6]Most U.S. born individuals receive a SSN through a process SSA refers to as Enumeration-at-Birth (EAB). Under EAB parents can apply for a SSN for their newborn child at the hospital as part of the birth registration process. Under this process hospitals send birth registration information to a state or local bureau of vital statistics where it is put into a database. SSA accepts the data captured during the birth registration process as evidence of age, identity, and citizenship, and assigns the child a SSN without further parental involvement. The appropriate bureau of vital statistics forwards SSA the required information, usually by electronic means. Once SSA receives the required information, it performs edits, assigns the SSN, and issues the card.

similar documents, a second SSN was obtained by our investigators who submitted all material via the mail. In both cases, SSA staff verified our counterfeit documents as being valid. SSA officials told us that they are re-evaluating their policy for enumerating children under age one. However, they noted that parents often need a SSN for their child soon after birth for various reasons, such as for income tax purposes. They acknowledge that a challenge facing the agency is to strike a better balance between serving the needs of the public and ensuring SSN integrity.

In addition to the assignment of SSNs to children under the age of one, SSA's policy for replacing Social Security cards also increases the potential for misuse of SSNs. SSA's policy allows individuals to obtain up to 52 replacement cards per year. Of the 18 million cards issued by SSA in fiscal year 2002, 12.4 million, or 69 percent, were replacement cards. More than 1 million of these cards were issued to noncitizens. While SSA requires noncitizens applying for a replacement card to provide the same identity and immigration information as if they were applying for an original SSN, SSA's evidence requirements for citizens are much less stringent. Citizens applying for a replacement card need not prove their citizenship; they may use as proof of identity such documents as a driver's license, passport, employee identification card, school identification card, church membership or confirmation record, life insurance policy, or health insurance card. The ability to obtain numerous replacement SSN cards with less documentation creates a condition for requestors to obtain SSNs for a wide range of illicit uses, including selling them to noncitizens. These cards can be sold to individuals seeking to hide or create a new identity, perhaps for the purpose of some illicit activity. SSA told us the agency is considering limiting the number of replacement cards with certain exceptions such as for name changes, administrative errors, and hardships. However, they cautioned that while support exists for this change within the agency, some advocacy groups oppose such a limit.

Field staff we interviewed told us that despite their reservations regarding individuals seeking excessive numbers of replacement cards, they were required under SSA policy to issue the cards. Many of the field office staff and managers we spoke to acknowledged that the current policy weakens the integrity of SSA's enumeration process.

SSA's Verification of Driver License Applicants Helps Prevent Fraudulent Documents, but Vulnerabilities Still Exist

The events of September 11, 2001, focused attention on the importance of identifying people who use false identity information or documents, particularly in the driver licensing process. Driver licenses are a widely accepted form of identification that individuals frequently use to obtain services or benefits from federal and state agencies, open a bank account, request credit, board an airplane, and carry on other important activities of daily living. For this reason, driver licensing agencies are points at which individuals may attempt to fraudulently obtain a license using a false name, SSN, or other documents such as birth certificates to secure this key credential.

Given that most states collect SSNs during the licensing process, SSA is uniquely positioned to help states verify the identity information provided by applicants. To this end, SSA has a verification service in place that allows state driver licensing agencies to verify the SSN, name, and date of birth of customers with SSA's master file of SSN owners. States can transmit requests for SSN verification in two ways. One is by sending multiple requests together, called the "batch" method, to which SSA reports it generally responds within 48 hours. The other way is to send an individual request on-line, to which SSA responds immediately.

Twenty-five states have used the batch or on-line method to verify SSNs with SSA and the extent to which they use the service on a regular basis varies. About three-fourths of the states that rely on SSA's verification service used the on-line method or a combination of the on-line and batch method, while the remaining states used the batch method exclusively. Over the last several years, batch states estimated submitting over 84 million batch requests to SSA compared to 13 million requests submitted by on-line users. States' use of SSA's on-line service has increased steadily over the last several years. However, the extent of use has varied significantly, with 5 states submitting over 70 percent of all on-line verification requests and one state submitting about one-third of the total.

Various factors, such as costs, problems with system reliability, and state priorities affect states' decisions regarding use of SSA's verification service. In addition to the per-transaction fees that SSA charges, states may incur additional costs to set up and use SSA's service, including the cost for computer programming, equipment, staffing, training, and so forth. Moreover, states' decisions about whether to use SSA's service, or the extent to which to use it, are also driven by internal policies, priorities, and other concerns. For example, some of the states we visited have policies requiring their driver licensing agencies to verify all customers' SSNs. Other states may limit their use of the on-line method to certain

targeted populations, such as where fraud is suspected or for initial licenses, but not for renewals of in-state licenses. The nonverifying states we contacted expressed reluctance to use SSA's verification service based on performance problems they had heard were encountered by other states. Some states cited concerns about frequent outages and slowness of the on-line system. Other states mentioned that the extra time to verify and resolve SSN problems could increase customer waiting times because a driver license would not be issued until verification was complete.

Indeed, weaknesses in SSA's design and management of its SSN on-line verification services have limited its usefulness and contributed to capacity and performance problems. SSA used an available infrastructure to set up the system and encountered capacity problems that continued and worsened after the pilot phase. The capacity problems inherent in the design of the on-line system have affected state use of SSA's verification service. Officials in one state told us that they have been forced to scale back their use of the system because they were told by SSA that their volume of transactions were overloading the system. In addition, because of issues related to performance and reliability, no new states have used the service since the summer of 2002. At the time of our review, 10 states had signed agreements with SSA and were waiting to use the on-line system and 17 states had received funds from the Department of Transportation for the purpose of verifying SSNs with SSA. It is uncertain how many of the 17 states will ultimately opt to use SSA's on-line service. However, even if they signed agreements with SSA today, they may not be able to use the service until the backlog of waiting states is addressed. More recently, SSA has made some necessary improvements to increase system capacity and to refocus its attention to the day-to-day management of the service. However, at the time of our review, the agency still has not established goals for the level of service it will provide to driver licensing agencies.

In reviewing SSA's verification service, we identified a key weakness that expose some states to issuing licenses to applicants using the personal information of deceased individuals. Unlike the on-line service, SSA does not match batch requests against its nationwide death records. As a result, the batch method will not identify and prevent the issuance of a license in cases where an SSN name and date of birth of a deceased individual is being used. SSA officials told us that they initially developed the batch method several years ago and they did not design the system to match SSNs against its death files. However, in developing the on-line system for state driver licensing agencies, a death match was built into the new

process. At the time of our review, SSA acknowledged that it had not explicitly informed states about the limitation of the batch service.

Our own analysis of one month of SSN transactions submitted to SSA by one state using the batch method identified at least 44 cases in which individuals used the SSN, name, and date of birth of persons listed as deceased in SSA's records to obtain a license or an identification card.[7] We forwarded this information to state investigators who quickly confirmed that licenses and identification cards had been issued in 41 cases and were continuing to investigate the others. To further assess states' vulnerability in this area, our own investigators working in an undercover capacity were able to obtain licenses in two batch states using a counterfeit out-of-state license and other fraudulent documents and the SSNs of deceased persons. In both states, driver licensing employees accepted the documents we submitted as valid. Our investigators completed the transaction in one state and left with a new valid license.[8] In the second state, the new permanent license arrived by mail within weeks. The ease in which they were able to obtain these licenses confirmed the vulnerability of states currently using the batch method as a means of SSN verification. Moreover, states that have used the batch method in prior years to clean up their records and verify the SSNs of millions of driver license holders, may have also unwittingly left themselves open to identity theft and fraud.

Conclusions

The use of SSNs by both public and private sector entities is likely to continue given that it is used as the key identifier by most of these entities and there is currently no other widely accepted alternative. To help control such use, certain laws have helped to safeguard such personal information, including SSNs, by limiting disclosure of such information to specific purposes. To the extent that personal information is aggregated in public and private sector databases, it becomes vulnerable to misuse. In addition, to the extent that public record information becomes more available in an electronic format, it becomes more vulnerable to misuse. The ease of access the Internet affords could encourage individuals to engage in information gathering from public records on a broader scale

[7]SSA's death records may contain inaccuracies because SSA records all reports of death but only verifies those involving benefit payments.

[8]This state does not use SSA's batch verification process for initial licenses, but only for license renewals. Therefore, the use of the deceased person's SSN will not be caught by the system when the state ultimately verifies it using the batch method.

than they could before when they had to visit a physical location and request or search for information on a case-by-case basis.

SSA has made substantial progress in protecting the integrity of the SSN by requiring that the immigration and work status of every non-citizen applicant be verified before an SSN is issued. However, without further system improvements and assurance that field offices will comply fully with the new policies and procedures this effort may be less effective than it could be. Further, as SSA closes off many avenues of unauthorized access to SSNs, perpetrators of fraud will likely shift their strategies to less protected areas. In particular, SSA's policies for enumerating children and providing unlimited numbers of replacement cards may well invite such activity, unless they too are modified.

State driver license agencies face a daunting task in ensuring that the identity information of those to whom they issues licenses is verified. States' effectiveness verifying individuals' identities is often dependent on several factors, including the receipt of timely and accurate identity information from SSA. Unfortunately, design and management weaknesses associated with SSA's verification service have limited its effectiveness. States that are unable to take full advantage of the service and others that are waiting for the opportunity to use it remain vulnerable to identity crimes. In addition, states that continue to rely primarily or partly on SSA's batch verification service still risk issuing licenses to individuals using the SSNs and other identity information of deceased individuals. This remains a critical flaw in SSA's service and states' efforts to strengthen the integrity of the driver license.

GAO is preparing to publish reports covering the work I have summarized within the next several months, which will include recommendations aimed at ensuring the integrity of the SSN. We look forward to continuing to work with this Subcommittee on these important issues. I would be happy to respond to any questions you or other members of the Subcommittee may have.

Contacts and Acknowledgments

For further information regarding this testimony, please contact Barbara D. Bovbjerg, Director, or Dan Bertoni, Assistant Director, Education, Workforce, and Income Security at (202) 512-7215. Individuals making key contributions to this testimony include, Andrew O'Connell, John Cooney, Tamara Cross, Paul DeSaulniers, Patrick DiBattista, Jason Holsclaw, George Ogilvie, George Scott, Jacquelyn Stewart, Robyn Stewart, and Tony Wysocki.