



SOCIAL SECURITY
Office of the Inspector General

June 22, 2011

The Honorable Sam Johnson
Chairman, Subcommittee on Social Security
Committee on Ways and Means
U.S. House of Representatives
Washington, D.C. 20515

Attention: Kim Hildred

Dear Mr. Chairman:

This is in response to your June 9, 2011 correspondence asking questions for the record, further to my testimony on April 13, 2011 before the Subcommittee on Social Security at a hearing on the role of Social Security numbers in identify theft and ways to guard their privacy. I appreciate the opportunity to provide additional information regarding this critical issue. Below are responses to your specific questions.

1. K-12 schools continue to use students' Social Security numbers (SSN) as authenticators. Would you provide an update of this practice? How can we encourage school systems to stop this practice?

In July 2010, the Social Security Administration (SSA) Office of the Inspector General (OIG) issued an audit report, *Kindergarten Through 12th Grade Schools' Collection and Use of Social Security Numbers* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-10-11057.pdf>). At the time of our audit, we identified laws in seven States¹ that required K-12 schools to obtain students' SSNs. Additionally, we identified schools in at least 26 other States² that collected students' SSNs at registration, even though no State law required it.³ We also noted that a recent university study identified a trend among State departments of education to establish longitudinal databases of all K-12 children to track students' progress over time.⁴

¹ The States were Alabama, Arkansas, Florida, Georgia, Kentucky, Virginia, and West Virginia. Although these States require an SSN for enrollment, they also may provide alternative numbers for individuals who refuse to provide their SSN or who are not eligible for an SSN.

² The States were Connecticut, Delaware, Hawaii, Illinois, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Nebraska, Nevada, New Hampshire, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Texas, Utah, Wisconsin, and Wyoming.

³ We do not suggest that these are the only States in which K-12 schools collect SSNs at registration.

⁴ Joel R. Reidenberg et al., Fordham Law School Center on Law and Information Policy, *Children's Educational Records and Privacy*, October 2009.

The study found that privacy protections for these databases were generally lacking in most States.

In our report, we acknowledged that four States had enacted laws to prohibit K-12 schools or State educational agencies from using SSNs as primary student identifiers.⁵ However, we believe Federal legislation is needed to limit the collection, use, and disclosure of SSNs by K-12 schools—and by others who do not have a legitimate need for this information. SSA, the Congress, and the U.S. Department of Education can educate States about the dangers of this practice, and encourage them to use an alternate student identifier. Without Federal law and regulation, States may not have a strong incentive to change this practice.

2. Do you believe we are winning or losing the growing battle of ID theft? Why or why not?

We believe the Federal Trade Commission (FTC) would be better suited to provide this information, as it maintains comprehensive information on identity theft statistics and trends. With regard to our experience, SSN misuse cases made up approximately five percent of our investigative casework during fiscal years (FY) 2009 and 2010, totaling 350 and 318 cases, respectively. Although these statistics reflect a short period, we believe our focus on this issue has remained generally consistent over time.

Identity theft is a complex issue, and therefore, winning this battle involves many factors. We appreciate the work of this Subcommittee and believe there has been progress through legal changes championed by your current and past members. Additionally, my office is passionate in its responsibility to protect the SSN, and SSA has been proactive in making significant changes to improve controls within its enumeration process. However, tackling this problem necessitates widespread changes in areas such as immigration law, employment eligibility requirements, regulations over the collection and use of personal information, resources dedicated to enforcement on the Federal, State, and local levels, and even larger societal behaviors and beliefs. Therefore, we would be hard-pressed to opine that we are “winning” this battle.

3. How has ID theft changed over the last several years? Is it more widespread, sophisticated and harder to stop? Are there trends towards organized crime or state sponsored ID theft?

We believe FTC would be better able to identify trends in identity theft. Based on our limited investigative data, we have not seen an increase in organized crime or state-sponsored identity theft.

4. What is the most common form of ID theft? Is it lost or stolen Social Security cards, death records that are sold with SSNs, or via some public listing or even the internet? Are there other trends that you can discuss?

⁵ The States were New Hampshire, Ohio, Rhode Island, and Wisconsin. However, such laws may not prevent K-12 schools from collecting and using SSNs for other purposes.

Currently, we do not track the form of identity theft on cases we investigate. However, we are concerned about the availability of personally identifiable information on the internet, including death records that include the individual's SSN—sold as the SSA Death Master File. FTC may have more data regarding common forms of identity theft.

5. Can you tell us what burdens may occur by removing ‘unnecessary’ display of SSNs? Is there a way to encourage proper use of SSNs while minimizing those burdens?

Although we have not conducted specific audit work to identify burdens associated with removing SSNs from display, anecdotally we know that such challenges involve significant systems changes, as well as the process of physically redacting SSNs from documents or websites. However, we identify below examples from past audit work in which governments and private entities took steps to protect sensitive information.

- In a December 2004 audit report, *Universities' Use of Social Security Numbers as Student Identifiers in Region IV* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-05-15034.pdf>), we noted that several schools had reduced or eliminated their reliance on SSNs; and some States enacted laws to regulate colleges' use of SSNs. For example, in 2003, the Georgia Institute of Technology (Georgia Tech) stopped using SSNs of students, faculty, and staff on identification cards and as the primary means of identification in campus databases, because of increased identity theft concerns. The university created the Georgia Tech Identification Number, which identifies students in most campus databases. The Associate Registrar told us the conversion took two years of planning, but was not difficult. In fact, she stated the actual conversion took place over a weekend. We heard similar stories from universities across the country.
- In a September 2007 audit report, *State and Local Governments' Collection and Use of Social Security Numbers* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-07-17086.pdf>), we identified 11 States that had taken steps to remove SSNs from public documents, and 24 States that passed laws to prohibit SSNs from being on public documents. We also identified 15 States that passed laws to prohibit publicly displaying SSNs, printing them on cards, transmitting them over the Internet, and mailing them without safety measures. For example, Maricopa County, Arizona, had begun redacting SSNs from 83 million public documents posted on the Internet. County officials told us they undertook this \$4.5-million project in response to identity theft concerns, constituent complaints about the online SSN postings, and the desire to take a proactive approach to this issue. The county hired a contractor to redact the SSNs, and required that the contractor manually review each document to ensure all SSNs were removed. In fact, the county specified that two individuals review each document to ensure a 99.95-percent accuracy rate. The county also planned to purchase redaction software for its own future use.
- Finally, in a May 2008 audit report, *Removing Social Security Numbers from Medicare Cards* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-08-18026.pdf>), we identified Federal agencies, including the Departments of Veterans Affairs and Defense, that had removed the SSN from health insurance cards. Additionally, the Office of Personnel Management (OPM) directed all health insurance carriers affiliated with the Federal Employees Health Benefit Program to eliminate SSNs from insurance cards as soon as

practical. In making this change, OPM acknowledged that SSNs can serve as a critical link in identity theft cases and other crimes. In recent years, almost all health insurance carriers have removed SSNs from their health insurance cards. For example, a Blue Cross and Blue Shield of Texas official told us the company removed SSNs from about 10 million insurance cards (for both Federal and non-Federal subscribers). Although Blue Cross and Blue Shield still uses SSNs internally, it developed a unique identifier for use on insurance cards and correspondence.

6. Would you agree that thieves would have a harder time stealing a person's identity if we had better methods of authenticating consumers, or, in other words, better ways to prove a person is who they say they are?

Theoretically, we agree that thieves would have a harder time committing identity theft if there were better ways to prove a person is who they say they are. While SSA and the Department of Homeland Security (DHS) offer several authentication programs, they are neither fail-safe nor mandatory. These programs allow users to verify that a person's name and SSN combination is valid; and they identify deceased individuals. However, the programs will not detect all instances of identity theft, such as the misuse of a valid name and SSN combination. Therefore, other types of authentication, such as biometric verification, could be useful tools to verify a person's true identity. However, we have not performed audit work on biometric technologies to provide an opinion on their value. We describe SSA's and DHS' existing programs below.

- **Consent Based Social Security Number Verification (CBSV):** CBSV is a fee- and consent-based SSN service available to private businesses (including banks) and Federal, State, and local government agencies that need client SSN verification. Participating companies are required to obtain written consent from the individual before verifying the individual's SSN through CBSV, as required by the *Privacy Act of 1974*. CBSV verifies whether a name and SSN combination match the data in SSA's records. As of Calendar Year (CY) 2010, 124 companies had submitted about 1.3 million verification requests.
- **Social Security Number Verification Service (SSNVS):** SSNVS is a free online system, with a batch option, that allows employers and third-party submitters to verify employees' names and SSNs; and identifies deceased individuals. SSNVS helps ensure employees' names and SSNs match SSA records before their wage reports are submitted to SSA. In CY 2010, SSNVS processed about 106 million verification requests.
- **Employment Verification Program (E-Verify):** SSA supports DHS in administering the E-Verify program, which allows employers to verify electronically employee information taken from the *Employment Eligibility Verification* form (Form I-9) against Federal databases to verify the employment eligibility of newly hired citizens and noncitizens. E-Verify is voluntary for most employers and is provided at no charge. As of September 4, 2010, about 222,000 employers were enrolled to use E-Verify—and those employers had submitted approximately 15 million queries.

7. With respect to the Dr. Martinez case are there good examples of private or public sector entities doing more to recognize what has happened to a victim and in some way

“certify” his or her experience so he or she can move on with his or her life and not be repeatedly questioned about who they are?

Although we have not examined the practices of other private and public sector entities, we are aware of two initiatives that are intended to assist ID theft victims. First, when SSA assigns a new SSN because a person has been disadvantaged by the misuse of his/her number, SSA places a special indicator on the old SSN record to block issuance of replacement SSN cards and SSN printouts. In addition, FTC has an identity theft affidavit that the individual can fill out and keep as a permanent record to present to public and private entities if questioned about crimes committed using their identities.

If the Subcommittee would like my office to examine this issue further, we would be pleased to do so at your request.

8. What are your recommendations for legislation that Congress needs to pass regarding SSN protection?

We have worked closely with the Subcommittee in providing recommendations for legislation we believe Congress should enact to enhance SSN protection. Many of these recommendations have been included in prior legislation introduced by previous Chairmen of this Subcommittee, the most recent being H.R. 3306, introduced in the last session of Congress. Our recommendations focus on several areas.

- *The display, sale, and purchase of the SSN in the public and private sectors.* Among our recommendations for the protection of the confidentiality of the SSN:
 - uniform truncation of the SSN when displayed; i.e., using only the last four digits;
 - limiting access to those in government and the private sector with a need for access to the SSN for the effective administration of their duties;
 - prohibiting the display of the SSN on cards or tags required for access to goods services, or benefits, as well as on employee identification cards or tags; and
 - allowing for consent of the affected individual pursuant to regulations.
- *Enhanced enforcement.* Several of our recommendations regarding criminal penalties are in H.R. 3306, including amending section 208 of the *Social Security Act* to include:
 - possession of an SSN without lawful authority;
 - possession of an SSN card knowing it to have been stolen, counterfeited, or forged, or obtained from SSA by the use of false information;
 - disclosure, sale, or transfer by an individual of their own (or their child’s or relative’s) SSN with intent to deceive;
 - to offer on the internet for a fee, to acquire for any individual, or to assist in acquiring for any individual an SSN or a number that purports to be an SSN but is not acquired by the individual through SSA; and
 - penalties for SSA employees who knowingly and fraudulently issue SSNs or SSN cards (this would be a progressive penalty—up to 5 years for 50 or fewer, up to 10 years for 51 up to 100, and up to 20 years for over 100).

Additionally, several Assistant United States Attorneys (AUSA) have inquired as to whether section 208 of the *Social Security Act* contains a misdemeanor provision. It does not. Providing for a misdemeanor would provide AUSAs with greater leeway in plea negotiations with individuals charged under section 208.

Further, in the *Social Security Protection Act of 2004*, titles II, VII, and XVI were amended to provide that the court *may* order restitution pursuant to sections 3612, 3663, and 3664 of title 18 of the United States Code. If the court does not order full restitution, it has to explain on the record why it did not. Since the enactment of this legislation, several AUSAs have told my office that this provision should be mandatory. In addition to substituting “shall” for “may” in the statute, we would suggest that 18 U.S.C. § 3663A be substituted in place of 18 U.S.C. § 3663. 18 U.S.C. § 3663A(c)(1)(A)(ii) &(B) provides, in part, for mandatory restitution for an offense that is an offense against property under [title 18], ... including any offense committed by fraud or deceit; and, in which an identifiable victim or victims has suffered a physical injury or pecuniary loss.”

We also recommend amending the criminal provisions of title II, VIII, and XVI to provide for enhanced penalties relating to SSN misuse for more than one conviction, terrorism, drug trafficking, and crimes of violence. The recommendation is for up to 10 years if the individual has a prior offense under the applicable statute; up to 20 years if the crime facilitates drug trafficking or a crime of violence; and up to 25 years if it facilitates domestic or international terrorism.

Finally, we recommend amending section 1129 of the *Social Security Act*, to allow SSA to impose civil monetary penalties (CMP) for those who violate the current criminal provisions of section 208 relating to the SSN, and for the recommended criminal provisions above. The CMP program supplements the criminal enforcement tools available against SSN misuse. We have seen instances in the past in which an AUSA indicates they will decline criminal and civil prosecution in favor of our proceeding against the individual pursuant to the CMP program. Moreover, cases are often declined criminally because the fraud loss does not reach a minimum threshold required by the United States Attorney’s Office, which can range from \$25,000 up to \$100,000. In these cases, the ability to pursue a CMP has helped ensure that a person who has committed fraud against SSA’s programs will face consequences for that action.

- *Exempting the SSA OIG from the Computer Matching and Privacy Protection Act, 5 U.S.C. § 552a.* This would allow us to compare any Federal records with other Federal or non-Federal records, while conducting an audit, investigation, inspection, evaluation, or other review authorized to identify weaknesses that may lead to fraud, waste, or abuse, and to detect improper payments and fraud.

My office is available at the Subcommittee’s convenience to provide technical assistance in pursuing any of the aforementioned recommendations.

- 9. The Subcommittee is interested in removing the SSN from the Medicare card and inserting another identifying number for Medicare use, much like the military is doing with its ID cards. The SSA systems would not have to make any changes except**

interfacing with CMS to identify the new number with the correct SSN already in their system. Is this the simplest way to alter the system, and if so what are the costs and the time frames for achieving the change?

We issued an audit report regarding this issue in May 2008, *Removing Social Security Numbers from Medicare Cards* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-08-18026.pdf>). Nevertheless, we believe SSA and the Centers for Medicare and Medicaid Services would be better able to answer specific questions about costs, required system changes, and the time needed to make this change.

10. As you all testified, ID theft is one of the fastest growing crimes in America, and one of the reasons for this is the ease of finding SSNs on unprotected documents. In many states, each foster child receives an identity card with his or her SSN on the card, and the SSN is the primary identifier of the child. The federal government allows for an SSN change when a foster child is going through the adoption process. A new SSN largely cleans the financial slate for these children. Is issuing a new SSN a solution for minors, such as foster youth, who have been victims of ID theft? What is the impact of issuing a new SSN?

First, we are also concerned with the issue of identity theft among foster children. Therefore, we plan to initiate an audit of this issue in the next few months. We will share the results with the Subcommittee, and may be better able to respond to your questions at that time.

In general, however, SSA permits foster children (and other number holders) to obtain a new SSN if they continue to be disadvantaged by identity theft. According to SSA policy, if an individual (or, for a minor, their guardian) decides to apply for a new number, he or she must prove age, U.S. citizenship or lawful immigration status, and identity. He or she must also provide evidence that he or she is still being disadvantaged by the misuse. SSA cautions those who request a new SSN that a new number may not always stop the problems caused by identity theft. As SSA states (see <http://www.socialsecurity.gov/pubs/10064.html#new>):

Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit-reporting companies use the number, along with other personal information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

11. When a person uses an SSN to apply for credit or open an account, what mechanisms are there for the creditor to check the legitimacy of the SSN and whether or not it belongs to a minor? Would it raise a red flag if a creditor discovered the SSN belonged to a minor? Do creditors routinely check to determine if an SSN belongs to a minor?

We have not conducted audit or investigative work to respond adequately to these questions. However, we would be happy to review this issue at the Subcommittee's request. Alternatively, the Subcommittee may wish to pose these questions to FTC or to the major credit bureaus.

12. What are your recommendations for issuing SSNs to temporary workers? For foreign workers with SSNs, should it be possible for those numbers to be rescinded or suspended when the foreign worker leaves the country?

We have issued several audit reports highlighting vulnerabilities associated with assigning SSNs to certain noncitizen temporary workers. While we did not recommend that these SSNs be rescinded or suspended when these workers leave the country—and have performed no audit work to determine the feasibility of such actions—we have made several other recommendations, including changes in Federal law. While we could examine the possibility of SSN suspension or rescission at the request of the Subcommittee, in general, we believe these options would be logistically challenging for SSA to administer. To our knowledge, DHS still does not have *complete* information regarding departure dates of noncitizens. Without such information, SSA would have to rely on visa expiration dates, which often change. Thus, significant systems improvements and data-sharing arrangements would need to be in place before SSA could implement an accurate SSN suspension or rescission process.

Nevertheless, we do encourage legislation to address the requirement that SSA assign SSNs to noncitizens who are permitted to work temporarily in the country. In July 2007, we issued an audit report, *Assignment of Social Security Numbers to J-1 Exchange Visitors* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-07-17076.pdf>). J-1 exchange visitors who enter the United States as camp counselors or as a part of the “summer work/travel” program may work in the United States for 4 months, and must then return to their home countries. Under current law and regulation, because J-1s are eligible to work, they are eligible to obtain an SSN—even though they are exempt from paying Social Security taxes. Based on our estimates, SSA assigned approximately 100,000 SSNs to these categories of J-1 exchange visitors during FY 2005.

We believe this practice creates opportunities for potential SSN misuse. For example, an SSN makes it easier for exchange visitors to remain in the country and to continue working after their visa expires, which weakens SSN integrity and could affect homeland security. In addition, some exchange visitors leave their employer or return to their home country before receiving their SSN card, increasing the potential for dishonest individuals to obtain and misuse these cards. Further, some of the employers and SSA field office personnel with whom we spoke stated that exchange visitors who receive their SSN cards do not always adequately safeguard them—often misplacing the cards and requesting replacements. For these reasons, employers, international cultural exchange organizations, and field office personnel we interviewed questioned the assignment of SSNs to exchange visitors, and shared our concerns about the potential for SSN misuse.

We believe SSA and the Congress can reduce the risk of SSN misuse by considering alternatives to assigning SSNs to noncitizens who work in the United States for only a few months. One alternative could be to require the IRS to issue exchange visitors Individual Taxpayer Identification Numbers. We recommended that SSA seek such legislation in our audit report. However, the Agency disagreed with this proposal because our audit report did not identify specific instances of SSN misuse, and because such a policy would complicate SSA’s enumeration procedures.

We have similar concerns with K-1 fiancé visa holders, another category of noncitizens who may work temporarily in the United States. In May 2008, we issued an audit report, *Assignment of Social Security Numbers to Noncitizens with Fiancé Visas* (see <http://www.ssa.gov/oig/ADOBEPDF/A-08-07-17044.pdf>). U.S. citizens who consider marrying a citizen of another country may petition the U.S. Department of State to allow the noncitizen to enter the United States with a K-1 visa. The Department of State issues such visas for a 6-month period, during which the individual may enter the United States only once. Upon admission, however, the individual has 90 days to marry the U.S. citizen and apply for a change of status, or depart the country. Because they are eligible to work in the United States for this 90-day period, SSA must assign an SSN to K-1 applicants with proper DHS documentation.

K-1 visa holders are required to pay Social Security taxes. Further complicating this matter, section 466(a)(13) of the *Social Security Act*, 42 U.S.C. 666(a)(13), requires that anyone seeking a marriage license provide his or her SSN to the recording State. We believe assigning an SSN to a K-1 visa holder creates significant opportunities for SSN misuse, and could provide an avenue for those who choose not to marry to remain in the United States illegally. We believe laws should be revised so that K-1 visa holders are not assigned an SSN—until they marry a U.S. citizen and apply for permanent residency.

13. The number of replacement Social Security cards is now restricted. However, the number of printouts or “Numi Lites” is growing as individuals, or individuals prompted by law firms or other businesses, comes into the field offices for new printouts. The level of identity required for these is less than a new replacement card making them more open to ID theft. Should we be charging fees to remove the incentive to obtain repeat printouts and if so at what level should the fee be to cover costs and provide the proper disincentive? Should we also be charging a fee for replacement cards and what is the proper level to cover cost and still provide a disincentive to get multiple replacement cards?

We share the Subcommittee’s concern over the growth in demand for SSN printouts (Numi Lites), as well as the less probative identity documents required for number holders to obtain these documents. In December 2007, we issued an audit report, *Controls for Issuing Social Security Number Verification Printouts* (see <http://www.ssa.gov/oig/ADOBEPDF/A-04-07-27112.pdf>), making a number of recommendations to strengthen SSA’s process for issuing these sensitive documents. We are currently completing a second review to examine whether vulnerabilities still exist, and will issue that review by the end of FY 2011. We will provide a copy of this report to the Subcommittee.

Additionally, at Chairman Johnson’s request, we are examining the feasibility of charging user fees for certain SSA services, including issuing replacement Social Security cards and SSN printouts. We plan to issue the results of this study to the Subcommittee by the end of July 2011. In our report, we will discuss SSA’s estimated cost for processing these two workloads (an average of \$32 for issuing Social Security cards, and roughly \$20 for issuing

SSN printouts).⁶ We will also provide information regarding SSA’s estimated cost for processing remittances (\$26). Given our short timeframe, we will not be able to provide definitive costs that we feel would dissuade customers seeking these documents. However, we will provide options for your consideration. We would be happy to discuss the results of our review—and to explore further areas in which you may still have concerns.

14. In your testimony, you mentioned the Freedom of Information Act as a factor in obtaining printouts and replacement cards. Can you explain further the nexus between the two?

In compliance with both the *Privacy Act of 1974* and the *Social Security Act*, SSA’s information disclosure policy dictates that it will protect the privacy of individuals to the fullest extent possible, while permitting the exchange of information needed to fulfill its administrative and program responsibilities. Notwithstanding some exceptions, Federal law gives individuals the right to access information about themselves that is in SSA’s records.

Generally, individuals have access to SSA records that the Agency can retrieve by name, SSN, or other personal identifier. This includes SSN-related records, such as the original *Application for a Social Security Card*, the Numident,⁷ and the SSN printout. SSA’s policies for issuing SSN printouts are less stringent than those for issuing replacement SSN cards, because the Agency has attempted to comply with the spirit of the *Privacy Act*. That is, in compliance with the *Privacy Act* and OMB guidelines, Agency policies allow individuals to obtain these documents without undue burden. Nevertheless, SSA continues to issue a large number of SSN printouts—and this number has grown each year since the Agency began issuing them. As such, we believe SSA should improve its procedures to control and account for the issuance of SSN printouts, while also making efforts to reduce the unnecessary demand for the document as a form of SSN verification.

Thank you for the opportunity to clarify these issues for the Subcommittee on Social Security. I trust that I have been responsive to your request. If you have further questions, please feel free to contact me, or your staff may contact Misha Kelly, Congressional and Intra-Governmental Liaison, at (202) 358-6319.

Sincerely,

S

Patrick P. O’Carroll, Jr.
Inspector General

⁶ SSA charges third parties \$46 to provide an SSN printout with consent of the number holder (for example, an employer who requests an SSN printout with the consent of the employee). Of this fee, SSA estimates \$26 recovers the remittance cost for collecting the fee and \$20 recovers the cost of work performed in providing the SSN printout.

⁷ The Numident is an electronic record of the information contained on an individual’s original application for an SSN and subsequent applications for replacement cards. Numident printouts are not issued by SSA field offices. To obtain a Numident, an individual must send a written request to SSA’s Central Office, and pay a \$16 fee.