U.S. House of Representatives

Committee on Ways and Means
Subcommittee on Oversight
Subcommittee on Social Security

Statement for the Record

Hearing on Identity Theft and Tax Fraud

The Honorable Patrick P. O'Carroll, Jr.
Inspector General, Social Security Administration

May 8, 2012

Good morning, Chairman Johnson, Chairman Boustany, Ranking Member Becerra, Ranking Member Lewis, and members of both Subcommittees. It is a pleasure to appear before you, and I thank you for the invitation to testify today. I have appeared before Congress many times to discuss issues critical to the Social Security Administration (SSA) and the services the Agency provides to American citizens; earlier this year I testified before the Subcommittee on Social Security at separate hearings on SSA's Disability Insurance program and the Death Master File (DMF).

Today, we are discussing the Social Security number (SSN) and ways to improve SSN protection and guard against misuse, identity theft, and tax fraud. Your Subcommittees have previously worked with SSA and the Office of the Inspector General (OIG) to address these issues, but with SSN use widespread throughout government programs and financial transactions, and technology constantly evolving, the threat of SSN misuse and identity theft persists. My office is well aware of the central role that the SSN plays in American society, and part of our mission is to maintain its integrity along with other personally identifiable information (PII) within SSA records. To provide some context, in Fiscal Year (FY) 2011, SSA assigned about 5.4 million original SSNs, issued 10.9 million replacement cards, and processed more than 1.4 billion SSN verifications. The Agency also received about $660 billion in employment taxes related to earnings. Protecting the SSN and properly posting employees' wages is paramount to ensuring the integrity of our personal information.

Despite our efforts as well as those of SSA and the IRS to protect this critical information, we all remain targets for identity thieves. The Federal Trade Commission (FTC) estimates that as many as 9 million Americans have their identities stolen each year. The number of identity theft-related incidents on tax returns reached about 248,000 in 2010, about five times more than in 2008, according to the Government Accountability Office. We in the OIG understand the concern your Subcommittees have for citizens and their families with regard to identity theft, and we investigate as many SSN misuse cases as our resources allow each year. As we pursue these criminal investigations, we have also conducted numerous audits and made recommendations to SSA and to the Congress to improve the SSN's security.

SSN Misuse Investigations

OIG's primary mission is to protect SSA programs and operations, and the majority of our investigations are related to SSA program fraud. However, our organization receives thousands

of allegations of SSN misuse each year; in FY 2011, about 14 percent of all fraud referrals received involved SSN misuse. It is our experience that investigations into SSN misuse will often reveal some form of identity theft. At times, they can also involve Social Security benefit fraud and tax fraud that can lead to the recovery of significant government funds.

I would like to share with your Subcommittees some of our most recent cases involving SSN misuse for the purpose of tax fraud:

- The OIG, the IRS Criminal Investigation Division (CID), the Treasury Inspector General for Tax Administration, and other agencies conducted a joint investigation of several individuals who misused the names and SSNs of approximately 300 residents of Puerto Rico so they could file fraudulent tax returns. This scheme caused the IRS to issue more than $2 million in fraudulent tax refunds. A judge sentenced three individuals to between 3 months and 30 months in prison, and ordered them to pay restitution of nearly $230,000 to the IRS.
- My office investigated a California woman who used fraudulent SSNs to file Federal income tax returns. The woman applied for and obtained more than 20 Social Security cards, falsely claiming she gave birth to that many children at a Los Angeles hospital in 2002. The woman then prepared and filed fraudulent tax returns, claiming multiple dependent deductions for family members and friends. She recently pleaded guilty to theft, fraudulent use of SSNs, and preparing false tax returns. A judge sentenced her to 18 months' incarceration and ordered her to pay restitution of more than $302,000 to the IRS.
- The OIG, IRS CID, and other agencies investigated two New Jersey men who misused the names and SSNs of victims who used a health-service provider in the area. The men used the victims' personal information to file false tax returns, improperly claiming about $507,000 in refunds from the IRS. The men pleaded guilty in 2011, and a judge sentenced them to 60 months and 120 months in prison and ordered them to pay restitution of more than $207,000 and about $300,000 to the IRS, respectively.

As we pursue investigations similar to these, our agents also participate on about 45 SSN misuse task forces throughout the country, which cover mortgage fraud, bankruptcy fraud, and document and benefit fraud, as well as identity theft.

SSA's Death Master File

SSA has made significant efforts to improve SSN integrity and encourage individuals to protect PII. However, the SSNs of deceased individuals are also vulnerable to misuse. As such, the public release of the DMF raises concerns related to SSN misuse and identity theft, as seen in recent news media reports and evidenced by ongoing legislative efforts. SSA has, on the Numident—the Agency's master database of SSN holders—a record of reported deaths. Because of a Consent Judgment in a 1978 *Freedom of Information Act* (FOIA) lawsuit—*Perholtz vs. Ross*—SSA was required as of 1980 to provide death records that included the SSN, the last name, and the date of death of deceased number holders; the result was the creation of the DMF, an extract of Numident data. SSA later expanded the DMF to include individuals' first and middle name, date of birth, residential state and zip code.

In November 2011, SSA made changes to the DMF. First, the Agency ceased providing the decedent's residential state and Zip code. In addition, SSA removed about 4.2 million State records from the DMF, based on a provision in the *Social Security Act* prohibiting SSA from disclosing death records the Agency receives through its contacts with the States, except in limited circumstances.

Today, each DMF record usually includes the following: SSN, full name, date of birth, and date of death. Therefore, even with SSA's recent changes, the DMF still contains more information than required by the Consent Judgment in *Perholtz.* The file contains about 86 million records, and it adds about 1.1 million records each year.

SSA provides the DMF to the Department of Commerce's National Technical Information Service (NTIS), a clearinghouse for scientific and technical information, which, in turn, sells the DMF to public and private industries—government, financial, investigative, credit reporting, and medical customers. Those customers use the data to verify death and prevent fraud, among other uses. SSA also currently distributes all death information it maintains, including State death records, under agreements with eight government agencies, including the IRS and the Centers for Medicare & Medicaid Services. SSA provides this death information to the IRS weekly. SSA also provides IRS a weekly file that includes the names and SSNs of newborns, as well as their parents' names and SSNs.

Criminal Use of Public Death Records

The DMF has important and productive uses. For example, medical researchers and hospitals track former patients for their studies; investigative firms use the data to verify deaths related to investigations; and pension funds, insurance companies, and government entities need to know if they are sending payments to deceased individuals. In addition, the financial community and Federal, State, and local governments can identify and prevent identity theft by running financial and credit applications against the DMF. However, the form in which the DMF is currently distributed provides opportunity for individuals to misuse SSNs and commit identity theft.

These OIG investigations show how individuals can use available death data to obtain SSNs and commit fraud:

- In August 2010, we began investigating about 60 fraudulent retirement benefit claims that used the name, SSN, and date of birth of individuals who died decades ago. We determined that the PII used to file the fraudulent claims was available to the public through a genealogical website. The OIG and other law enforcement agencies identified suspects in the case and executed search and arrest warrants; however, the main suspect took his own life before he was taken into custody. His two accomplices, both relatives of his, were indicted and pled guilty to the charges. A judge sentenced the two individuals to 20 months' and 25 months' incarceration followed by deportation from the U.S., and one was ordered to pay restitution of more than $145,000 to SSA.
- An OIG investigation of a Colorado man revealed that he employed individuals so he could obtain names and SSNs of long-deceased individuals from a genealogical website. The man then fabricated employment records and instructed others to use the obtained names and SSNs and false employment information to create fraudulent tax returns, which were submitted to the IRS online. To determine deceased individuals' SSNs, the man said he compared data available from the public Internet site with a

certain State's death data. A judge sentenced the man to 46 months in prison for SSN misuse, making false claims, and wire fraud; and ordered him to pay more than $282,000 in restitution to the IRS.

According to news media reports, in December 2011, this genealogical website said it would no longer display the Social Security information for anyone who has died in the last 10 years; the site also said it would place its Social Security Death Index behind a pay wall and only allow access to the index to family history researchers.

The Congress has recognized the seriousness of this issue, as current bills for consideration address access to the DMF. In November 2011, Chairman Johnson and several members of the Subcommittee on Social Security introduced the *Keeping IDs Safe Act*, which would end the sale of the DMF. The bill would help protect the death data of all number holders. My office also supports an exemption to the bill that would allow government and Federal law enforcement agencies—like the OIG—to access the DMF to combat fraud.

Reviews and Recommendations

The OIG recognizes that limiting or discontinuing the DMF's availability is ultimately a legislative and policy decision for the Congress and SSA to make. Even so, my office has long taken the position that to the extent possible, SSA should limit public access to the DMF that required by law, and take all possible steps to ensure its accuracy. We have made several recommendations to this effect.

Our March 2011 report, *Follow-up: Personally Identifiable Information Made Available to the Public via the Death Master File*, examined whether SSA took corrective actions to address recommendations we made in a June 2008 report on the DMF. In the June 2008 report, we determined that, from January 2004 through April 2007, SSA's publication of the DMF resulted in the potential exposure of PII for more than 20,000 living individuals erroneously listed as deceased on the DMF. In some cases, these individuals' PII was still available for free viewing on the Internet—on ancestry sites like genealogy.com and familysearch.org—at the time of our report.

In the March 2011 report, we found SSA did not take actions on two of our recommendations. SSA did not implement a delay in the release of DMF updates, as the Agency indicated that public and private organizations rely on the DMF to combat fraud and identity theft. According to SSA, those organizations must have immediate and up-to-date information to be effective. The Agency also did not attempt to limit the amount of information included on the DMF, and it did not explore alternatives to the inclusion of an individual's full SSN, citing the *Perholtz* consent judgment and potential litigation under FOIA. SSA added that a deceased individual does not have a privacy interest, according to FOIA.

Our follow-up audit work indicated that between January 2008 and April 2010, SSA published at least 35,000 living numberholders' PII in the DMF. According to SSA, there are about 1,000 cases each month in which a living individual is mistakenly included in the DMF. SSA said that when the Agency becomes aware it has posted a death report in error, SSA moves quickly to correct the situation, and the Agency has not found evidence of past data misuse. However, we remain concerned about these errors, because erroneous death entries can lead to benefit termination and cause severe financial hardship and distress to affected individuals. We also have concerns that DMF update files, some with the SSNs of living individuals, are a potential

source of information that would be useful in perpetrating SSN misuse and identity theft. DMF updates can reveal to potential criminals the PII of individuals who are still alive.

Legislative Efforts

We support the prior bipartisan legislative efforts of these Subcommittees to limit the use, access, and display of the SSN in public and private sectors, and to increase penalties against those who misuse SSNs. Most recently, the Subcommittee on Social Security introduced the *Social Security Number Privacy and Identity Theft Prevention Act of 2009*. This legislation included new criminal penalties for the misuse of SSNs; criminal penalties for SSA employees who knowingly and fraudulently issue Social Security cards or SSNs; and enhanced penalties in cases of terrorism, drug trafficking crimes, or prior offenses.

The legislation would also expand the types of activities that are subject to civil monetary penalties (CMPs) and assessments under Section 1129 of the *Social Security Act*. Currently, an individual who misuses an SSN is not subject to a CMP, except in cases related to the receipt of Social Security benefits or Supplemental Security Income. The legislation would authorize the imposition of CMPs and assessments for activities such as providing false information to obtain an SSN, using an SSN fraudulently obtained, or counterfeiting an SSN.

The expanded use of the SSN in today's society has made it a valuable commodity for criminals. In addition to being a lynchpin for identity theft crimes, it also helps an individual assimilate into our society, and in some instances, to avoid detection. The importance of SSN integrity to prevent identity theft and ensure homeland security is universally recognized. Providing enhanced, structured penalties is appropriate to reflect the vital importance of the SSN.

Citizens' Accountability

While government agencies such as SSA have controls in place to protect the SSN and other personal information, individuals must also take basic preventive steps to protect their own information from improper use. We urge everyone to keep Social Security cards in a secure place, shred personal documents, and be aware of phishing schemes, because no reputable financial institution or company will ask for personal information like an SSN via the phone or the Internet. It is also important to protect personal computers with a firewall and updated anti-virus protection.

Additionally, we should all be judicious in giving out an SSN in business transactions, because while it is required for some financial transactions, an SSN is not necessary for everyday transactions, like applying for a gym membership. We can monitor our financial transactions and regularly check our credit reports from the three major credit bureaus. Concerned citizens may also contact SSA at 1-800-772-1213 if they suspect someone is using their SSN work purposes; SSA will review work earnings to ensure its records are correct. Anyone who suspects identity theft should report it to the FTC at 1-877-438-4338; and may need to contact the IRS to address potential tax issues. By knowing how to protect ourselves, and actually taking these important steps, we make life much more difficult for identity thieves.

Conclusion

SSA has a long history of protecting PII, and while current conditions may be the most challenging yet, we are confident SSA will rise to the occasion and address the challenges of

today and tomorrow. Identify theft will undoubtedly persist for years to come, because of the reliance on the SSN as a national identifier and advances in technology and communication. Nevertheless, we are committed to ensuring that the information in SSA's records remains safe and secure.

While we support efforts to limit public access to this data through legislative or policy changes (such as the *Keeping IDs Safe Act)*, barring such changes, SSA should implement a risk-based approach for distributing the DMF, and the Agency should limit the amount of information included on the DMF. These actions would protect PII and reduce the potential for misuse and abuse of SSNs and identity theft.

Our investigators are committed to pursuing SSN misuse and identity theft cases, and our auditors will continue to offer recommendations to safeguard the SSN and prevent theft of government funds. Finally, we will continue to provide information to your Subcommittees and Agency decision-makers about this critically important issue. I thank you again for the opportunity to speak with you today. I am happy to answer any questions.