

U.S. House of Representatives
Committee on Ways and Means
Subcommittee on Social Security

Statement for the Record

Field Hearing on Social Security Numbers and Child Identity Theft

Robert Feldt
Special Agent-in-Charge, Dallas Field Division, Social Security Administration

Antonio Puente
Special Agent, Dallas Field Division, Social Security Administration

September 1, 2011

Good afternoon, Chairman Johnson and members of the Subcommittee. It is a pleasure to appear before you, and I thank you for the invitation to testify today. My name is Robert Feldt, and I am the Special Agent-in-Charge of the Social Security Administration (SSA) Office of the Inspector General's (OIG) Dallas Field Division (FD), one of OIG's 10 field divisions across the country. The Dallas FD handles Social Security fraud investigations here in Texas, as well as in Arkansas, Louisiana, Oklahoma, and New Mexico. Today, we are discussing the Social Security number (SSN) and ways to improve SSN protection and guard against misuse and child identity theft.

Your Subcommittee has discussed this issue with SSA and OIG before, but with SSN use widespread throughout government programs and financial transactions, and technology constantly evolving, the threat of SSN misuse and identity theft persists. We in OIG are well aware of the central role that the SSN plays in American society, and part of our mission is to protect its integrity along with the other personally identifiable information (PII) within SSA records. To provide some context on the issue, in Fiscal Year (FY) 2010, SSA assigned 5.5 million original SSNs, issued 11.2 million replacement SSN cards, and processed more than 1 billion SSN verifications. The Agency also received about \$670 billion in employment taxes related to earnings under assigned SSNs. Protecting the SSN and properly posting wages under SSNs is paramount to ensuring SSN integrity and protecting our citizens' PII.

While adults across the United States strive to protect their SSN and their identity to maintain a good credit rating, a correct earnings record with SSA, and accurate tax returns with the Internal Revenue Service, children are now becoming targets for identity thieves. At a recent forum on child identity theft sponsored by the Federal Trade Commission (FTC), experts estimated that more than 140,000 U.S. children are victims of identity theft each year. Experts pointed to a trend wherein identity thieves are targeting cyber attacks on schools and pediatric centers to obtain children's SSNs, which are valuable because a child generally receives an SSN at birth, but does not use it for credit purposes for about 18 years. This allows for the potential long-term undetected abuse of a genuine SSN—and the potential long-term harm to a young person's financial future.

We in OIG understand the concern your Subcommittee has for families and their children with regard to identity theft, and we pursue as many SSN misuse cases as our resources allow each year. In FY 2010, the Dallas FD opened more than 700 investigations based on allegations of violations including Social Security disability fraud, SSA employee fraud, and SSN misuse. Our FY 2010 investigative efforts in the Dallas FD resulted in the recovery of more than \$3.2 million to SSA, and projected savings of more than \$43 million in SSA funds. As we pursue SSN misuse and identity theft cases when possible, we have also made numerous recommendations to SSA and to the Congress to improve the SSN's security.

SSN Protections

As the Subcommittee is well aware, SSA created the SSN in 1935 to keep an accurate record of each person's Social Security-covered earnings. However, over the years, Federal and State governments have relied on the SSN as the identifier of choice for a variety of programs. Financial institutions are also required to obtain the SSNs of their customers. With each new use, the SSN has more value, and when you create something of value, inevitably someone will try to steal it. In May 2006, President Bush established the National Identity Theft Task Force, which created directives for Federal agencies to strengthen efforts to protect against identity theft. Our reviews have found that SSA has followed these directives for years and strives to improve SSN integrity.

SSA has implemented numerous improvements in its SSN assignment, or enumeration, process. We believe SSA's improved procedures have reduced its risk of improperly assigning these important numbers. Some of the Agency's notable improvements include:

- establishing enumeration centers that focus on assigning and issuing SSN cards
- requiring that field office personnel who process SSN applications used a standardized Web-based process known as SSNAP, which reinforces Agency enumeration policies and standardizes data collection; and
- strengthening the requirements for identity documents presented with SSN applications.

In addition, to prevent misuse of personal information, SSA has reported the following actions:

- SSA removed SSNs from the Social Security Statement, displaying only the last four digits.
- The Department of the Treasury removed the SSN and other types of numeric identifiers from Federal checks.
- SSA no longer releases SSNs or any PII to a caller who cannot provide his or her SSN. SSA now refers such callers to field offices for further identity verification before releasing information.
- When SSA assigns a new SSN because a person has been harmed by the misuse of his or her original SSN, the Agency places a special indicator on the old SSN record to block issuance of replacement SSN cards and SSN printouts.

We in OIG have also spearheaded many efforts to protect and improve SSN integrity. For example, the work of OIG attorneys, auditors, and investigators led to the removal of SSNs from Selective Service mailings and the Thrift Savings Plan Website—two practices by which the

Federal Government was itself putting the SSN at risk. We are also pleased to see that the Department of Defense (DOD) is replacing the SSN with a new DOD identification number on all identification cards, to protect the privacy and personal information of our military personnel and their families.

We applaud these and other efforts, but even now, SSA has no authority to prohibit the legitimate collection and use of SSNs. Nevertheless, our audit and investigative work has taught us that the more SSNs are unnecessarily used, the higher the probability that these numbers can be used to facilitate the commission of crimes throughout society. We believe SSA should support legislation to limit public and private entities' collection and use of SSNs, and to improve the protection of the information when obtained; continue its efforts to safeguard and protect PII; and develop appropriate authentication measures to ensure the highest level of security and identity assurance before offering replacement SSN cards over the Internet.

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, and it is our experience that investigations into SSN misuse will often involve the elements of identity theft. At times, they can also involve Social Security fraud and can lead to the recovery of significant SSA funds.

For example, last year our El Paso, Texas office investigated the case of Mr. Elias Barquero. The investigation revealed Mr. Barquero used another man's SSN beginning in 1990, to assume the man's identity. He obtained a U.S. passport and a Texas identification card, and then applied for disability benefits. From 2001 to 2010, he fraudulently collected nearly \$95,000 for himself, and nearly \$48,000 on behalf of his two children.

Barquero's victim passed away in 2004, but Barquero misused his identity for almost 15 years. Authorities arrested him and charged him with theft of public money and identity theft. He was sentenced in October 2010 to two years in prison, and court-ordered restitution of more than \$142,000 to SSA.

As we pursue investigations similar to the case of Mr. Barquero, 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. In FY 2010, we secured 441 criminal convictions based on our SSN misuse investigations nationwide.

Identity theft investigations have their share of challenges, as this crime takes on many forms; victims can have their name, birth date, and SSN stolen, and thieves can misuse the information in many ways. Also, there are many cases in which a person does not know his or her identity has been stolen. Therefore, if law enforcement learns an SSN has been misused, there exists the challenge of identifying and locating both the perpetrator and the victim.

Because jurisdiction over identity theft cases often overlaps, we have to determine who will investigate and prosecute the case. In fact, we investigate many of these cases jointly with other law enforcement agencies. Here in Texas, we have worked with the Austin County Sheriff's Office, the Harris County Sheriff's Office, the Texas Health and Human Services Commission OIG, the Texas Department of Public Safety, and the San Antonio Police Department. We have also worked with other Federal agencies, including the Department of Homeland Security's

Homeland Security Investigations, the Federal Bureau of Investigation, the Postal Inspection Service, the Secret Service, and the Department of State's Diplomatic Security Service.

The proliferation of Credit Privacy Numbers (CPNs) is a relatively new SSN misuse scheme and a threat to the security of child identity information. CPNs are nine-digit numbers that resemble the SSN or the IRS-provided Individual Tax Identification Number or Employer Identification Number, but CPNs are a means of misusing the SSN and possibly committing identity theft.

Numerous unscrupulous agencies and organizations are providing CPN—also known as Credit Profile Numbers and Credit Protection Numbers—for a fee, as a method of creating a new, separate credit file for individuals with low credit scores, bankruptcy, and slow or late payments on their current credit record. Websites offering CPNs advertise a new credit file with the use of a CPN, at costs ranging from about \$40 to as much as \$3,500. Despite what many of these credit repair Websites imply, consumers should know that CPNs are not legal.

According to the Identity Theft Resource Center, these credit repair companies appear to be targeting dormant SSNs, particularly those belonging to children, for reasons I have mentioned. However, there is no tangible evidence to indicate that children's SSNs are more vulnerable than the rest of the public.

Legislative Efforts

We support the prior bipartisan legislative efforts of this Subcommittee to limit the use, access, and display of the SSN in public and private sectors, and to increase penalties against those who fraudulently misuse the SSN. Most recently, the Subcommittee 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 violence, 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 obtained through false information, 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 assists an individual to 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.

Reviews & Recommendations

Our ongoing and recently completed audit work has highlighted vulnerabilities and suggested some ways in which SSA can persuade public and private organizations to limit the collection, use, and disclosure of SSNs.

Regarding child SSNs, our report, *Kindergarten Through 12th Grade Schools' Collection and Use of SSNs*, released in July 2010, determined that many schools used SSNs as the primary identifier for students or for other purposes, even when another identifier would have sufficed. We believe that while some schools use SSNs as a matter of convenience, administrative convenience should never be more important than safeguarding children's personal information.

We have previously recommended that SSA seek legislation to limit SSN collection by State and local governments, and to limit access to SSNs by prisoners participating in work programs. In fact, our work on prisoners' access to SSNs preceded the President's signing of the *Social Security Number Protection Act of 2010*, which prohibited prison work programs from granting prisoners access to SSNs.

Additionally, although temporary residents may have authorization to work in the United States for the limited time they are here, we question the propriety of assigning an SSN to these individuals, because the SSN may be a key to the temporary resident's ability to overstay his or her visa. We are working on or have completed related reviews on non-immigrant workers, noncitizens with fiancé visas, and exchange visitors.

Another issue to consider is SSA's procedures for issuing SSN verification printouts. Under the *Privacy Act*, individuals are allowed to obtain their SSN information from SSA, and the printout is among the items available. The printout is a limited version of SSA's Numident record, but it still contains the same basic information as the Social Security card. The printout, however, has no security features.

In response to the *Intelligence Reform and Terrorism Prevention Act of 2004*, SSA revised its policies for issuing Social Security replacement cards. Some of SSA's actions included increasing the identity requirements, such as presenting valid photo identification documents for obtaining a replacement SSN card; and limiting the number of replacement Social Security cards an individual can receive to no more than three in a year and 10 in a lifetime.

SSA's current disclosure regulations that implement the *Privacy Act* allow an individual to provide less probative identity documents to obtain an SSN printout. In certain circumstances, an individual can obtain an SSN printout from a field office without any identity documents. In a December 2007 report, *Controls for Issuing Social Security Number Verification Printouts*, we said procedures for issuing the printouts should follow SSA's improved replacement card procedures.

However, SSA did not implement similar procedures in the SSN printout issuance process. We will soon release a report that determined the Agency issued about 7 million printouts in FY 2009, up from about 4.6 million in FY 2003, the first full year SSA issued the printouts. We continue to believe SSA should strengthen its controls for issuing printouts. Since December 2007, we have found an increase in the occurrences of fraud involving printouts. We also measured - every SSA field office's printout output, and we found the 18 field offices located within 30 miles of the United States-Mexico border—including eight offices in Texas—did not generally issue a greater number of printouts than other field offices.

Citizens' Accountability

Identity theft, especially child identity theft, is serious, and while OIG and SSA have controls in place to protect the SSN, we should all be aware of the dangers of being careless with our and

our children's personal information. We urge people to keep their and their children's Social Security cards in a secure place, to shred personal documents, and to 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 or enrolling a child in piano lessons. It is also critically important that we all monitor our financial transactions regularly by checking credit reports from one of 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 believes his or her SSN is being misused should contact the FTC at 1-877-438-4338, and he or she may also need to contact the IRS to address any potential tax issues.

Finally, we urge parents not to give their children their SSNs until the children understand how and why to protect the numbers. 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. Identity 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. The SSN was never intended to do more than track a worker's earnings and to pay that worker benefits. However, as the use of the SSN has expanded over the decades, its value has increased as a tool for criminals, who are now targeting our children's personal information. Therefore, we must continue to ensure the integrity of the enumeration process; limit the collection, use, and public display of the SSN; encourage the protection of the SSN by those who use it legitimately; and provide meaningful sanctions for those who fail to protect the SSN or misuse it.

Our investigators are committed to pursuing SSN misuse and identity theft cases, and our auditors will continue to offer recommendations to safeguard the SSN. We will continue to provide information to your Subcommittee 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.