U.S. House of Representatives

Committee on Ways and Means
Subcommittee on Social Security

Statement for the Record

Enhancing Social Security Number Privacy

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

June 15, 2004

Good Morning, Mr. Chairman, Mr. Matsui, and members of the Subcommittee. Let me first thank you for the invitation to be here today for this important hearing to discuss the pervasive problem of Social Security number (SSN) misuse and the Committee's proposed legislation to protect the privacy of SSNs, the Social Security Number Privacy and Identity Theft Prevention Act of 2003 (H.R. 2971).

The SSN as a National Identifier

I would like to begin my testimony today with a simple declaration: The SSN is a national identifier. In past years, many would challenge that statement. Today, we live in a changed world, and the SSN's role as a national identifier is a recognized fact. Unfortunately, with that knowledge, we must also accept that because the SSN is so heavily relied upon as an identifier, it is a valuable commodity for lawbreakers. Given the importance of this unique, nine-digit number and the tremendous risk associated with its misuse, one of the most important responsibilities my office undertakes each day is oversight of SSN integrity. Today I would like to focus my testimony on how the SSN is misused to commit crimes, my office's role in addressing homeland security and identity theft and what more needs to be done to ensure the integrity of the SSN.

Misuse of the SSN to Commit Crimes

While financial crimes involving SSN misuse are more numerous than terrorism-related crimes, the potential threat to homeland security nevertheless justifies intense concern. An SSN allows an individual to assimilate themselves into U.S. society. SSNs, therefore, become valuable tools for terrorists or others who wish to live in the United States and operate under the ''radar screen.'' Such individuals may obtain SSNs by purchasing them, creating them, stealing them, utilizing the SSN of a deceased individual or obtaining them from SSA directly through the use of falsified documents. Once an individual has an SSN, he has the ability to work, buy a home, and engage in a wide range of financial transactions including the raising and transferring of funds.

I am also concerned about the escalating occurrences of identity theft, which is the fastest-growing form of white-collar crime in the United States. In September 2003, the Federal Trade Commission (FTC) released a survey showing that 27.3 million Americans were victims of

identity theft between 1998 and 2003—including 9.9 million people in the study's final year. FTC also reported that during the study's final year, losses to businesses and financial institutions totaled nearly $48 billion and consumer victims reported $5 billion in out-of-pocket expenses. Clearly, this is an epidemic that must be brought under control.

Identity theft is an ''enabling'' crime, one that facilitates other types of crime, ranging from passing bad checks and defrauding credit card companies to committing acts of terrorism. Additionally, criminals use identity theft to defraud Federal agencies and programs of millions of dollars.

For example, based on an investigation conducted by our Atlanta Field Division, a St. Petersburg, Florida resident was recently sentenced to 27 months of incarceration and ordered to make restitution to SSA for over $79,000 in survivors benefits she received for herself and three nonexistent children. To perpetrate this scheme, the individual assumed the identity of a former acquaintance by obtaining a North Carolina identification card in her friend's name. With this new identity, she used fraudulent birth certificates to apply for SSNs on behalf of two fictitious children. She also altered court marriage and divorce documents, falsely claiming that a known deceased man was her ex-husband and the fictitious children's father. She perpetrated this elaborate scheme so that she could apply for and receive Social Security survivors benefits for the fictitious children—and, until caught, was successful in doing so. Further investigation revealed that she had previously committed a similar crime resulting in additional survivors benefits for herself and another fictitious child.

Other Federal agencies such as the Department of Housing and Urban Development (HUD) have also experienced a significant increase in the number of identity theft occurrences in their programs. Within programs administered by HUD, identity thieves are using someone else's SSN to obtain and then default on home mortgages—leaving taxpayers to pay their bills.

For those with an illicit motive, an SSN can be obtained in many ways:

- Presenting false documentation to SSA.
- Stealing another person's SSN.
- Purchasing an SSN on the black market.
- Using the SSN of a deceased individual.
- Creating a nine-digit number out of thin air.

Although SSA may never be able to completely prevent individuals from purchasing an SSN on the black market or stealing the SSN of another, we are proud that our efforts are making it more difficult to do so.

Our Role in Addressing Homeland Security and Identity Theft

Recognizing the importance of SSNs to terrorists and identity thieves, SSA and the OIG take very seriously our responsibility to ensure that these numbers are only issued to those with a legal reason for having one. As such, we continuously seek innovative ways to prevent SSN

misuse and create collaborative partnerships with other Federal, State, and local entities to address both homeland security and identity theft concerns.

OIG Homeland Security Activities:

Our active involvement in addressing homeland security began on September 11, 2001, with our agents assisting in rescue efforts and site security at the World Trade Center. We immediately assigned supervisors and agents to the FBI Command Centers in New York City and New Jersey to process information and investigate leads. The Inspector General ordered all Field Divisions to assist in Joint Terrorism Task Forces (JTTF) and Anti-Terrorism Task Forces (ATTF) around the country—in fact, we are now active participants in 63 Joint Terrorism Task Forces and 29 Anti-Terrorism Task Forces, as well as the Foreign Terrorist Tracking Task Force.

While participating in these task forces, our agents have assisted in better securing many of our Nation's airports and nuclear facilities by ensuring that employees and individuals having access to secure areas within these locations are working under their true names and SSNs. Further, as part of its anti-terrorism activities in the Buffalo area, our New York Field Division investigated six men from neighboring Lackawanna suspected of terrorist-related activities. Our investigators determined the identities of the ''Lackawanna Six'' and their attendance and participation in an al Qaeda terrorist training camp in Afghanistan. One suspect had two Social Security cards in his possession at the time of his arrest. All six suspects pleaded guilty to providing material support or resources to designated foreign terrorist organizations and received sentences of 7 to 10 years in prison.

In carrying out our homeland security responsibility, we coordinate closely with other Federal agencies. For example, we recently met with representatives of the Department of Homeland Security (DHS) to discuss methods in which we could work together to address the SSN's role in homeland security. We welcome this opportunity and believe cooperative ventures such as these are imperative to ensure that all of the links in the homeland security chain stay connected. Based on our initial discussions, we plan to work with DHS to explore possible data matching and cross-verification opportunities—those that are currently provided for under law and those for which additional legislation may be required.

OIG Identity Theft Activities:

By law and by mission, our office has a narrow but important role in the overall effort to address identity theft. Much of the Federal government's response to identity theft issues rightly belongs to the FTC. State and local law enforcement agencies and financial institutions also have critical roles to play.

Because our primary mission is to protect the integrity of SSA's programs and operations, in the majority of our identity theft investigations, we continue to focus investigative efforts on cases that affect SSN integrity. For example, our Chicago Field Division took part in a 3-day inter-agency undercover operation that resulted in the arrest of 12 suspects dealing in fraudulently obtained Social Security cards, State driver's licenses, and U.S. passports. Our investigators determined that the group's leader and 11 others took part in an elaborate document-

counterfeiting scheme to obtain valid SSNs for non-existent children. The names belonged to undocumented noncitizens who paid up to $5,000 each for valid documents. Members of the group were sentenced to up to 2 years in prison or given immunity from prosecution for their cooperation in the undercover sting.

To maximize our investigative resources, we dedicate agents that work on task forces with other law enforcement agencies nationwide to investigate identity crimes. We also work closely with prosecutors to bundle SSN misuse cases that, when presented separately, may not have been accepted for prosecution.

We are also continuing our efforts to identify opportunities for SSA to further strengthen the integrity of the SSN. One of my major concerns has been the use of fraudulent documents to obtain SSNs. In an August 2002 audit, we estimated that during FY 2000, SSA assigned at least 63,000 SSNs to noncitizens based on invalid immigration documents that SSA processes did not detect. Based on our recommendation, SSA improved its controls in this area and now verifies all immigration documents presented by noncitizens with the issuing agency before assigning an SSN. We believe SSA's decision to adopt our recommendation was laudable and significantly reduced the circumstances under which an unauthorized noncitizen may obtain a legitimate SSN from the Agency. We are currently examining the Agency's compliance with this and other enumeration controls. Additionally, we continue to explore and recommend further controls the Agency can implement to strengthen SSA's important responsibility of assigning SSNs.

SSN Integrity Protection Team:

Protecting the integrity of the SSN has become a major part of the work we do. The President's Fiscal Year 2004 Budget enabled us to begin staffing our SSN Integrity Protection Team to combat SSN misuse and identity theft. The Team is an integrated model that combines the talents of auditors, investigators and attorneys in a comprehensive approach, allowing SSA and OIG to:

- Support Homeland Security.
- Identify patterns and trends of SSN misuse.
- Locate systemic weaknesses that contribute to SSN misuse such as in the enumeration and earnings related processes.
- Recommend legislative or other corrective actions to enhance the SSN's integrity.
- Pursue criminal and civil enforcement provisions for individuals misusing SSNs.

Our SSN Integrity Protection Team will enable us to better target audit and investigative work. The Team will participate with other Federal, State and local entities to collaborate on potential SSN misuse activities. It is critical that we continue to receive funding in future budgets for this important initiative.

SSA Initiatives to Address SSN Integrity:

SSA has made significant progress in strengthening the defenses of the SSN, implementing important suggestions our office has made, and working with us to find solutions. In November 2001, the Commissioner of Social Security established an Enumeration Response Team (ERT) comprised of executives across the Agency, including representatives from the OIG. The

Commissioner charged this group with identifying steps the Agency could take to improve the enumeration process and to enhance the integrity of the SSN. Since that time, the Commissioner and the ERT have implemented numerous policies and procedures designed to better ensure that only individuals authorized to do so, receive an SSN. For example, the ERT recommended, and SSA adopted, more stringent circumstances under which an individual may obtain a nonwork SSN. We are proud to serve on workgroups such as these and applaud the Commissioner and SSA for its strong commitment to improving SSN integrity.

Prior to the ERT, the Agency implemented other initiatives such as the Comprehensive Integrity Review Process (CIRP) and Enumeration at Entry process. The CIRP system identifies vulnerabilities in the enumeration process and issues alerts to SSA's field offices (FO) to develop and certify. The FO reviewer, usually a manager or supervisor, performs an enumeration integrity review of each alert. If the reviewer determines that there is a possibility of fraud, the alert is forwarded to the OIG for development and disposition.

The Enumeration at Entry initiative is a collaboration with the Department of Homeland Security (DHS) and the Department of State (DOS) to not only facilitate issuance of SSNs to legally admitted aliens whose immigration status permits such issuance, but it ensures through DHS and DOS certifications that the identity and immigration status of the alien is what is purported.

What Actions Still Need to Be Taken to Address SSN Misuse

Despite the significant progress SSA and Congress have made in recent years to address SSN misuse, we believe SSN integrity and protection still need improvement at three stages: at issuance, during the life of the number-holder, and following the number-holder's death.

At Stage One (issuance of the SSN), my office is doing more work than ever, working closely with this Subcommittee and SSA to strengthen controls over the enumeration process, ensure the integrity of identification documents, and make it as difficult as possible to fraudulently obtain an SSN from the Federal government. Together with you and with SSA, we have made important strides in reducing enumeration vulnerabilities, and that effort continues. Still, to strengthen our defenses even further, we believe SSA should implement the following changes.

- Establish a reasonable threshold for the number of replacement SSN cards an individual may obtain during a year and over a lifetime.
- Continue to address identified weaknesses within the enumeration process to better safeguard SSNs.
- Verify the validity of birth records with the issuing State before issuing an SSN to U.S. citizens under age 1.
- Work with State Bureaus of Vital Statistics to incorporate additional controls in SSA's Enumeration-at-Birth program, such as periodically reconciling the number of SSNs assigned through the program to the number of births reported by participating hospitals.

It is at Stages Two (during the life of the number holder) and Three (after the number holder's death) where we have focused the majority of our efforts, and where we have made the most progress. In the last several years, we have conducted numerous audits and made extensive

recommendations to SSA to improve the SSN misuse problem in the earnings reporting process, and most importantly, to improve controls over SSN misuse as it pertains specifically to Homeland Security. Nevertheless, to more completely address SSN integrity during the life of the number holder and following that number holder's death, we believe SSA and lawmakers should examine the feasibility of the following initiatives.

- Limiting the SSN's public availability to the greatest extent practicable, without unduly limiting commerce.
- Prohibiting the sale of SSNs, prohibiting their display on public records, and limiting their use to legitimate transactions.
- Enacting strong enforcement mechanisms and stiffer penalties to further discourage SSN misuse.
- Cross-verifying all legitimate databases that use the SSN as a key data element.
- Review the implications of releasing information on deceased individuals.

Limiting the SSN's Public Availability and Sale of the SSN

Perhaps the most important step we can take in preventing SSN misuse is to limit the SSN's easy availability. We believe legislation designed to protect the SSN must strictly limit the number's availability on public documents. As long as criminals can walk into the records room of a courthouse or local government building and walk out with names and SSNs culled from public records, it will be extremely difficult to reverse the trend. We believe effective legislation should also specifically prohibit the sale of SSNs—including one's own SSN—on the open market. As long as criminals can buy a list of names and SSNs through an Internet auction, we will continue to be plagued by the consequences.

To be fully effective, we also believe legislation must limit the use of the SSN to appropriate and valid transactions. The financial industry relies on the SSN, and no one is suggesting that we change the way legitimate business is conducted in the United States. But the use of the SSN as a student or patient identification number, as part of a car rental contract or to rent a video, must be curtailed.

Congress enacted the Identity Theft and Assumption Deterrence Act in 1998, responding to the growing epidemic of identity thefts by imposing criminal sanctions for those who create a false identity or misappropriate someone else's. The Internet False Identification Prevention Act, adopted in 2000, closed a loophole left by the earlier legislation, enabling our office and other law enforcement organizations to pursue vendors who previously could sell counterfeit Social Security cards legally by maintaining the fiction that such cards were ''novelties'' rather than counterfeit documents. More legislative tools are needed, and we have worked with Congress to identify legislation necessary to protect the integrity of the SSN. For example, the House is now considering H.R. 2971, the Social Security Number Privacy and Identity Theft Prevention Act of 2003, which would seriously restrict the use of SSNs in the private and public sector, and criminalize the sale of SSNs.

Penalties

The Identity Theft legislation I discussed earlier provides criminal penalties, but those penalties were designed for broader crimes involving Social Security cards and/or SSNs, not for SSN misuse itself. We believe legislation should not only provide criminal penalties in the Social Security Act, but also enhance penalties for those few SSA employees who betray the public trust and assist criminals in obtaining SSNs.

For example, a former SSA Service Representative was sentenced to 3 years probation and community service after pleading guilty to a bribery charge in connection with issuing 100 to 200 Social Security cards to illegal aliens. She received between $50 and $150 for each card. We believe it is critically important to send a strong message to SSA employees tempted to facilitate crimes against Agency programs by pursuing the maximum sentence possible.

The House Committee on the Judiciary recently approved H.R. 1731, the Identity Theft Penalty Enhancement Act, which established enhanced penalties for aggravated identity theft. While increased criminal penalties are a welcomed addition to the arsenal available for use in combating identity theft, we also believe legislation should provide an administrative safety net in the form of Civil Monetary Penalties to allow for some form of relief when criminal prosecution is not available for SSN misuse and other Social Security-related crimes.

Cross-verification

Additionally, we strongly support cross-verification of SSNs through both governmental and private sector systems of records to identify and address inaccuracies. Our experience has shown that cross-verification can combat and limit the spread of false identification and SSN misuse. Further, we believe all law enforcement agencies should be provided the same SSN cross-verification capabilities currently granted to employers. In doing so, the law enforcement community would use data already available to the Federal, State and local governments and the financial sector.

Potentially, the rewards of cross-verification can be great, yet it would not require major expenditures of money or the creation of new offices or agencies. We believe legislation is needed to require mandatory cross-verification of identification data between governmental, financial and commercial holders of records and the SSA on a recurring basis. To offset SSA's cost for providing such services, the Agency could charge a modest fee to commercial and financial entities. The technology to accomplish these data matches and verifications exists now. Coupled with steps already underway by SSA to strengthen the integrity of its enumeration business process, cross-verification, once initiated, would be a critical step in combating the spread of identity fraud.

Let me give you an example of an identity theft case in which cross-verification may have prevented a crime against a Federal government program, saving taxpayers $62,000. A Salt Lake City grandmother learned last year from one of my Denver Field Division agents that her SSN was used to purchase a $146,000 HUD home. This identity theft went undiscovered until the home went into foreclosure because the criminals used this grandmother's SSN, but another name to purchase the home. Had HUD been allowed to verify the accuracy of the borrower's name and SSN with SSA, HUD would have recognized the discrepancy and denied the loan. In

this one case alone, the Government would have saved the thousands of program dollars HUD had to pay to foreclose and resell the property. Additionally, this elderly Salt Lake City grandmother would have been spared the time and expense of repairing her credit record.

We believe cross-verification is one of the most important tools the Government and private sector can employ to reduce the instances of identity theft. We understand the important issue of consumer privacy that must be considered by Congress and others before allowing such data integrity matches. However, our ability to prevent these egregious crimes would be enhanced by additional legislation balancing the need for consumer privacy with the need for accurate identifying information.

Conclusion

We always appreciate the invitation to speak with this committee and the very important work you do to help ensure the integrity of SSA programs and the SSN. We are very pleased with the progress Congress and SSA have made in addressing the issue of SSN integrity over the last several years. However, we reiterate our concern that more must be done to ensure that only those individuals authorized to have an SSN receive one and that anyone who fraudulently obtains and misuses an SSN is adequately penalized. As such, we support legislation such as H.R. 2971, the Social Security Number Privacy and Identity Theft Prevention Act of 2003, which severely limits the sale, purchase and display of SSNs to the general public. We also believe legislation such as H.R. 1731, the Identity Theft Penalty Enhancement Act, is a significant step toward holding accountable individuals who misuse SSNs to commit egregious crimes. We encourage this Committee and others in Congress to stay firm in your resolve to enact these two bills. We also ask that Congress consider other measures such as increased cross□verification among Government and private sector entities, Civil Monetary Penalties for SSN misuse and other Social Security-related crimes when criminal prosecution is not available, and stronger penalties for those few SSA employees that betray the public trust by selling SSNs. We will certainly continue our vigilance in addressing these issues and stand ready to do more to enhance the safety and well-being of all Americans. I would now be happy to answer any questions you may have.