U.S. Senate
Committee on Finance

Statement for the Record

The Homeland Security and Terrorism Threat from Document Fraud, Identity Theft and Social Security Number Misuse

Patrick P. O'Carroll
Assistant Inspector General for Investigations
Social Security Administration

September 9, 2003

Good afternoon, Chairman Grassley, Ranking Member Baucus. Let me first thank you for the invitation to be here today for this important hearing on the homeland security and terrorism threat from identity theft, document fraud, and Social Security number (SSN) misuse.

The SSN as a National Identifier

Let me begin with a simple declaration: The SSN has become a national identifier. Two years ago, many people challenged that statement. Today, we live in a changed world, and the SSN's role as a national identifier is a recognized fact. The issuance of SSNs and driver's licenses based on invalid documentation creates a homeland security risk, and any failure to protect the integrity of the SSN can have enormous consequences.

Identity theft is the fastest-growing form of white-collar crime in the United States. Many expect that incidents of identity theft will more than triple from .5 million in 2000, to 1.7 million in 2005. While identity theft existed prior to the advent of the Internet, there is no question that in recent years, criminals have taken advantage of all of the readily available confidential information on the Internet. Some studies indicate that 10 percent of identity theft currently originates through the Internet. It is projected that by 2005 that number will rise to 25 percent. The proliferation of Internet-based information brokers also represents another resource for identity thieves. Most of these are third-party service providers, whose services help financial institutions track down deadbeat borrowers or conduct credit checks, are legitimate.

In most cases, identity theft begins with the misuse of the SSN. No aspect of the Social Security Administration's (SSA) Office of the Inspector General's (OIG) mission of protecting Social Security programs from fraud, waste, and abuse is more important than our oversight of the SSN. The SSN is so heavily relied upon as an identifier that it is a valuable commodity for lawbreakers. It 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.

Identity fraud is a growing public concern, national in scope, and dangerous to both our economic health and our homeland security. Counterfeit identity documents such as those displayed in this hearing room remain a key component of identity theft. Identity theft is an "enabling" crime, one that facilitates other forms of crime. Those crimes may range from passing bad checks and defrauding credit card companies to acts of terrorism. In one case, a man stole the identities of 17 victims, and used them for credit card fraud, to purchase vehicles, horses, and other valuable items. One of the victims was the only U.S. Marine fighter ace to serve in both World War II and Korea, and another was a Hollywood actor. The identity thief was sentenced to 7 years in federal prison and ordered to repay $200,000 to SSA and $33,000 to the victims, though the total loss was $379,000.

Misused SSNs, stolen or misappropriated birth certificates, and false or fraudulently-obtained driver's licenses are the keys to identity fraud in the United States. With any one of these three documents, you can generally obtain the other two. We investigate thousands of SSN fraud and identity theft cases every year, and we often find the criminals have not only stolen or forged SSN information, but stolen or forged driver's licenses as well. We maintain a strong working relationship with the American Association of Motor Vehicle Administrators (AAMVA), and we have supported the development, deployment, and monitoring of the commercial driver's license and motor carrier safety programs throughout the United States.

Our Role in Homeland Security

While financial crimes involving SSNs are more numerous than terrorism-related crimes involving misuse of the SSN, the potential threat to homeland security nevertheless justifies intense concern.

Those connected with terrorism will at some point try to obtain SSNs. They may buy them, they may create them, or they may try to obtain them from SSA directly through the use of falsified documents. They need those numbers, and we must ensure that those numbers do not come from government agencies.

Our active involvement in 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—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 and the Pakistani Task Force. We have participated in ATTF-sponsored homeland security projects focused on the Nation's critical infrastructure sites. Since 9/11 we have been involved in 132 such projects nationwide, to include 63 airports and 24 nuclear facilities, resulting in over 1,200 arrests.

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

Since 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 will affect SSN integrity. We continuously seek innovative ways to prevent SSN misuse and create collaborative partnerships with other Federal, State, and local entities. To maximize our investigative resources, we have dedicated agents to work in task forces with other law enforcement agencies to investigate identity crimes. We are working closely with prosecutors to bundle SSN misuse cases that, when presented separately, may not have been accepted for prosecution. The additional benefit of law enforcement agencies pooling their investigative resources is our ability to investigate more program and SSN misuse cases.

SSA issued approximately 18 million original and replacement Social Security cards in fiscal year (FY) 2002. We have found that SSNs have been issued to individuals using fraudulent documents. For example, an August 2002 audit estimated that during FY 2000, SSA assigned at least 63,000 SSNs to non-citizens based on invalid immigration documents that SSA processes did not detect. While SSA has improved its procedures in this area, we have no way of determining how many SSNs have been improperly assigned to non-citizens.

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 May 2002, we issued a Management Advisory Report entitled Social Security Number Integrity: An Important Link in Homeland Security. That report stated that it is critical that SSA independently verify the authenticity of documents presented by SSN applicants. We also noted that SSA had established a task force to address some of these concerns, including improved verification procedures. For example, in September 2002 SSA started independently verifying all non-citizen immigration documents prior to issuing an SSN. We are currently assessing the Agency's compliance with these new procedures.

Protecting the integrity of the SSN has become a major part of the work we do. The FY 2004 President's Budget will allow 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 ensure 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 receive full funding in the President's Budget for FY 2004 in order to accomplish this important initiative.

Legislation is critically needed to strengthen SSN integrity

Legislation to strengthen SSN integrity is critically needed in three distinct areas our audit and investigative work identifies. The first area is limiting the use and display of the SSNs in the public and private sectors. Second, the present arsenal of criminal, civil, and administrative penalties need to be

strengthened to deter and/or punish identity thieves. The third approach is requiring the cross-verification of SSNs, which I will discuss further in a moment, to combat the spread of false of identification and limit SSN misuse.

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.

The House is now considering H.R. 2971, which would seriously restrict the use of SSNs in the private and public sector, and criminalize the sale of SSNs. We have asked for an administrative safety net in the form of Civil Monetary Penalty authority for those instances of SSN misuse that could not be criminally prosecuted. We have also sought more meaningful criminal penalties in the Social Security Act for those few SSA employees who betray the public trust and assist criminals in obtaining SSNs. We are following the progress of H.R. 2971, and we would be glad to work with Senate Committee on Finance on such legislation.

We would like to explore the cross-verification of SSNs through both governmental and private sector systems of records to identify and address inaccuracies in SSA's files, and in data bases at various levels of government and the financial sector. Cross-verification can combat and limit the spread of false of identification and SSN misuse. All law enforcement agencies should be provided the same SSN cross-verification capabilities currently granted to employers. It would use data already available to the Federal, State and local governments and the financial sector.

The rewards of cross-verification can be impressive, yet it would not require major expenditures of money or the creation of new offices or agencies. Congress could pass legislation requiring mandatory cross-verification of identification data between governmental, financial and commercial holders of records and the SSA on a recurring basis. Commercial and financial

entities could be charged a modest fee-for-service to offset SSA's costs for providing this service. 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.

We continue to work with Joint Terrorism Task Forces and Anti-Terrorism Task Forces participating in homeland security projects. We remain in constant contact with this and other committees of both houses of Congress to provide expertise and assistance in the analysis of data and creation of legislation aimed at protecting the SSN and preventing it from being used improperly. We have attorneys working either as Federal prosecutors or with them to enforce the Social Security Act's felony provisions. We continue our audit work, reviewing SSA's enumeration process and making recommendations for much-needed improvements. We are preparing to institute our SSN Integrity Protection Team to intensify and focus our efforts to combat SSN misuse and identity theft.

And we stand ready to do more. We appreciate your interest in these issues, and look forward to working with you to enhance the safety and well-being of all Americans.