U.S. House of Representatives

Committee on Ways and Means
Subcommittee on Social Security

Statement for the Record

Fourth in a Series of Subcommittee Hearings on Social Security Number High-Risk Issues

The Honorable Patrick P. O'Carroll, Jr.

Inspector General, Social Security Administration

March 16, 2006

Good morning, Chairman McCrery, Congressman Levin, and Members of the Subcommittee. This is our fourth hearing in this series on high-risk Social Security number (SSN) issues, and I applaud your efforts and dedication in giving these issues the attention they deserve. The SSN is a key to American life in many ways, and as we have seen throughout this series of hearings, its misuse has repercussions that cause a ripple effect across the American landscape.

Much of my testimony in the first three hearings has centered on largely administrative issues. At the first hearing, we discussed enumeration, the process by which the Social Security Administration (SSA) issues SSNs; at the second hearing, we discussed SSN misuse in the context of misreported wages, particularly by foreign-born workers without authorization to work in the United States; and, at the third hearing earlier this month, we discussed enumeration of foreign-born individuals and the payment of benefits to those born or residing abroad.

Today, I would like to discuss our investigative efforts to combat SSN misuse in all forms. Our Office of Investigations (OI) is dedicated to preventing and detecting fraud against SSA's programs and operations, and SSN misuse is an important facet of that overall investigative effort. Obviously, with finite resources, and with many areas of responsibility, including program fraud, employee fraud, contract fraud, and others, we are mindful that our primary responsibility is to protect the Trust Funds that provide benefits to millions of Americans every month. At the same time, our responsibility to protect the integrity of the SSN cannot be overstated. We strive continuously to strike an appropriate balance.

To give you some sense of how we strike that balance, consider that in Fiscal Year (FY) 2005, the Office of the Inspector General (OIG) received about 85,000 allegations of fraud, 84 percent of which involved fraud against a Social Security program, such as disability insurance benefits. Approximately 13 percent-almost 11,000 allegations-involved SSN misuse. It is important to understand that these SSN misuse allegations are limited to incidents of SSN misuse involving a Social Security program or otherwise directly related to the administration of the Social Security Act.. Allegations of pure identity theft, financial fraud, and other non-SSA-related crimes are referred to appropriate sources, and are not included in this total.

Looking at actual investigations conducted during FY 2005, OI opened approximately 9,500 cases, of which 79 percent involved crimes against Social Security programs, while just over 16 percent involved SSN misuse. Thus, while we actually investigate a higher proportion of

allegations in the SSN misuse category than in the program fraud category, we still invest more than four times more resources in program fraud than in SSN misuse. The results of an audit we will issue shortly, in which we provide an estimate of the rate of overpayments in Social Security's disability programs, underscores the importance of our emphasis on program fraud. Our statutory mission is to protect SSA programs and operations, and to the extent that an allegation of SSN misuse does not touch on those programs, our resources do not generally allow us to pursue it.

We do, however, play a role in the overall government effort to protect against SSN misuse in a multijurisdictional context. Our affirmative and aggressive approach to SSN misuse of this type is designed to maximize our resources through the effective use of task forces, workgroups, and other cooperative efforts.

At this time, our investigators across the country are members of almost 200 task forces and workgroups in all ten of our field divisions. These groups, comprised of Federal, State, and local law enforcement agencies, pool resources and, when permitted, share information to accomplish more than each member could ever accomplish on its own. The groups range from Joint Terrorism Task Forces run by United States Attorneys, to white collar crime groups, to financial fraud workgroups.

The work done by these groups is astounding. For example, our agents on the Central Florida Identity Theft task force, a group comprised of ten law enforcement agencies, concluded a case last year in which they apprehended fifteen members of an identity fraud ring who would obtain lists of individuals with good credit histories, and use the personal information of those individuals to defraud a variety of commercial entities in the Orlando area. Twelve of the fifteen individuals arrested were sentenced to prison terms, and the total restitution ordered to victims exceeded $2 million.

In another case, our New York Field Division, working on a task force with other agencies including the U.S. Secret Service, investigated the hijacking of a deceased Social Security beneficiary's bank account. The complex investigation revealed that the subjects not only continued to receive the deceased woman's benefits-totaling some $80,000-but also used her bank account to launder counterfeit checks created with the help of a corrupt bank employee. They then went on to steal other SSNs and identities and open additional accounts, which they would use both to create additional fraudulent checks and to launder them. In all, they cashed about $300,000 in bad checks and opened credit card accounts from which they stole another $100,000.

Since cases like this represent an opportunity to achieve a significant return with only minimal investment of resources-our agent in this ten-agency task force still maintains a "normal" caseload-we can afford to contribute substantially to the overall effort to stop SSNs being used as instruments of a crime. If each of the 200 task forces in which we participate makes only a few cases like this each year, we are able to have a far greater effect than we could ever have working alone.

However, our day-to-day program-related SSN misuse caseload is no less daunting, and our solo work is equally impressive. We see allegations of SSN misuse in its myriad forms come in every

day by phone, fax, e-mail, and in electronic referrals from SSA employees. One such referral from an SSA District Office concerned a woman who was confronted by SSA with the fact that she appeared to be receiving disability benefits under two separate SSNs. Each set of benefits was going to the same name, the same address, and for the same disability, but under two different SSNs. The woman informed SSA, and subsequently our investigators, that she had a twin sister. Despite the fact that both sets of benefits were going to the same address, the woman alleged that she and her identical twin were estranged and did not speak.

Our investigators obtained a copy of the woman's birth certificate from the state vital records office. It showed that hers had been a single birth, not a twin birth. Additional investigation uncovered no other evidence that a twin had ever existed. Our investigators asked the woman to provide a copy of her birth certificate, and she eventually provided the same document we had obtained from the state without her knowledge. It had the same control number and the same signatures, but the altered copy she provided showed a twin birth. We recontacted the vital statistics office and confirmed that no official change had been made since we'd obtained our copy. The woman, unaware that we had her original birth certificate, continued to demand that her duplicate benefits be reinstated, even going so far as to write to her Congressman to demand that he intercede on her behalf. We showed the Congressman the two versions of the birth certificate, and that ended the woman's ill-conceived mission.

In another case, our investigation revealed that a woman had been working full-time since 1978 under one SSN and receiving Title XVI disability payments since 1973 under a second SSN. From 1978 until 2001, she worked full-time for various healthcare agencies while certifying each year to SSA that she was not working. In 2001, the woman applied for Title II disability benefits under the first SSN, based on her extensive work history. A Title XVI claims representative recognized the woman during her appointment to apply for Title II benefits, and referred the case to OIG. She later admitted to OIG agents that she had been working for 23 years while receiving Title XVI payments. She eventually pled guilty to theft of government funds and making false statements, and was sentenced in May 2005 to 6 months' incarceration in federal prison, 6 months' home detention with an electronic monitoring device, and 5 years' probation, and was ordered to pay full restitution of $166,767.

While SSN misuse cases like these are made by our investigators every day, we encounter cases involving counterfeit Social Security cards much less frequently. The practical reality is that most of us were issued our Social Security cards not long after we were born, and we long ago committed our SSNs to memory. But the cards themselves were probably placed in a drawer or box many years ago, and have rarely been seen or used since. Almost every entity imaginable, from government, to medical facilities and insurance carriers, to creditors, to employers and beyond may and often do ask for SSNs; but rarely, if ever, do they ask to see the card itself.

Our work reviewing SSA's automated employee verification services, such as the Social Security Number Verification Service (SSNVS), further underscores this reality. Employers seeking to confirm the SSN of a current or prospective employee need only take advantage of this service to go online and match the employee's name, SSN, date of birth, and gender against SSA's records-all without ever laying eyes on an actual Social Security card. Of course, for verification services such as SSNVS to be truly effective, we must be confident that the information in SSA's databases is as accurate as possible, and our prior audit work has revealed

that this may not always be the case. Nevertheless, SSNVS and other verification services even further minimize the need to carry or present the card. Indeed, today, the card is little more than a "hard copy" of a number that is already contained in various databases throughout society and government. This is consistent with the purpose for which the card was created 70 years ago, and while there should always be security enhancements made to stay one step ahead of tech-savvy counterfeiters, it would be hard to justify the expense involved in replacing all Social Security cards with "hard" cards as long as their utility remains as limited as it is.

From time to time, there is talk of expanding the card's use beyond its current functions, and obviously, this issue is one for Congress to debate. If a decision is made to transform the Social Security card into something more than it is, significant improvements may then have to made in the document. Moreover, it could create a significant new workload for SSA-one that might fall outside of the Agency's current and historical function, or even further heighten the tension between service and integrity.

Whatever Congress may determine is an appropriate role for the Social Security card to play, our office is happy to provide whatever audit and investigative work might prove helpful. In the interim, we will continue our tireless efforts to prevent and detect misuse of the Social Security number as well as the Social Security card itself.