

**Committee on the Judiciary**

**Subcommittee on Technology, Terrorism, and  
Government Information**

**United States Senate**



**Identity Theft  
James G. Huse, Jr.**

**Inspector General of Social Security**

**March 7, 2000**

It is an honor to provide this Subcommittee with the Social Security Administration's Office of the Inspector General's (SSA-OIG) status of ongoing work and our perspective on the direction we need to take to reduce the incidents of identity theft. Thanks to the leadership of Senator Kyl and the efforts of this Subcommittee, the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act) was passed in October 1998. That Act provided this office with a powerful weapon to combat Social Security number (SSN) misuse when used to commit identity theft. While the SSN was never intended to be a "national identifier," this Act acknowledges that the SSN is a commonly used means of identification. Even before the passage of the Identity Theft Act, this office had gained insight into the widespread occurrence of identity theft, because of the vast number of complaints received by the SSA-OIG Fraud Hotline. Because of this, we developed an action plan to focus on SSN misuse. The American public has an expectation that the Government will establish safeguards to protect their SSNs from misuse. They also expect governmental action when misuse occurs. This office will do its best to meet the public's expectation.

From the beginning, our office has taken a proactive stance to work with other Federal organizations to reduce the incidents and impact of identity theft crimes by participating in national and international work groups. We worked closely with the Federal Trade Commission (FTC) to develop informational materials that provide a consistent message throughout the Federal Government to assist and educate victims of identity theft. We have met with several U.S. Attorney's Offices to discuss the prosecutorial guidelines for identity theft and because this issue is so important, I have detailed an attorney from my office to the Department of Justice to assist in the prosecution of identity theft cases.

Our office continues to share knowledge and data with the FTC. The FTC and our Office of Investigations are developing a referral system that will allow for the automated transfer of data between the agencies. This referral system will not only improve our ability to assist victims but allow us to detect individuals committing identity theft more quickly. Based on a recent analysis by FTC, we estimate that referrals of SSN misuse could reach 8,000 a month in addition to the 2,500 we already receive. Because of this expectation, we are redesigning our systems to capture SSN misuse referrals in a more defined structure that will delineate SSN misuse by type.

Our Office of Investigations is using existing programs to further develop the referral process with the FTC. The fugitive felon program—designed to implement sections of the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (commonly known as the Welfare Reform Act)—identifies individuals illegally receiving Supplemental Security Income (SSI) payments through computer matching agreements with State and local law enforcement entities. Oftentimes, these data matches identify individuals whose SSN has been assumed by a fugitive. We refer this information to the FTC and our investigative units follow up on leads of those individuals who assumed the victim's SSN.

In Fiscal Year 1999, our Office of Investigations launched SSN misuse pilot projects in five cities across the Nation. Our special agents provide the lead in working with Federal and State law enforcement agencies to review Hotline allegations and open an investigation, if warranted. Partnering with other law enforcement agencies allows us to have a greater impact with limited resources. Because of this partnership, we are able to present cases for prosecution, which if

presented separately, would not be accepted. In the past year through these task forces, we opened 79 investigations, which so far, have resulted in the conviction of 18 individuals. U.S. Attorney's Offices and Federal and State law enforcement agencies have enthusiastically welcomed these pilots and have applauded my office for taking the investigative lead. In one city, Federal and State law enforcement agencies that were not part of the task force have asked to join because of its success.

I would like to provide the Subcommittee with a synopsis of three different investigations related to SSA programs and identity theft that were successfully prosecuted.

In the first case, our Office of Investigations was instrumental in the conviction of what is believed to be the first Federal prosecution under the Identity Theft Act. Our Milwaukee Sub-office opened an investigation, based on a referral from the Wisconsin Capitol Police, of Waverly Burns who was receiving SSI payments. During the course of the investigation, we discovered that Mr. Burns acquired the SSN of another individual and then used this number to secure employment as a cleaning crew supervisor. While working in this capacity, he gained access to the offices of the Wisconsin Supreme Court and stole over \$80,000 in computer equipment. Meanwhile, he lied to SSA officials, in a statement for determining continuing eligibility for SSI, claiming that he was unemployed and continued to receive full SSI payments. Mr. Burns used the stolen SSN to secure a State of Wisconsin identity card, to open bank accounts and file fraudulent tax forms under the victim's name and SSN.

On April 21, 1999, Waverly Burns was indicted for identity theft, SSN misuse, and making false statements to SSA and the Internal Revenue Service. On May 5, 1999, OIG Special Agents arrested Mr. Burns after tracking him to Chicago. Mr. Burns pled guilty to using the identity of another person to obtain employment, then using that employment to commit burglary. Mr. Burns was sentenced to 21 months in prison and ordered to pay over \$62,000 in restitution directly to the Wisconsin Supreme Court.

In the second case, our SSA/OIG special agents as part of the Delaware Financial Crimes task force, investigated Zaid Gbolahan Jinadu as he schemed to defraud several federally insured financial institutions. He solicited the assistance of bank employees to provide SSNs and other identifying data to open fraudulent credit card and bank accounts. These compromised employees also helped him to take over current accounts, make fraudulent wire transfers, receive cash advances and negotiate numerous checks. Mr. Jinadu was indicted by a Federal Grand Jury in the District of Delaware on October 26, 1999, on four counts—one count each of bank fraud; identity theft; fraud in connection with access devices; and misuse of SSNs. On December 20, 1999, Mr. Jinadu and his co-defendants entered a guilty plea to one count of bank fraud and one count of identity theft. He is responsible for fraud losses of approximately \$281,122. Total known losses to financial institutes by Mr. Jinadu and his cohorts during the past 4 years exceeds \$4 million.

In our last case and perhaps one of the most egregious of identity theft crimes was one perpetrated against an elderly individual. Our Richmond Sub-office opened an investigation on Charles Fleming, a SSA disability beneficiary, who stole the identity of a 67-year old individual recovering from a stroke. He took personal documents from the victim's home and used them to

obtain a State driver's license and SSN under the victim's name. Using these documents, he opened credit card and loan accounts and found work. He concealed this employment from SSA in order to continue receiving full disability benefits. Mr. Fleming pled guilty to identity theft and received a sentence of 12 months and 1 day in a Federal penitentiary and 3 years of supervised release. The court ordered him to pay restitution to SSA of over \$29,000 and to creditors of over \$24,000. The victim is in the process of repairing his credit rating with the assistance of FTC.

While it is apparent that our initial action plan has been successful, we have recognized that identity theft is on the increase and we need to expand our role. I believe the SSA-OIG should continue to lead the law enforcement community in the investigations of SSN misuse and identity theft to ensure the integrity of the SSN and SSA's programs. Because of this, I directed our Offices of Audit and Investigations to work together to define the most susceptible areas where SSN misuse and identity theft impact on SSA's programs. After completing this analysis, I focused our investigative resources on the following areas involving SSN misuse if:

- there appears to be a failure of SSA's enumeration business process or the wage and earnings reporting system, since discrepancies in this vein can be indicative of SSN misuse;

- there is the suspicion or an allegation involving the counterfeiting of SSNs;

- there is concealment of work activity by false identification, especially to obtain or maintain eligibility for SSA benefits; and/or

- there appears that a fake SSN is being used to maintain a fictitious identity for the purpose of receiving other Federal and State program benefit payments.

The Office of Audit has also been instrumental in providing recommendations to the Agency that, when implemented, will strengthen the integrity and security of the enumeration function. Enumeration is the process by which SSA assigns original SSNs, issues replacement cards to individuals with existing SSNs, and verifies SSNs for employers and other Federal agencies. SSA issues about 16 million new and replacement cards annually. There are nearly 300 million active cards at this time.

Over the past 3 years, members of Congress have asked the Inspector General community to identify the most significant management issues facing their agencies. In my most recent response I included identity theft. False identities are being used to defraud SSA. Unscrupulous individuals can assume the identity of another person who is either alive or dead and work under the stolen identity. Individuals have also assumed the identity of another person and placed their assets under this identity in order to qualify for SSI payments under their own SSN. I have shared this assessment with the Agency and recommended that they concentrate on the prevention rather than the detection of identity fraud. Because of this, I am also encouraging the Agency to include SSN fraud and misuse as a key initiative in their Strategic Plan.

In addition, SSA's Deputy Commissioner for Finance, Assessment and Management and myself are co-chairs of the National Anti-Fraud Committee. We formed this Committee to facilitate an exchange of ideas—determining what problems we face and suggesting solutions. The Committee is comprised of 10 Regional Anti-Fraud Committees located throughout the country.

In the past year, identity theft and SSN misuse has become a major focus for discussion and because of its importance, we have included it as an agenda item for the National Anti-Fraud Conference that will take place in September.

Currently, there is proposed legislation before the Congress asking to extend civil monetary penalties to those committing crimes involving the misuse of a SSN, who are not being punished by the Federal courts. I urge you to endorse this legislation. There are other legislative remedies such as statutory law enforcement that will enable our investigative offices to process these cases more efficiently and I hope that you support this as well.

I thank the Subcommittee for giving me this opportunity to inform you of our work in the identity theft arena. I pledge, with your support, to vigorously attack the problem of SSN misuse and identity theft before it becomes a national crisis. I would be more than happy to provide the Subcommittee with any additional information or to answer any questions that may arise from these Hearings.