U.S. House of Representatives

Committee on Ways and Means
Subcommittee on Social Security

Statement for the Record

Use and Misuse of Social Security Numbers

The Honorable James G. Huse, Jr.
Inspector General, Social Security Administration

May 9, 2000

Good morning Mr. Chairman and members of the Subcommittee. I want to thank the Subcommittee for holding this hearing on Social Security number (SSN) misuse. Your interest in this critical issue, which impacts on the lives of American citizens, is heartening.

Today, I would like to provide you with a brief overview of how the SSN has been transformed, from a simple Agency record-keeping tool into a cornerstone of modern commerce and what this transformation means for the Social Security Administration (SSA), this Office of the Inspector General (OIG), and the American public. I would also like to provide you with an overview of our efforts in this area. Finally, I offer several options for preventing SSN misuse from the perspective of what I believe to be the responsibility of SSA and by extension, this OIG. The more extensive problem of identity theft requires far more Government action than SSA and this office can provide. I would like to inform you about that, and elicit your views as our oversight committee.

Evolution of the SSN

With the enactment of the Social Security Act in 1935, a system was developed to track the annual earnings of employed individuals. This system required a specific, unique identifier that could accurately maintain earnings records for decades to come. Thus, the SSN was born. The SSN was never intended to be a "national identifier," but over the years, the SSN became the "de facto" identifier for Federal and State Governments. For example, in 1967 the Department of Defense adopted the SSN in lieu of the military service number for identifying Armed Forces personnel. An SSN was required to enroll in schools, receive financial assistance, and to apply for State drivers' licenses. Over time, the SSN has also become a critical identifier for banks, credit bureaus, insurance companies, medical care providers, and innumerable other industries.

Not surprisingly, the introduction of the SSN into the stream of electronic commerce has been accompanied by a dramatic rise in SSN misuse. There is no end to the creativity and ingenuity employed by those with fraudulent intent. Our office is acutely aware of this problem due to the large number of SSN misuse allegations received by our Fraud Hotline and by the increasing number of requests for constituent assistance that we receive from Congressional offices. In FY 1999, our Fraud Hotline processed over 75,000 allegations. Over 80 percent of the allegations and referrals made to our office involve the misuse of an SSN. Specifically, 32,000 had SSN misuse implications involving SSA programs and an additional 30,000 represented SSN misuse

allegations with no direct program implication. In the future, we expect this number to escalate as we begin to process investigative referrals from the Federal Trade Commission (FTC), which was designated as the Federal clearinghouse for identity theft complaints in the *Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act)*. Once the public is fully aware of the FTC's new role, we expect a considerable increase in the number of referrals of SSN misuse each month. These daunting numbers will seriously challenge our already strained resources.

As such, I would now like to describe how SSN misuse impacts SSA's programs and operations, the public, and offer some possible solutions.

SSN Misuse and SSA's Programs and Operations

Our work has revealed that certain misuse occurs because of vulnerabilities in SSA's processes. In many instances, SSN misuse strikes at the core of SSA's programs and operations and we have dedicated substantial resources to this area. For example, our office has investigated numerous cases where individuals apply for benefits under erroneous SSNs. Additionally, we have uncovered situations where individuals counterfeit SSN cards for sale on America's streets. From time to time, we have even encountered SSA employees who sell legitimate SSNs for hundreds of dollars. Finally, we have seen examples where SSA's vulnerabilities in its enumeration business process adds to the pool of SSNs available for criminal fictitious identities. Each of these scenarios has a direct and material impact on the integrity of SSA's programs and operations.

To that end, we have conducted numerous undercover operations regarding trafficking in SSA cards and numbers. We have prioritized SSN misuse cases where there is a material impact on the SSA's Trust Funds, such as benefit application cases. And we have been unyielding in our commitment to root out employee fraud and abuse in the SSN arena. I am pleased to report that SSA employee fraud cases in this area have been few and far between.

Preventing SSN misuse will provide the greatest cost benefit to the Agency. To this end, we have dedicated substantial audit resources to study SSA's business processes, as it relates to the issuance of SSNs. Once an improperly issued SSN enters the stream of commerce, there is scant hope for preventing subsequent damage. As such, we would like to share some of our suggested preventative measures with this Subcommittee.

In May 1999, we issued a Management Advisory Report entitled *Using Social Security Numbers to Commit Fraud*. This report detailed cases in which the Agency issued SSNs based on fraudulent documentation. Thereafter, the improperly issued SSNs were used to commit identity crimes. For example, one individual and his associates obtained 1,120 SSNs for nonexistent children using fraudulent birth certificates. During our investigation, we learned a number of the SSNs were linked to a larger criminal network being investigated by a Secret Service task force where credit card companies were defrauded out of approximately $30 million. We recommended that SSA incorporate preventative controls in its Modernized Enumeration System and as a result, SSA is developing automated edits within the system to identify transactions that have the greatest potential for fraud. This systems upgrade will alert employees to suspicious SSN applications, which they can then refer to the OIG for investigation. The efforts of SSA's

work in this area will potentially result in thousands of cases being referred to our office for investigation over and above what we currently receive.

This month, we released a follow-up report that further examined SSA's procedures for examining evidentiary documents. This draft audit report, entitled *Review of the Social Security Administration's Procedures for Verifying Evidentiary Documents Submitted with Original Social Security Number Applications*, traced the SSN issuance process for over 3,000 SSNs. We selected a judgmental sample of original SSN issuances from a universe of transactions where SSA sent 10 or more SSN cards to a single address within a six-month period. While our small sample was not statistically selected, making extrapolations to the entire SSN universe inappropriate, it was quite instructive in identifying specific vulnerabilities in the SSN issuance process. In our sample, 28 percent of the original SSNs reviewed, or 999 SSNs, were based on invalid evidentiary documents. While a substantial portion of these improperly issued numbers were used to obtain employment, the majority of these numbers were not. It is not implausible to believe that these SSNs were obtained for identity-related crimes. Our draft audit also uncovered the following instances where false identification documents were used to acquire SSNs:

- SSA sent 43 SSN cards to three post office boxes in a small southern town. At our request, Immigration and Naturalization Service (INS) reviewed the application documents and determined that 98 percent of the documents presented were invalid.
- SSA sent 56 SSNs to nonexistent children at seven different addresses. In support of their SSN applications, the "parents" or "guardians" of these purported children had presented invalid birth certificates.

Our draft report concludes that SSA needs stronger procedures and better tools to verify evidentiary documents. Specifically, we will be recommending that SSA employees obtain independent verification of alien evidentiary documents, prior to issuing SSNs. We are also recommending that SSA accelerate negotiations with INS and the State Department to implement an "Enumeration at Entry" program; that SSA not mail new SSNs to a post office box; and that SSA employees receive work credit and recognition for fraud detection and development. Without such recognition, we see little hope for long-term improvements.

We have also determined that there is a direct correlation between SSN misuse and SSA's responsibility to maintain accurate earnings records for individuals. When SSA cannot reconcile SSNs and identifying information provided by employers, SSA sends notices to wage earners requesting pertinent information to resolve the discrepancy. Most of the responses are returned "undeliverable—addressee unknown" to SSA. Some individuals provide the necessary information so that the earnings records can be reconciled while others reply that they do not have a legal SSN.

Our office performed an audit in 1999, entitled *Patterns of Reporting Errors and Irregularities by 100 Employers with the Most Suspended Wage Items*, to determine which major employers had the most suspended wage items, and to examine why this was occurring. Ninety-six of the 100 employers reported over 109,000 SSNs that had never been assigned by SSA. Over 3,000 of these numbers were entirely comprised of zeroes. As for the others, employers admitted that many workers provide incorrect names and SSNs because they do not want to be identified. One of our recommendations to SSA was to develop and implement a corrective action plan for these

100 employers and continue its efforts to contact those employers who are responsible for large numbers of suspended wage items. It is important to take this action because it only costs SSA 50 cents to post a wage item when originally submitted, as compared to $300 to correct it later.

SSN Misuse and Its Impact on the Public

SSN theft also has a substantial impact on the lives of private citizens, as well as private industry. Theft of SSNs is also becoming more and more prevalent as a result of today's electronic environment, which has facilitated easy access to individuals' SSNs and other personal identifying information. This point was highlighted in great detail at the Administration's Identity Theft Summit in March of this year, where several victims explained how the theft of their SSN turned their lives upside down.

Since the passage of the *Identity Theft Act*, which provided the OIG with additional tools to fight SSN theft, the OIG has been in the forefront of the Federal Government's efforts to fight identity theft crimes. The OIG, in conjunction with the U.S. Attorneys' Office in Milwaukee, Wisconsin, was responsible for one of the first criminal prosecutions under this new law. This case exemplifies the extent to which SSN theft has an impact on both SSA's operations and the public.

In Milwaukee, Waverly Burns, a Supplemental Security Income recipient, had commandeered another person's SSN. This stolen SSN was used to secure employment as a cleaning crew supervisor. While on the job, Mr. Burns stole over $80,000 in computer equipment from the offices of the Wisconsin Supreme Court. The stolen SSN was used to obtain a State of Wisconsin identity card, to open bank accounts in the victim's name, and to file fraudulent tax returns. Meanwhile, Mr. Burns continued to falsely represent to SSA that he was disabled and unemployed; indeed no earnings had appeared under his true SSN. On May 5, 1999, OIG special agents arrested Mr. Burns after tracking him to Chicago. Ultimately, Mr. Burns was sentenced to 21 months in prison and ordered to pay over $62,000 in restitution.

We would like to pursue the thousands of potential identity theft cases that we receive each month. With less than 300 investigators nationwide, however, we lack the investigative capacity to handle the entire volume of identity theft referrals. As a result, we are forced to focus on major cases that directly impact on SSA's operations such as the Wisconsin case. Or, we work collectively through task forces with other law enforcement agencies to make the most efficient use of our resources. One of our toughest challenges is to find realistic strategies to fight this battle in an effective and efficient manner, while remaining focused on SSA's programs.

To that end, our Office of Investigations launched an SSN misuse pilot operation in five major American cities last summer. We partnered with Federal and State law enforcement agencies to target identity crimes and SSN misuse. This allowed us to "bundle" smaller SSN cases for prosecutions—cases that would not typically be prosecuted if presented independently. In less than one year, we have opened 125 investigations which have resulted in 30 convictions to date. U.S. Attorneys' Offices and outside law enforcement entities have enthusiastically welcomed such pilots and have thanked our office for taking the investigative lead.

To prepare for the future, we are developing for our fiscal year 2002 budget submission, an integrated model that combines the talents of our auditors, investigators, and attorneys. If authorized, this group will focus its efforts on developing patterns and trends to better target our audit work, refer cases for investigation, and liaison with other relevant public and private sector entities. This appears to be the most effective way of using our resources.

Without any change to our current priorities, I believe we have a responsibility to focus our resources on the SSN's integrity as it relates to SSA core business practices. In particular, we need to focus our audit and investigative attention where there is:

1. an apparent failure of SSA's business processes for issuing SSNs;
2. an apparent failure in SSA's wage and reporting systems;
3. a suspicion that SSN cards are being counterfeited;
4. concealment of work activity using false identifications to obtain or maintain eligibility for Federal benefits.

However, this approach will only provide protection for what is SSA's area of responsibility. It will be little consolation to the thousands of identity theft victims, including private industry, whose cases are the responsibility of an array of Federal, State, and local law enforcement. We have a responsibility to participate in this effort as a major partner to whatever extent we are able.

Possible Solutions

We have several suggestions for SSA and Congress to consider, in addition to our formal audit recommendations that I have discussed previously:

1. Regulating the sale of SSNs;
2. Prohibiting businesses from refusing services for nondisclosure of an SSN when not relevant to the services being provided;
3. Requiring photo identification when conducting business with SSA;
4. Urging the implementation of new technologies and data bases to help employers, Government, and private industry verify that names and/or SSNs are correct to improve the identification process;
5. Legislating statutory law enforcement authority for our investigators; and
6. Broadening civil monetary penalty authority for the sale or misuse of an SSN.

As I close, I hope I have informed this Subcommittee that we presently cannot investigate every instance of identity theft, while fulfilling our mission to protect SSA's programs from fraud, waste, and abuse. When SSN misuse compromises SSA business processes and the Social Security Trust Funds, our involvement is necessary and vigorous. Even in this context, the magnitude of SSN misuse is vast, and our resources are limited. To focus on our mission, we make tough choices to ensure that we bring the most benefit to SSA. Yet, we often become the court of last resort for victims of identity theft. Therefore, I would appreciate your views on how to fulfill the role that the public seems to expect from SSA and this OIG.

Thank you for the opportunity to appear today to discuss this most important issue. I would be happy to answer any further questions from the Subcommittee.