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

July 10, 2003

Good Morning, Mr. Chairman, Mr. Matsui, and members of the Subcommittee. As always, it is a pleasure to be here to assist you in your important work. We have been fighting Social Security number (SSN) misuse and identity theft together for quite a number of years now, starting when I was Acting Inspector General of the Social Security Administration's (SSA) Office of the Inspector General. On March 30, 2000, I testified before this Subcommittee about SSA program integrity issues in general. On that occasion, I expressed my appreciation that the Subcommittee had recognized the importance of confronting SSN misuse, and looked forward to separate hearings that you promised to hold on the issue.

Five weeks later, on May 9, 2000, I returned and reported at length on the misuse of SSNs in many areas, including identity theft. I explained that my office could not possibly investigate every instance of identity theft that involved an SSN. I testified that we were working vigorously on the audit side to identify and eliminate weaknesses in SSA's enumeration process, and just as vigorously on the investigative side to stop SSN misuse crimes that had a direct impact on SSA's programs and operations.

In the year that followed, even as we worked to tighten controls over the issuance of SSNs and fought to deter and punish SSN misuse, identity theft continued to increase. It became apparent that under existing law, we could not do enough to stop criminals from obtaining SSNs, and did not have sufficient enforcement tools to deter them from doing so.

So on May 22, 2001, I returned to this Subcommittee asking for its help. I asked for legislation that would severely restrict the use of SSNs in the private and public sector, and that would criminalize the sale of SSNs. I 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. And I pledged my office's unwavering support of the Subcommittee's efforts to prevent SSN misuse and, by extension, identity theft.

The Subcommittee's response was swift. H.R. 2036, which provided all of the relief I had requested and more, was an important step forward. Tragically, before we could take that step forward, we all took an enormous step back. September 11, 2001 stopped us all in our tracks, and H.R. 2036 understandably took a temporary back seat to more pressing Congressional responsibilities.

But it was a very short time before we collectively realized that H.R. 2036 and September 11 shared more common ground than we had ever contemplated. We had always seen SSN misuse as a bureaucratic problem for the government and a financial problem for the private sector and the citizenry. As our investigative offices were besieged with requests from the FBI for assistance in the September 11 investigation, we quickly came to realize that SSN misuse and identity theft threatened not only credit ratings and government records, but lives as well.

Shortly after the attacks on New York and Washington, I again came before this Subcommittee and testified about individuals seeking to assimilate themselves into our society for nefarious purposes. The assimilation process begins with the use of an SSN whether obtained legally or fabricated. Without it, I explained, it would be all but impossible to function in our society for any extended period. H.R. 2036, which had been an important piece of legislation eight weeks earlier, had become a critical one. Unfortunately, despite the best efforts of this Subcommittee and my office, the 107th Congress adjourned before that Bill became law.

Then just last week, Treasury Secretary John Snow called upon Congress to take additional steps to help stem what he correctly terms "the growing menace of identity theft." While the Secretary's focus was on the harm identity theft visits upon consumers, this Subcommittee knows the damage is much broader than that.

So, I am pleased to be here today, and to see that the Subcommittee's continuing and tenacious dedication to stopping and reversing what is now a long-standing upward trend in SSN misuse and identity theft has never wavered. As you well know, the use of the SSN in American society has expanded to the breaking point. Created in 1935 to track workers' earnings and pay them retirement benefits, its use has increased so dramatically that it has become a part of more government functions and financial transactions than we could ever count. It is our national identifier, and while it serves its purpose well, we as a government remain ill-equipped to afford it the protection it needs and deserves.

I have previously testified as to the need to protect the SSN at three stages: upon issuance, during the life of the number-holder, and following the number-holder's death. This three-tiered approach remains critical.

At Stage One, 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 obtain an SSN from the Federal government fraudulently. If we cannot accomplish this much-ensuring that the government is not an unwitting accomplice to identity theft and other SSN-related crimes-then we will have failed before we have begun. But I can testify today with confidence that this is not the case. Together with you and with SSA, we have made important strides in reducing enumeration vulnerabilities, and that effort continues. Still, legislation is sorely needed to limit the number of replacement Social Security cards an individual can obtain, and to require better cross-verification of records in the enumeration at birth process, to ensure that SSNs are not inappropriately issued in this important program. Excellent progress has been made in the enumeration arena, and we remain

dedicated to even further improvements. At present, SSA is drafting two regulations to tighten the issuance of SSNs to non-workers and foreign students.

Similarly, Stage Three, following the death of the number-holder, is an area in which we are working hard to ensure that, through timely reporting, appropriate cross-matching, and better controls, the SSNs of deceased individuals are not recycled for inappropriate purposes.

But it is at Stage Two 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 sweeping 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. Further, over the last six months, we have led the President's Council on Integrity and Efficiency community in conducting an audit in assessing their respective Agency's practices in the use of SSNs. The final report noted that despite safeguards to prevent improper access, as well as disclosure and use of SSNs by external entities, many agencies remain at risk.

As I stated, the SSN was never intended for the uses to which it is now put millions of times every day. The Identity Theft and Assumption Deterrence Act of 1998 and the Internet False Identification Prevention Act of 2000 provided law enforcement with the initial tools necessary to punish SSN misuse as it relates to identity theft. But each SSN begins and ends at SSA, and true stewardship over that number must reside in the Act that created it, the Social Security Act. That stewardship must focus not only on punishment and deterrence, but also on prevention.

Perhaps the most important step we can take in preventing SSN misuse is to limit the SSN's easy availability. Any meaningful 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, we can never reverse the trend. Any meaningful legislation must 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 in an Internet auction, we will continue to be plagued by the consequences. And legislation, if it is to be meaningful, 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. Secretary Snow commented, "Secure, reliable information is the lifeblood of all financial services, among which consumer credit is fundamental. It is not an overstatement to suggest that preserving the integrity and availability of consumer credit in this economy is preserving prosperity itself. " This is why I have testified that Congress should consider requiring the cross-verification of SSNs through both governmental and private sector systems of records to identify and address anomalies in SSA's files, and in data bases at various levels of government and the financial sector. Only in such a way can we combat and limit the spread of false of identification and SSN misuse. In fact, SSA has taken initial steps toward implementing provisions of the

Patriot Act. This Act requires the Treasury Department to develop a system for domestic financial institutions to verify the identities of foreign nationals seeking to open accounts with information held by Government agencies.

If we can implement these changes, all of which come down to the acceptance of the fact that the SSN has become our national identifier and the application of common sense, criminals will have a far more difficult time obtaining an SSN from SSA or from other sources, and we will be able to better focus on enforcement.

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. Meaningful legislation that is focused solely on SSN misuse must provide meaningful criminal penalties in the Social Security Act, must provide enhanced penalties for those few SSA employees who betray the public trust and assist criminals in obtaining SSNs, and must 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.

Finally, I respect and support SSA's strict privacy regulations. The information SSA stores on each of us is personal, and is entitled to all of the protections we can afford it. I have learned, however, through a series of unfortunate events, that there are times when that privacy must be abridged for the greater good. Following September 11th, and again during last year's sniper attacks in the Washington, D.C. area, it became necessary to share with appropriate law enforcement authorities information stored by SSA to permit those authorities to conduct their investigations and, more importantly, prevent additional lives from being lost. On both occasions, I asked the Commissioner of Social Security to use the ad hoc authority vested in the Commissioner by SSA regulations to permit me to share SSA information with our law enforcement partners. I now ask this Subcommittee for statutory authority that would enable the Inspector General to make such disclosures when necessary to protect human lives without prior formal authorization from the Commissioner. When lives are at stake, we cannot waste precious moments.

Before I close, I would like to emphasize one part of my discussion. While the SSN is issued by SSA, the responsibility for protecting its integrity reaches far beyond this Agency's walls. While SSA has come very far and is willing to do more, other Federal, State and local jurisdictions, as well as the private sector must each do their part. With everyone's participation, we can protect the SSN and ultimately our homeland.

I thank you for your continuing commitment to these critical issues, and would be happy to answer any questions.