U.S. Senate

Special Committee on Aging

Statement for the Record

Identity Theft: The Nation's Fastest Growing Crime Wave Hits Seniors

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

July 18, 2002

Good morning, Chairman Breaux, Ranking Member Craig, and members of the Senate Special Committee on Aging. I want to commend you for holding this important hearing today on identity theft and America's senior citizens.

Criminals do not steal the identities of the elderly so they can pretend to be old and wise. They do it because senior citizens are more likely than most of us to have significant assets--savings, investments, paid-up mortgages, good credit, and Federal entitlement checks. People over age 50 control at least 70 percent of the Nation's household net worth.

Some senior citizens are easier and safer to rob because they are less sure of themselves, more trusting, and less aware of simple precautions. They may be less likely to review their monthly financial statements. They may hesitate to take action if they *do* find something wrong because they are afraid a relative is responsible for robbing them, or because they are afraid they will make their families feel they can no longer be trusted to live independently. As the Federal Trade Commission (FTC) Identity Theft Data Clearinghouse has reported, incidents of identity theft targeting persons over the age of 60 increased from 1,821 victims in 2000 to 5,802 victims in 2001, a threefold increase. Anybody can steal candy from a baby, but criminals know our older Americans have money for the taking and they don't cry out loud.

Identity theft is an "enabling" crime, one that permits criminals to commit *other* crimes more effectively. Those crimes may range from passing bad checks and defrauding credit card companies to horrific acts of terrorism. In most cases, identity theft begins with the misuse of the Social Security number (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 use--and misuse--of the SSN.

There is an almost infinite variety to these cases.

- The New York Times reported recently that thieves are finding houses owned by elderly people, assuming the identity of the true owners and stripping equity out of the houses without their owners' knowledge or consent. In two such cases in Detroit, the Federal Bureau of Investigation (FBI) made its case and identified thieves through resources of the Identity Theft Task Force of Federal, State and local authorities. We serve on that task force with State and local police, various prosecutors, the FBI, Secret Service, and the Postal Inspection Service. The Privacy Rights Clearinghouse says the home sale racket is one of the more innovative types of identity theft officials are encountering.

- Our agents in San Diego were alerted when local law enforcement became suspicious as to the validity of an SSN presented by a man they were questioning. We found that the SSN belonged to a 70 year-old South Dakota woman. This man had been a fugitive felon for 17 years, with 4 prior felony convictions including prison escape. He had created, through the use of fraudulently obtained or counterfeited identification documents, 33 separate and distinct identities. Some were stolen, while others were entirely fictitious. He had used them not only to avoid capture, but to obtain employment as the chief of a fire department, the security chief for a county fair, and other positions of trust. He also committed bank fraud by obtaining credit cards and loans under his assumed identities while receiving Social Security benefits under three of his identities.
- Our Office of Investigations went after a man in Phoenix who had purposely engaged in telemarketing activity targeting individuals who were alone and elderly, and who hoped for something which would give them a better life. His practice generally involved an amount of money less than $500, which made the victim less likely to pursue legal action. He devised telemarketing schemes to defraud SSA beneficiaries, as well as other fraudulent lottery schemes through the mail, for a loss to the victims of approximately $1.3 million. He would send correspondence to these seniors bearing the words "Social Security Administration" and the official SSA seal, advising them they had been approved to receive an additional SSA benefit check, but they would have to pay a "processing fee" ranging from $9 to $99. In some cases, he requested banking information in order to process the fee, and after receiving that information, he withdrew money directly from their checking accounts.

From October 1994 to October 1998, this same man mailed letters and made phone calls using the names Rainbow International, Magic Numbers, and Future Concepts to tell seniors they were part of a group that could participate in pooled lottery winnings upon payment of a processing fee. When individuals mailed checks to one of several mailboxes he maintained at commercial mail receiving companies, he used their signatures and created fictitious authorization forms to gather information, and again withdrew money from their checking accounts.

After our investigation resulted in a 14-count indictment, the man pleaded guilty to mail fraud. The judge termed his activity "despicable," and sentenced him to 36 months incarceration, a special assessment fee of $100, a fine of $7,500, restitution to the 20 victims of approximately $6,736, and 3years supervised release. The special conditions of supervised released included that he not enter into any major financial purchases or obligations without the approval of probation, that he cooperate with the Internal Revenue Service to file tax returns, and that he not engage in telemarketing or the sale of discount merchandise unless in a retail establishment.

- A Virginia man used an SSN to steal an elderly man's identity so he could work under the stolen SSN while continuing to collect disability benefits he no longer deserved under his own number. While using the SSN, he also took out over $24,000 worth of loans and credit for goods and services purchases. The older man's credit was damaged, and his Social Security benefits were interfered with because of the earnings posted to his earnings record at SSA. We got the identity thief and the courts made him repay SSA and the creditors. He was also incarcerated for 1 year, received 3 years of supervised released and was ordered to pay a $100special assessment. But he created a lot of needless hassles for the victim and the financial institutions.

These are not necessarily small operations with solitary victims.

- One investigation we conducted confirmed that over 25,000 people, residents of nearly every State, had been duped by anonymous hoax flyers. Such flyers, which were widely distributed to the elderly, falsely promised recipients they would receive money from the government if they mailed information to a post office box listed on the flyer. One flyer promised $5,000 pursuant to a fictional "Slave Reparations Act." Another promised an unwarranted lump sum payment or an increase in SSA benefits. "Notch Babies" (persons born between 1911 and 1926) were urged to become part of a "National Victims' Register" by sending in a variety of personal information. These flyers required the recipient to provide sensitive personal information such as name, address, telephone number, SSN, and date of birth. Many elderly Americans were so thoroughly confused by the flyers, that they sent copies of identity documents, including Social Security cards, driver's licenses, birth certificates, and military papers to the address on the flyers. By falsely promising additional Social Security payments, the anonymous mailings tricked them into parting with a wealth of personal information. Congress has helped us alert seniors to such frauds.
- We also brought a series of enforcement actions in Texas, in which several companies were ordered to stop sending deceptive Social Security-related advertisements, primarily to senior citizens. Acc-U-Lead, Inc., United States Senior Services, Inc., Mass Mail Media, Inc. and Lead Marketing Alliance, all Texas companies, were ordered to cease such mailings. The founders were also directed to pay penalties of $200,000 to SSA. These payments were part of a settlement in a case brought by our office and the U.S. Attorney's Office regarding government look-a-like documents that appeared to be from SSA. The government's case alleged that these companies sent misleading solicitations that used terms such as "Social Security Supplement Policy" or "2001 Benefit Update," when in reality the solicitations were meant to entice senior citizens to provide sensitive personal information. The defendant companies would then sell this data to private insurance companies and/or agents for up to $16 for each senior's reply. The data purchasers would then contact the seniors and pitch various products such as burial insurance and other related policies. As a result of such deceptive practices, the companies generated substantial revenues over several years from the sale of this sensitive personal information, unwittingly provided by seniors.

These stories illustrate that identity theft is a mushrooming reality. Though it is not a new phenomenon, today's computer technology makes it a great deal easier than it used to be. Amassing somebody's personal details is facilitated by the plethora of databases available today. We each leave markers in our daily commerce -- in credit card charges, loan applications, medical questionnaires, and so on. They are recorded, aggregated, and resold by information brokers without our knowledge and consent, as if they owned our good names. This process of assembly and dissemination is overly facile and extremely fast because of our modern information media. There are seldom sufficient checks and balances to these activities, and too many have access to these details about all of us.

Typically, the victims of such scams are elderly individuals who have a trusting relationship with SSA. Such advertisements cleverly play to their desire for more Social Security-related information or additional Social Security benefits. Many victims never even realize that they

have been tricked into parting with their personal information--they simply assume that SSA never responded to their request for information.

Senior citizens need to be alerted continuously to the dangers of giving away such information. They must be told about toll-free numbers, such as our Fraud Hotline (1-800-269-0271), and Internet sites, such as our own, where they can check on suspicious government mailings. They must be asked to be suspicious of purported government mailings that offer free money in exchange for personal information.

The victims are often scarred emotionally. They feel violated and helpless—and very angry. I've talked to many who were psychologically overwhelmed, because they could not stop what was happening to them. I've talked with elderly people who were terrified of losing their life savings and their homes. Their lives are seriously disrupted because someone else's crooked credit history is recorded on their credit report. In 1999, a Privacy Rights Clearinghouse survey found the average amount of time spent by victims to regain their financial integrity was 175 hours, over a period of 2 years, at an average cost of over $800.

Congress enacted *The Identity Theft and Assumption Deterrence Act* in 1998 and *The Internet False Identification Prevention Act* in 2000. The former was the first legislative response to the growing epidemic of identity thefts and imposed criminal sanctions for those who create a false identity or misappropriate someone else's. The latter closed a loophole left by the first, enabling my office and other law enforcement organizations to pursue those who previously could sell counterfeit Social Security cards legally by maintaining the fiction that such cards were "novelties" rather than counterfeit documents. Both pieces of legislation are helpful, but both treat the disease of identity theft in its later stages, rather than at the onset.

The ability to *prevent* identity theft is even more essential. Previously, I've said that the time has come to put the SSN back into its box. While we cannot return the SSN to its original limited function because of the complexity of how the SSN is used today, we must take steps to limit its use and to limit the *expansion* of its use. First and foremost, the time has come to make the difficult determinations as to those uses that are appropriate and necessary, and those that are merely convenient. The SSN has become a *de facto* national identifier and its daily use has, in many instances, become a luxury we can no longer afford. Similarly, the availability of SSNs on public documents and over the Internet must come to a stop.

Congress should consider requiring the cross verification of SSNs through both governmental and private sector systems of records. Only in such a way can we combat and limit the spread of false of identification and SSN misuse. Similarly all law enforcement should be provided the same SSN verification capabilities currently granted to employers.

We need legislation that regulates the use of the SSN and provides enforcement tools to punish its misuse. If we are to head off the many crimes identity theft breeds--the fraud against public and private institutions, the ruin of people's security, possibly even the disguising of terrorists as ordinary people--we need legislation with provisions such as:

- Restrictions on the private and governmental use of SSNs. This should include restrictions on the sale of SSNs by governmental agencies, prohibition of the display of

SSNs on government checks and driver's licenses or motor vehicle registrations, and some prohibitions of the sale, purchase, or display of the SSN in the private sector.
- Prohibitions of inmate access to SSNs.
- Refusal to do business without receipt of an SSN could be considered an unfair or deceptive act or practice.
- Confidential treatment of credit header information.

In this vein, I applaud the decision announced last week by the Department of the Treasury to remove the SSN from all Treasury checks, including Social Security and Supplemental Security Income checks, as part of Treasury's efforts to protect the privacy of the customer's SSN and help reduce the opportunity for identity theft. This good decision needs to be codified into law.

Parallel legislative changes are needed that do not bear directly on identity theft, but which would also add protections for older Americans and others. They would include:

- Amending the Social Security Act provisions to direct, with certain limitations, the Commissioner of Social Security to fully reimburse Social Security beneficiaries for any part of their benefit that was misused by a representative payee. There are currently about 5 million representative payees who are appointed to receive and apply the benefits of Social Security recipients who cannot manage their own affairs. The potential for harm to seniors is obvious. It would also make good sense to bar the appointment as representative payees of fugitive felons, attorneys who have received certain sanctions, and people who have been convicted of any offense under Federal or State law resulting in imprisonment for more than one year, unless the Commissioner deems their appointment to be appropriate.
- Dishonest representative payees seem to think they have permission to appropriate the identities they are supposed to represent. Recently we worked with the Department of Veterans Affairs (VA) OIG to put away a Kansas man who was representative payee for several older recipients of VA and SSA benefits. He had stolen their benefits to keep his wife satisfied and to pay for his drinking habit, and had sold at least three recipients' farms for more than $70,000 each.
- Strengthening existing provisions of the Social Security Act that prohibit the misuse of symbols, emblems, or names in reference to Social Security or Medicare, to help combat the frauds that lead trusting seniors to send their identity information to criminals who pose as Government agencies.

With such legislation, and the continuing dedication of the Government agencies involved, and of this Special Committee, I am confident that we can reverse the trend of identity theft against older Americans. SSA, my office, the Congress, and the American people must act together to accord both the SSN and our senior citizens the protections against identity theft that both deserve.

Thank you, and I'd be happy to answer any questions.