**Statement of Alice S. Fisher**
**Deputy Assistant Attorney General**
**Criminal Division**
**Before the**
**Special Committee on Aging**
**United States Senate**

**July 18, 2002**

Mr. Chairman and Members of the Committee, thank you for the opportunity to come here today to testify about identity theft and senior citizens. As the Attorney General recently stated, identity theft is one of the fastest growing crimes in the United States. An estimated 500,000 to 700,000 Americans each year have their identity stolen, according to the Privacy Rights Clearinghouse, and many more Americans are victimized by the crimes that identity theft facilitates. These crimes range from bank and credit-card fraud to international terrorism.

Identity theft is an especially difficult crime because the criminal and the victim of the identity theft may never have any personal contact. Identity thieves obtain valuable personal data – such as Social Security numbers, credit-card numbers and expiration dates, and bank account numbers – from a growing variety of sources. Some criminals may use high-tech methods, such as hacking and "spoofing" of websites (i.e., creating fraudulent websites that look like legitimate sites), to conduct their identity thefts through computers and the

Internet. In a federal case recently indicted in the Eastern District of New York, *United States v. McNeese*, the defendant was the administrator of a computer database containing personnel records for approximately 60,000 employees of the Prudential Insurance Company. The defendant allegedly stole the database for which he was responsible, and proceeded to solicit bids for the sale of that information over the Internet. Fortunately, one of the bidders was a detective assigned to the New York Electronic Crimes Task Force, who used an undercover identity to communicate with the defendant, leading to his arrest.

Many identity thieves, however, continue to rely on low-tech means of obtaining other people's forms of identification. These low-tech approaches range from breaking into cars or stealing from mailboxes to "dumpster diving" – that is, rummaging through dumpsters or trash bins to find bank or credit-card statements or "preapproved" credit-card materials that the recipients did not shred or tear up. In one case that a person reported last week to the Department of Justice, a driver employed at the same company as the victim simply took the victim's Social Security number off a company document and proceeded to apply for multiple credit cards in the victim's name.

Perhaps because identity theft in general does not require direct contact between criminal and victim, identity thieves as a group do not appear to be specifically targeting senior citizens in particular. There is no doubt, however, that in certain situations, criminals plan and carry out identity theft and fraud knowing full well that their victims are senior citizens. Here are some examples of federal prosecutions involving identity theft and seniors:

- In a case now under federal indictment in the Eastern District of Michigan, *United States v. Billings*, the defendants and others allegedly worked together to identify houses in the metropolitan Detroit area that were owned free and clear by elderly people. The defendants would allegedly steal the identity of the true owner. They would then strip the equity out of the houses without the owner's knowledge or consent. The defendants allegedly accomplished this by faking a "re-financing" of the property (where they would withdraw equity and obtain a mortgage in the owner's name, and then default on the mortgage). Alternatively, they would fake a "straw sale" of the home. (In these cases they would forge a quit claim from the true owner to a second subject and then "sell" the home to a third subject, who would obtain a mortgage on the property.

The second subject obtained the proceeds of the "sale", and the third subject defaulted on the mortgage.)

- In a completed federal prosecution in the Eastern District of North Carolina, *United States v. Hooks*, the defendant stole mail from senior citizens throughout North Carolina, used the biographical information contained in the stolen mail to produce fake drivers' licenses and counterfeit checks, and then used the licenses and checks to withdraw the citizens' life savings out of their bank accounts. To produce the licenses, the defendant had obtained an official North Carolina Department of Motor Vehicles license machine. (He later claimed that he purchased the DMV machine on eBay.) In this case, which the United States Secret Service investigated, the loss resulting from the defendant's criminal conduct was $177,472.63. The defendant ultimately pleaded guilty to mail theft, production of false identification documents, and use of false identification, and was sentenced on November 1, 2000, to 63 months imprisonment. The conviction was upheld by the U.S. Court of Appeals for the Fourth Circuit in 2001.
- In another federal prosecution in the Eastern District of North Carolina, *United States v. Robinson*, the defendant took a job as a live-in companion

for an elderly woman. After the elderly woman was hospitalized, the defendant obtained and used credit cards in the elderly woman's name, stealing $47,051.35. In this case, which the United States Secret Service also investigated, the defendant pled guilty to access device fraud and production of false checks, and was sentenced in May 2000 to 31 months imprisonment.

There is no doubt that identity theft can create significant hardships for its victims. Once an identity thief has obtained access to the victim's bank or financial accounts, the victim may suffer significant financial losses and considerable emotional distress. In a 2001 federal prosecution in the Northern District of Texas, *United States v. Lake*, one of the victims was an 80-year-old military widow whose checkbook had been stolen from her vehicle. After the criminals had drained thousands of dollars from her bank account, her physician states that he had to treat her for high stress she experienced as a result of the identity theft.

In some cases, long periods of time may go by before the identity theft victim realizes that he or she has been targeted. In a federal prosecution in the

District of Arizona, *United States v. Hooper*, the defendant, a Canadian citizen, pleaded guilty on April 5, 2002 to fraudulent use of a Social Security number. The defendant admitted that since 1982 she had been using the Social Security number of a naturalized U.S. citizen for the purpose of concealing her true identity and obtaining credit. The victim had had her Social Security card and other identification documents stolen in Canada in 1982. Because the victim was originally a Canadian citizen and was averse to using credit for purchases, the defendant's fraud went undetected for 20 years. During that period, the defendant, while using the victim's Social Security number, got an Arizona driver's license, filed for bankruptcy in Oklahoma, and was arrested.

Identity theft victims, beyond any direct financial losses they may suffer, often encounter unanticipated additional burdens. For many identity theft victims, the process of contacting credit bureaus and creditors and trying to restore their good names and credit can be extremely frustrating. While creditors may want victims to produce evidence of the identity theft, such as a police report, many police officers may not know that identity theft is a crime in their state and may be disinclined to take a police report if they believe that the

actual frauds resulting from the identity theft took place outside their jurisdiction.

The Department of Justice regards identity theft as a serious criminal violation that requires a coordinated response from all levels of law enforcement --federal, state, and local. The Department has therefore undertaken a three-pronged approach to identity theft. First, the Department is vigorously pursuing identity theft prosecutions across the country. Most recently, in May 2002, the Department conducted a nationwide "sweep" of federal prosecutions targeting identity theft. In that sweep, the Department brought 73 criminal prosecutions against 135 individuals in 24 districts.

Second, the Department is pursuing additional legislation to address the most serious cases of identity theft and to provide greater protection to the public, through enhanced criminal penalties. S. 2541, which Senator Feinstein introduced with bipartisan sponsorship on May 22nd, would create a new crime of aggravated identity theft. This new class of identity theft is defined by the nature and seriousness of the crimes committed through the use of another's identity. Under the provisions of S. 2541, individuals found guilty of

aggravated identity theft will receive an additional two years imprisonment over and above their sentences for the underlying offense, or an additional five years imprisonment where the underlying offense is terrorism-related. S. 2541 would also enhance the current identity theft statute, section 1028, by prohibiting not just the transfer or use of another's identity information, but also possession of such information in conjunction with the requisite criminal intent. In addition, the maximum penalties for identity theft are increased and a higher maximum penalty is included for identity theft used to facilitate acts of domestic terrorism.

Third, the Department recognizes the importance of educating law enforcement and the general public about identity theft. Too many people, even criminal justice professionals, do not fully understand what identity theft is or how it can affect their lives and assets. As a result, the Department is sponsoring or directly supporting a number of approaches to identity theft education and prevention.

With respect to law enforcement, the Department has integrated training about identity theft into many of the curricula for federal prosecutors at the

Department's National Advocacy Center. Basic courses on white-collar crime and cybercrime, as well as advanced training on Internet fraud and other types of major fraud, now include training modules on identity theft. In addition, the Department has enthusiastically cosponsored a series of law enforcement training seminars about identity theft with the Federal Trade Commission and the United States Secret Service. To date, these joint training seminars, which have been held in Washington, D.C., Chicago, Des Moines, and San Francisco, have provided much-needed training to more than four hundred local, state, and federal law enforcement officers. Another of these training seminars is set for August 2002 in Dallas. The Department, the FTC, and the Secret Service are now actively discussing plans to expand these seminars to other areas of the country.

One of the elements of our training seminars on identity theft involves the Identity Theft Data Clearinghouse of the Federal Trade Commission's Consumer Sentinel database. The Clearinghouse offers investigators secure online access to an extensive database of more than 189,000 complaints as of the end of June 2002 about identity theft. Because the Department regards Consumer Sentinel as an invaluable resource in investigating identity theft cases, our training explains

what kinds of complaint data are available in Consumer Sentinel and how investigators and prosecutors can get access to Consumer Sentinel to search the Data Clearinghouse.

In addition, the Secret Service and the International Association of Chiefs of Police are now exploring the development of a "roll call" video that would be made available to police departments throughout the United States. This roll call video would allow police departments to provide their officers at roll calls with a concise explanation of identity theft and its significance as a criminal problem. More police departments need to understand the problem of identity theft and the importance of responding to identity theft victims by taking police reports. We are hopeful that this project can encourage many more officers to assist victims and pursue identity theft cases in their states.

With respect to the general public, the Department also supports a variety of education and prevention efforts. For example, the Department has a website on identity theft that explains the crime, how it can be committed, and what people should do if they think they have become identity theft victims. Very recently, the Department has added to its website an identity theft quiz for

consumers. This quiz, which can be found at www.usdoj.gov, provides consumers with a handy checklist of what they can do to reduce the risks of becoming identity theft victims, and how to report if they think they have become victims. Finally, the Department works closely with the FTC in its ongoing public education efforts about identity theft. We believe that the FTC has done an excellent job of public outreach and prevention on this subject, and are happy to provide continuing support of its efforts.

Mr. Chairman, that concludes my prepared remarks. I will be happy to respond to any questions that you or other members of the Committee may have.

* * *