STATEMENT OF DOUGLAS COOMBS

Deputy Special Agent in Charge
United States Secret Service
Financial Crimes Division

Before the Special Committee on Aging

United States Senate

July 18, 2002

Mr. Chairman, I would like to thank you, as well as the distinguished Ranking Member, Senator Craig, for the opportunity to address the Committee on the issue of identity theft and the Secret Service's efforts to combat this problem. I am particularly pleased to be here with my colleagues and partners in fighting identity theft from the Federal Trade Commission, Department of Justice, and the Social Security Administration.

The Secret Service was originally established within the Department of the Treasury in 1865 to combat the counterfeiting of U.S. currency. Since that time, this agency has been tasked with the investigation of other Treasury related crimes, as well as the protection of our nation's leaders, visiting foreign dignitaries and events of national significance. With the passage of new federal laws in 1982 and 1984, the Secret Service was provided jurisdiction for the investigation of the counterfeiting of identification documents, as well as access device fraud. The explosive growth of these crimes has resulted in the evolution of the Secret Service into an agency that is recognized worldwide for its expertise in the investigation of all types of financial crimes.

The burgeoning use of the Internet and advanced technology coupled with increased investment had led to a great expansion of activity within the financial sector. Although this provides benefits to the consumer through readily available credit and consumer oriented financial services, it also creates a target rich environment for today's sophisticated criminals, many of who are organized and operate across international borders.

Information collection has become a common byproduct of the newly emerging e-commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by entrepreneurs intent on increasing their market share. This has led to an entirely new business sector being created which promotes the buying and selling of personal information. Consumers routinely provide personal, financial and health information to companies engaged in business on the Internet. They may not realize that the information they provide in credit

card applications, loan applications, or with merchants they patronize are valuable commodities in this new age of information trading. With the advent of the Internet, companies have been created for the sole purpose of data mining, data warehousing, and brokering of this information. These companies collect a wealth of information about consumers, including information as confidential as their medical histories. Like all businesses, data collection companies are profit motivated, and as such, may be more concerned with generating potential customers rather than safeguarding their information to prevent its misuse by unscrupulous individuals. The private sector represents the first line of defense in identity theft and has a responsibility to safeguard the data that it has collected. The greater the protections that industry provides to the public, the fewer the opportunities for identity theft.

Based upon this wealth of available personal information, the crime of identity theft can be perpetrated with minimal effort on the part of even relatively unsophisticated criminals.

There is no area today that is more relevant or topical than that of identity theft. Simply stated, identity theft is the use of another person's identity to commit fraudulent activity.

Identity theft is not typically a "stand alone" crime. It is almost always a component of one or more crimes, such as bank fraud, credit card or access device fraud, or the passing of counterfeit financial instruments. In many instances, an identity theft case encompasses multiple types of fraud. According to statistics compiled by the FTC for the year 2001, 20% of the 86,168 victim complaints reported involved more than one type of identity theft. The major complaints, which include multiple types of reported fraud, were:

- **42%** of complaints involved credit card fraud – i.e. someone either opened up a credit card account in the victim's name or "took over" their existing credit card account;

- **20%** of complaints involved the activation of telephone, cellular, or other utility service in the victim's name;

- **13%** of complaints involved bank accounts that had been opened in their name, and/or fraudulent checks had been negotiated in the victim's name;

- **7%** of complaints involved consumer loans or mortgages that were obtained in the victim's name;

- **9%** of complaints involved employment-related fraud;

- **6%** of complaints involved government documents/benefits fraud; and

- **17%** of miscellaneous fraud, such as medical, bankruptcy, criminal, and securities fraud.

IMPACT

Identity theft, unlike many types of crime, affects all Americans, regardless of age, gender, nationality, or race. Victims include everyone from restaurant workers, telephone repair technicians, and police officers, to corporate and government executives, celebrities and high-ranking military officers. What victims do have in common is the difficult, time consuming, and potentially expensive task of repairing the damage that has been done to their credit, their savings, and their reputation. Obviously, the impact is magnified when it affects one of America's most valued assets, our senior citizens, as they represent a generation with a trusting nature that is easy to exploit. This group is particularly dependent on other caregivers for assistance, such as relatives, medical staff, service personnel, an oftentimes, complete strangers. This dependency increases their vulnerability to certain schemes involving identity theft.

LEGISLATION

In past years, victims of financial crimes such as bank fraud or credit card fraud were identified by statute as the person, business, or financial institution that incurred a financial loss. All too often the individuals whose credit was ruined through identity theft were not even recognized as victims. This is no longer the case. The Identity Theft and Assumption Deterrence Act, passed by Congress in 1998, represented a comprehensive effort to re-write the federal criminal code to address identity theft. This new law amended Section 1028 of title 18 of the United States Code to provide greater protections for victims of identity theft. These protections included:

- expanding the definition of victim to include not just those persons, businesses or institutions that incurred monetary loss, but also those individuals whose credit was compromised as a result of financial crimes such as bank fraud or credit card fraud;

- The establishment of the Federal Trade Commission (FTC) as the central clearinghouse for victims to report incidents of identity theft. This centralization of all identity theft cases allows for the identification of systemic weaknesses and provides law enforcement with the ability to retrieve investigative data at one central location. It further allows the FTC to provide victims with the information and assistance they need in order to take the steps necessary to correct their credit records;

- Sentencing potential and asset forfeiture provisions were enhanced to help to reach prosecutorial thresholds and allow for the repatriation of funds to victims; and

- The elimination of a significant loophole in existing statutes. Previously, only the production or possession of false identity documents was unlawful. With advances in technology such as E-commerce and the Internet, criminals did not need actual, physical identity documents to assume an identity. This legislative change made it

illegal to steal another person's personal identification *information* with the intent to commit a violation, regardless of actual possession of identity *documents*.

We believe that the passage of this legislation was the catalyst needed to bring together both the federal and state government's resources in a focused and unified response to the identity theft problem. Today, law enforcement, regulatory and community assistance organizations have joined forces through a variety of working groups, task forces, and information sharing initiatives to assist victims of identity theft.

Amendments later made to the Identity Theft and Assumption Deterrence Act of 1998 provided a two level increase and a minimum offense level of 12 for offenses involving (1) the possession or use of equipment that is used to manufacture access devices; (2) the production of, or trafficking in, unauthorized and counterfeit access devices; or (3) affirmative identity theft. This legislation also defined affirmative identity theft as the "breeding" of means of identification, and enhanced penalties under certain circumstances, such as the possession of five or more means of identification that were unlawfully produced.

These amendments also provided a revised minimum loss rule for offenses involving counterfeit or unauthorized access devices. Specifically, this rule requires that a minimum loss amount of $500 per access device be used when calculating the loss involved in the offense, with the exception of the possession, not the use of, telecommunications access devices, in which case the minimum loss per unused device is $100.

Finally, these amendments encouraged an upward departure if the offense level does not accurately reflect the seriousness of the offense. Examples of cases in which a departure may be warranted include those in which (1) an identity theft cause substantial harm to the victim's reputation or credit record; (2) an individual is arrested, or is denied a job, because of a misidentification that resulted from an identity thief; or (3) a defendant essentially assumed the victim's identity.

Violations of the Act are investigated by federal law enforcement agencies, including the Secret Service, the U.S. Postal Inspection Service, the Social Security Administration (Office of the Inspector General), and the Federal Bureau of Investigation. Schemes to commit identity theft or fraud may also involve violations of other statutes, such as credit card fraud, computer fraud, mail fraud, wire fraud, financial institution fraud, or Social Security fraud, as well as violations of state law. Because identity theft is often connected to criminal activity that comes under the jurisdiction of the Secret Service, we have taken an aggressive stance and continue to be a leading agency for the investigation and prosecution of such criminal activity.

Finally, we aware of the legislation, S. 2541, recently proposed by the Administration and introduced by Senators Feinstein, Kyl, Sessions and Grassley. There are some excellent ideas included in this legislation that we believe will be highly useful in all of our efforts to combat the crime of identity theft.

SECRET SERVICE INVESTIGATIONS

Although financial crimes are often referred to as "white collar" by some, this characterization can be misleading. The perpetrators of such crimes are increasingly diverse and today include organized criminal groups, street gangs and convicted felons. This can be attributed to many factors including:

- The probability of high financial gain versus low sentencing exposure;
- The increased availability of goods or services which can be obtained on credit; and
- The proliferation of computer technology in our society that provides easy access to the information needed to commit many financial crimes, as well as a means for committing them remotely.

The personal identifiers most often sought by criminals are those generally required to obtain goods and services on credit. These are primarily social security numbers, names, and dates of birth.

The methods of identity theft vary. It has been determined that many "low tech" identity thieves obtain personal identifiers by going through commercial and residential trash, a practice known as "dumpster diving". The theft of both incoming and outgoing mail from mailboxes is a practice used equally as often by individuals and organized groups, along with thefts of wallets and purses.

With the proliferation of computers and increased use of the Internet, many identity thieves have used information obtained from company databases and web sites. A case investigated by the Secret Services that illustrates this method involved an identity thief accessing a public web site to obtain the social security numbers of military officers. In some cases, the information obtained is in the public domain, and in others, it is proprietary, and is obtain by means of a computer intrusion.

The method that may be most difficult to prevent is theft by a collusive employee. The Secret Service has discovered that individuals or groups who wish to obtain personal identifiers or account information for a large-scale fraud ring will often pay or extort an employee who has access to this information through their employment at workplaces such as a financial institution, medical office, or government agency.

In most of the cases our agency has investigated involving identity theft, criminals have used another individual's personal identifiers to apply for credit cards or consumer loans. Less commonly, they are used to establish bank accounts, leading to the laundering of stolen or counterfeit checks, or are used in a check-kiting scheme.

The majority of identity theft cases investigated by the Secret Service are initiated on the local law enforcement level. In most cases, the local police department is the first

responder to the victims once they become aware that their personal information is being used unlawfully. Credit card issuers as well as financial institutions will also contact a local Secret Service field office to report possible criminal activity.

At the present time, the Secret Service does not compile statistics related to the age of victims for any type of investigation. The FBI's Uniform Crime Report, the premier crime statistic resource, does capture victim statistics, but only for the crime of murder. It should be noted, however, that due to the FTC's designation as the clearinghouse for consumer complaints, their statistics are readily available and delineated by geography, age, and type of fraudulent activity.

A significant probability exists that older Americans will become an increasingly attractive target by criminal elements given the fact that 70% of our nation's wealth is controlled by those 50 years of age and older. Additionally, the common perception is that it is difficult for elderly victims to repair the effects of identity theft due to a lack of technical knowledge and uncertainty on how to protect themselves. Often, the level of diligence in monitoring personal finances decreases among the elderly or, after discovering the fraudulent activity, some are embarrassed and unsure of the steps necessary to report the compromise.

COORDINATION

The Secret Service continues to attack identity theft by aggressively pursuing our core violations, which include violations involving counterfeit checks, counterfeit and fraudulently obtained credit cards, other counterfeit instruments, and false identification. Many of these schemes would not be possible without compromising the personal financial information of an innocent victim.

Our own investigations have frequently involved the targeting of organized criminal groups that are engaged in financial crimes on both a national and international scale. Many of these groups are prolific in their use of stolen financial and personal information to further their financial crime activity.

It has been our experience that the criminal groups involved in these types of crimes routinely operate in a multi-jurisdictional environment. This has created problems for local law enforcement agencies that generally act as the first responders to their criminal activities. By working closely with other federal, state, and local law enforcement, as well as international police agencies, we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise which bridges jurisdictional boundaries. This partnership approach to law enforcement is exemplified by our financial and electronic crime task forces located throughout the country. These task forces primarily target suspects and organized criminal enterprises engaged in financial and electronic criminal activity that falls within the investigative jurisdiction of the Secret Service. Members of these task forces, which include local and state law enforcement, private industry and academia, pool their resources and expertise in a collaborative effort to detect and prevent electronic crimes.

While our task forces do not focus exclusively on identity theft, we recognize that a stolen identity is often a central component of other electronic crimes. Consequently, our task forces devote considerable time and resources to the issue of identity theft, including the "pure" identity theft cases that meet prosecutive guidelines and are consistent with the task force's case prioritization strategy.

Another important component of the Secret Service's preventative and investigative efforts has been to increase awareness of issues related to financial crime investigations in general, and of identity theft specifically, both in the law enforcement community and the general public. The Secret Service has tried to educate consumers and provide training to law enforcement personnel through a variety of partnerships and initiatives.

For example, criminals increasingly employ technology as a means of communication, a tool for theft and extortion, and a repository for incriminating information. As a result, the investigation of all types of criminal activity, including identity theft, now routinely involves the seizure and analysis of electronic evidence. In response to this trend, the Secret Service developed, in conjunction with the International Association of Chiefs of Police (IACP), the "Best Practices for Seizing Electronic Evidence Manual", to assist law enforcement officers in recognizing, protecting, seizing and searching electronic devices in accordance with applicable statutes and policies.

As a follow-up to this guide, the Secret Service and the IACP developed "Forward Edge"; a computer based training application designed to allow officers to "virtually" seize different types of evidence, including electronic evidence, at various crime scenes.

Further, the Secret Service, in conjunction with the U.S. Postal Inspection Service and the Federal Reserve Bank System, produced an identity theft awareness video. The video, which explains how easily one can become a victim and what steps should be taken to minimize damage, has been made available to Secret Service offices for use in public education efforts.

In April of 2001, the Secret Service assisted the FTC in the design of an identity theft brochure, containing information to assist victims on how to restore their "good name", as well as how to prevent their information and identities from becoming compromised.

Finally, the International Association of Chiefs of Police (IACP and the Secret Service have partnered to produce an "Identity Theft Roll-Call Video" geared toward local police officers throughout the nation. The purpose of this video is to emphasize the need for police to document a citizen's complaint of identity theft, regardless of the location of the suspects. In addition, the video and its companion reference card will provide officers with information that can assist victims with remediation efforts.

The Secret Service is also actively involved with a number of government-sponsored initiatives. At the request of the Attorney General, the Secret Service joined an interagency identity theft subcommittee that was established by the Department of

Justice. This group, which is comprised of federal, state, and local law enforcement agencies, regulatory agencies, and professional agencies, meets regularly to discuss and coordinate investigative and prosecutive strategies as well as consumer education programs.

Last spring, the Secret Service's Financial Crimes Division assigned a full time special agent to the FTC to support all aspects of their program to encourage the use of the Identity Theft Data Clearinghouse as a law enforcement tool. The Identity Theft and Assumption Deterrence Act established the FTC as the central point of contact for identity theft victims to report all instances of identity theft. The FTC has done an excellent job of providing people with the information and assistance they need in order to take the steps necessary to correct their credit records, as well as undertaking a variety of "consumer awareness" initiatives regarding identity theft. To date, the Secret Service representative at the FTC has:

- Met with and made presentations to federal, state and local law enforcement about the FTC's Identity Theft Data Clearinghouse and it's victim assistance program;

- Worked closely with agents in the field to ensure that they have access to the Consumer Sentinel system and are comfortable using the Identity Theft Data Clearinghouse database;

- Used the Identity Theft Data Clearinghouse to identify possible case leads, and developed a protocol for selecting which victim complaints are most likely to be successful case leads for criminal law enforcement agencies;

- Developed points of contact at the local, state and federal levels of government to receive case lead referrals from the Identity Theft Data Clearinghouse database, and also identified routines and procedures to be followed when referring such cases;

- Served as both a presenter and an instructor at 11 law enforcement training conferences hosted by various law enforcement agencies or organizations, such as the International Association of Financial Crimes Investigators (IAFCI) and the U.S. Marshal's Investigators Conference; and

- Coordinated and sponsored Identity Theft Seminars which have been attended by approximately 1,400 state and local law enforcement personnel.

It is important to recognize that public education efforts can only go so far in combating the growth of identity theft. Because social security numbers, in conjunction with other personal identifiers, are used for such a wide variety of record keeping and credit related applications, even a consumer who takes appropriate precautions to safeguard such information is not immune from becoming a victim.

PRECAUTIONS AND REMEDIES

The Secret Service recommends that consumers take the following steps to protect themselves from credit card fraud and identity theft:

- Maintain a list of all credit card accounts that is not carried in a wallet or purse so that immediate notification can occur if any cards are lost or stolen;

- Avoid carrying any more credit cards in a wallet or purse than is actually needed;

- Cancel any accounts that are not in use;

- Be conscious of when billing statements should be received, and if they are not received during that window, contact the sender;

- Check credit card bills against receipts before paying them;

- Avoid using a date of birth, social security number, name or similar information as a password or PIN code, and change passwords at least once a year;

- Shred or burn pre-approved credit card applications, credit card receipts, bills and other financial information that you do not want to save;

- Order a credit report once a year from each of the three major credit bureaus to check for inaccuracies and fraudulent use of accounts; and

- Avoid providing any personal information over the telephone unless you initiated the call, and be aware that individuals and business contacted via the Internet may misrepresent themselves.

Should an individual become the victim of identity theft, the Secret Service recommends the following steps:

- Report the crime to the police immediately and get a copy of the police report;

- Immediately notify your credit card issuers and request replacement cards with new account numbers. Also request that the old account be processed as "account closed at consumers' request" for credit record purposes. Ask that a password be used before any inquiries or changes can be made on the new account. Follow up the telephone conversation with a letter summarizing your requests;

- Call the fraud units of the three credit reporting bureaus, and report the theft of your credit cards and/or numbers. Ask that your accounts be flagged, and add a victim's statement to your report that requests that they contact you to verify future credit applications. Order copies of your credit reports so you can review them to make sure no additional fraudulent accounts have been opened in your name;

- Notify the Social Security Administration's Office of Inspector General if your social security number has been used fraudulently;

- File a complaint with the Federal Trade Commission (FTC) by calling 1-877-ID-THEFT or writing to them at Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, DC 20580. Their website can also be accessed at www.ftc.gov/ftc/complaint.htm; and

- Follow up with the credit bureaus every three months for at least a year and order new copies of your reports so that you can verify that corrections have been made, and to make sure that no new fraudulent accounts have been established.

CONCLUSION

For law enforcement to properly prevent and combat identity theft steps must be taken to ensure that local, state and federal agencies are addressing victim concerns in a consistent manner. All levels of law enforcement should be familiar with the resources available to combat identity theft and to assist victims in rectifying damage done to their credit. It is essential that law enforcement recognize that identity theft must be combated on all fronts, from the officer who receives a victim's complaint, to the detective or Special Agent investigating an organized identity theft ring.

The Secret Service has already undertaken a number of initiatives aimed at increasing awareness and providing the training necessary to address these issues, but those of us in the law enforcement and consumer protection communities need to continue to reach out to an even larger audience. We need to continue to approach these investigations with a coordinated effort – this is central to providing a consistent level of vigilance and addressing investigations that are multi-jurisdictional while avoiding duplication of effort.

As you know, Mr. Chairman, the President has proposed transferring our agency and all of its functions to the new Department of Homeland Security. The Secret Service strongly supports this proposal, and we are confident that our ability to build partnerships with state and local law enforcement, as well as the private sector, will allow us to continue our preventative and investigative efforts with respect to identity theft as a leading agency in the new department.

The Secret Service is prepared to assist this committee in protecting and assisting the nation's largest growing population segment, with respect to the prevention, identification and prosecution of identity theft criminals.

Mr. Chairman, that concludes my prepared remarks and I would be happy to answer any questions that you or other members of the committee may have.