Statement of Mr. Timothy Caddigan

Special Agent in Charge
Criminal Investigative Division
United States Secret Service

Presentation to the Senate Committee on Banking, Housing and Urban Affairs

United States Senate

June 19, 2003

Mr. Chairman, Senator Sarbanes, thank you for inviting me to be part of this hearing today, and the opportunity to address the committee regarding the Secret Service's efforts to combat identity crime and protect our nation's financial infrastructure.

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 financial crimes, as well as the protection of our nation's leaders, visiting foreign dignitaries and events of national significance. Although we have moved to the Department of Homeland Security, the Secret Service has maintained historic relationships with the Department of the Treasury in our ongoing efforts to ensure a secure financial services infrastructure.

With the passage of new federal laws in 1982 and 1984, the Secret Service was provided primary authority for the investigation of access device fraud, including credit and debit card fraud, and parallel authority with other law enforcement agencies in identity crime cases. 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. Our efforts to detect, investigate and prevent financial crimes are aggressive, innovative and comprehensive.

The burgeoning use of the Internet and advanced technology, coupled with increased investment and expansion, has intensified competition within the financial sector. With lower costs of information-processing, legitimate companies have found it profitable to specialize in data mining, data warehousing and information brokerage. Information collection has become a common byproduct of newly-emerging e-commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by businesses seeking to find the best customers for their products. This has led to a new measure of growth within the direct marketing industry that promotes the buying and selling of personal information. In today's markets, consumers

routinely provide personal and financial identifiers 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. Consumers may be even less aware of the illegitimate uses to which this information can be put. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders. But legitimate business can provide a first line of defense against identity crime by safeguarding the information it collects. Such efforts can significantly limit the opportunities for identity crime, even while not eliminating its occurrence altogether.

Simply stated, identity crime is the theft or misuse of an individual's personal or financial identifiers in order to gain something of value or to facilitate other criminal activity. Types of identity crime include identity theft, credit card fraud, bank fraud, check fraud, false identification fraud, and passport/visa fraud. Identity crimes are almost always associated with other crimes such as narcotics and weapons trafficking, organized crime, mail theft and fraud, money laundering, immigration fraud, and terrorism.

According to statistics compiled by the FTC for the year 2002, 22% of the 161,819 victim complaints reported involved more than one type of identity crime. The complaints were broken down as follows (note that some complaints involved more than one of the listed activities):

- **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;

- **22%** of complaints involved the activation of telephone, cellular, or other utility service in the victim's name;

- **17%** of complaints involved bank accounts that had been opened in the victim's name, and/or fraudulent checks had been negotiated in the victim's name;

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

- **8%** of complaints involved government documents/benefits fraud;

- **6%** of complaints involved consumer loans or mortgages that were obtained in the victim's name; and

- **16%** of complaints involved some type of miscellaneous fraud, such as medical, bankruptcy and securities fraud.

Identity crime is not targeted against any particular demographic; instead, it affects all types of 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. According to a report by the General Accounting Office, the average victim spends over 175 hours attempting to repair the damage done by identity criminals.

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. As a result of the passage of the Identity Theft and Assumption Deterrence Act in 1998, this is no longer the case. This legislation represented the first comprehensive effort to re-write the federal criminal code to address the insidious affects of identity theft on private citizens. This new law amended Section 1028 of Title 18 of the United States Code to provide enhanced investigative authority to combat the growing problem of identity theft. These protections included:

- 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;

- The enhancement of asset forfeiture provisions to allow for the repatriation of funds to victims; and

- The closing of a significant gap in then-existing statutes. Previously, only the production or possession of false identification documents was unlawful. However, with advances in technology such as E-commerce and the Internet, criminals did not need actual, physical identification documents to assume an identity. This statutory 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 federal and state government resources in a focused and unified response to the identity crime 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 crime.

As you know, Mr. Chairman, the Senate recently passed the Identity Theft Penalty Enhancement Act of 2002. The intent of this act is to establish increased penalties for aggravated identity theft -- that is, identity theft committed during and in relation to certain specified felonies. This act, in part, provides for two years imprisonment for the identity crime, in addition to the punishment associated with the related felony and five years imprisonment if the related felony is associated with terrorism. Additionally, the

Act prohibits the imposition of probation and allows for consecutive sentences. While this particular legislation cannot be expected to completely suppress identity theft, it does recognize the impact identity theft has on consumers and the need to punish those engaging in criminal activity for personal or financial gain. The Secret Service supports these ideas and believes they represent additional tools that law enforcement can utilize to the fullest extent in protecting the American people.

Identity crime violations 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 crime may also involve violations of other statutes, such as computer crime, mail theft and fraud, wire fraud, or Social Security fraud, as well as violations of state law. Because most identity crimes fall 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.

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 both domestic and international organized criminal groups, street gangs, convicted felons and terrorists.

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. Identity crimes also involve the theft or misuse of an individual's financial identifiers such as credit card numbers, bank account numbers and personal identification numbers.

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

With the proliferation of computers and increased use of the Internet, many identity criminals have used information obtained from company databases and web sites. A case investigated by the Secret Services that illustrates this method involved an identity criminal accessing public documents to obtain the social security numbers of military officers. In some cases, the information obtained is in the public domain while in others it is proprietary and is obtained 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 or financial identifiers 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 that our agency has investigated involving identity theft, criminals have used an individual's personal identifiers to apply for credit cards or consumer loans. Additionally, these identifiers were also used to establish bank accounts, leading to the laundering of stolen or counterfeit checks or were used in a check-kiting scheme.

The majority of identity crime 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 or financial identifiers are 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.

The events of September 11, 2001 have altered the priorities and actions of law enforcement throughout the world, including the Secret Service. Immediately following the attacks, Secret Service assisted the FBI with their terrorism investigation through the leveraging of our established relationships, especially within the financial sector, in an attempt to gather information as expeditiously as possible.

As part of the new Department of Homeland Security, the Secret Service will continue to be involved in a collaborative effort with the intention of analyzing the potential for identity crime to be used in conjunction with terrorist activities through our liaison efforts with the Bureau of Immigration and Customs Enforcement, Operation Direct Action, FinCEN, the Diplomatic Security Service and the Terrorist Financing Operations Section of the FBI.

The Secret Service continues to attack identity crime by aggressively pursuing our core Title 18 investigative violations, including access and telecommunications device fraud, financial institution fraud, computer fraud and counterfeiting. Many of these schemes are interconnected and depend upon stealing and misusing the personal and financial identifiers of innocent victims.

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 identifiers to further their other criminal 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 that bridges jurisdictional boundaries. This partnership approach to law enforcement is exemplified by our financial and electronic crime task forces located throughout the country, pursuant to our section 1030 computer crime authority. 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, who include representatives from local and state law enforcement, prosecutors offices, private industry and academia, pool their resources and expertise in a collaborative effort to detect and prevent electronic crimes. The value of this crime fighting and crime prevention model has been recognized by Congress, which has authorized the Secret Service (pursuant to the USA/Patriot Act of 2001) to expand our electronic crime task forces to cities and regions across the country. Recently, four new Electronic Crimes Task Forces were established in Dallas, Houston, Columbia (SC) and Cleveland, bringing the total number of ECTFs to 13.

While our task forces do not focus exclusively on identity crime, we recognize that stolen identifiers are often a central component of other electronic or financial crimes. Consequently, our task forces devote considerable time and resources to the issue of identity crime.

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 crime 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 crime, now routinely involves the seizure and analysis of electronic evidence. In fact, so critical was the need for basic training in this regard that the Secret Service joined forces with the International Association of Chiefs of Police and the National Institute for Justice to create the "Best Practices Guide to Searching and Seizing Electronic Evidence" which is designed for the first responder, line officer and detective alike. This guide assists law enforcement officers in recognizing, protecting, seizing and searching electronic devices in accordance with applicable statutes and policies.

We have also worked with these same partners in producing the interactive, computer-based training program known as "*Forward Edge*," which takes the next step in training officers to conduct electronic crime investigations. *Forward Edge* is a CD-ROM that incorporates virtual reality features as it presents three different investigative scenarios to the trainee. It also provides investigative options and technical support to develop the case. Copies of state computer crime laws for each of the fifty states as well as corresponding sample affidavits are also part of the training program and are immediately accessible for instant implementation.

Thus far, we have distributed over 300,000 "Best Practices Guides" to local and federal law enforcement officers and have distributed, free of charge, over 20,000 *Forward Edge* training CDs.

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.

In addition, we have just completed the Identity Crime Video/CD-ROM which contains over 50 investigative and victim assistance resources that local and state law enforcement officers can use when combating identity crime. This CD-ROM also contains a short identity crime video that can be shown to police officers at their roll call meetings which discusses why identity crime is important, what other departments are doing to combat identity crime, and what tools and resources are available to officers. The Identity Crime CD-ROM is an interactive resource guide that was made in collaboration with the U.S. Postal Inspection Service, the Federal Trade Commission and the International Association of Chiefs of Police.

Next week, we will be sending an Identity Crime CD-ROM to every law enforcement agency in the United States. Departments can make as many copies of the CD-ROM as they wish and distribute this resource to their officers to use in identity crime investigations. Over 25,000 Identity Crime CD-ROMs have been produced and are being prepared for distribution.

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.

In a joint effort with the Department of Justice, the U.S. Postal Inspection Service, the Federal Trade Commission and the International Association of Chiefs of Police, we are hosting Identity Crime Training Seminars for law enforcement officers. In the last year and a half we have held seminars for officers in Chicago, Dallas, Las Vegas, Iowa, Washington D.C., and Phoenix. In the coming months we have training seminars scheduled in New York, Seattle and Texas. These training seminars are focused on providing local and state law enforcement officers with tools and resources that they can immediately put into use in their investigations of identity crime. Additionally, officers are provided resources that they can pass on to members of their community who are victims of identity crime.

The Secret Service's Criminal Investigative Division assigned a special agent to the Federal Trade Commission (FTC) as a liaison to support all aspects of their program to encourage the use of the Identity Theft Data Clearinghouse as a law enforcement tool. 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.

It is important to recognize that public education efforts can only go so far in combating the growth of identity crime. Because social security numbers, in conjunction with other personal and financial 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.

The Secret Service recommends that consumers take the following steps to protect themselves from identity crime:

- Maintain a list of all credit card accounts and corresponding phone numbers. Keep this list in a place other than your 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;

- Secure your incoming and outgoing mail;

- Establish passwords where possible with credit card companies or financial institutions that you have accounts with in order to avoid unauthorized change of address, transfer of funds or orders of additional cards;

- 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;

- 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. Complaints can also be filed via their website 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 crime, 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 crime and to assist victims in rectifying damage inflicted on their credit. It is essential that law enforcement recognize that identity crimes 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 crime ring.

The Secret Service has already launched 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. The Secret Service is prepared to assist this committee in protecting and assisting the people of the United States, with respect to the prevention, identification and prosecution of identity 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.