

**Sent:** 17 SEP 2002 17:48:19  
**From:** Brett M. Kavanaugh ( CN=Brett M. Kavanaugh/OU=WHO/O=EOP [ WHO ] )  
**To:** Lisa J. Macecevic ( CN=Lisa J. Macecevic/OU=OMB/O=EOP@EOP [ OMB ] )  
**Cc:** Patrick J. Bumatay ( CN=Patrick J. Bumatay/OU=WHO/O=EOP@EOP [ WHO ] )  
**Subject:** : LRM LJM162 - - TREASURY (Secret Service) Testimony on Preserving the Integrity of SSNs and Preventing Their Misuse by Terrorists  
[P\\_JP08A003\\_WHO.TXT\\_1.doc](#)

##### Begin Original ARMS Header #####

RECORD TYPE: PRESIDENTIAL (NOTES MAIL)

CREATOR: Brett M. Kavanaugh ( CN=Brett M. Kavanaugh/OU=WHO/O=EOP [ WHO ] )

CREATION DATE/TIME: 17-SEP-2002 17:48:19.00

SUBJECT: LRM LJM162 - - TREASURY (Secret Service) Testimony on Preserving the Integrity of SSNs and Preventing Their Misuse by Terrorists

TO: Lisa J. Macecevic ( CN=Lisa J. Macecevic/OU=OMB/O=EOP@EOP [ OMB ] )

READ: UNKNOWN

CC: Patrick J. Bumatay ( CN=Patrick J. Bumatay/OU=WHO/O=EOP@EOP [ WHO ] )

READ: UNKNOWN

##### End Original ARMS Header #####

No objections.

----- Forwarded by Brett M. Kavanaugh/WHO/EOP on  
09/17/2002 05:50 PM -----

Patrick J. Bumatay  
09/17/2002 04:28:29 PM  
Record Type: Record

To: Brett M. Kavanaugh/WHO/EOP@EOP  
cc:  
Subject: LRM LJM162 - - TREASURY (Secret Service) Testimony on Preserving the Integrity of SSNs and Preventing Their Misuse by Terrorists

----- Forwarded by Patrick J. Bumatay/WHO/EOP on  
09/17/2002 04:29 PM -----

From: Lisa J. Macecevic on 09/17/2002 04:06:32 PM  
Record Type: Record

To: See the distribution list at the bottom of this message  
cc: See the distribution list at the bottom of this message  
Subject: LRM LJM162 - - TREASURY (Secret Service) Testimony on Preserving the Integrity of SSNs and Preventing Their Misuse by Terrorists

The attached Secret Service testimony is for a joint hearing Thursday before the House Ways and Means Committee's Subcommittee on Social Security and the House Judiciary Committee's Subcommittee on Immigration, Border Security, and Claims. Please respond with any comments by Noon tomorrow - Wednesday, September 18th. Thank you.  
- ID theft.Bond statement (long).doc

LRM ID: LJM162  
EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
Washington, D.C. 20503-0001

Tuesday, September 17, 2002

LEGISLATIVE REFERRAL MEMORANDUM

TO: Legislative Liaison Officer - See Distribution  
below  
FROM: Richard E. Green (for) Assistant Director for  
Legislative Reference  
OMB CONTACT: Lisa J. Macecevic  
PHONE: (202)395-1092 FAX: (202)395-3109  
SUBJECT: TREASURY (Secret Service) Testimony on Preserving the  
Integrity of SSNs and Preventing Their Misuse by Terrorists

DEADLINE: Noon Wednesday, September 18, 2002  
In accordance with OMB Circular A-19, OMB requests the views of your  
agency on the above subject before advising on its relationship to the  
program of the President. Please advise us if this item will affect  
direct spending or receipts for purposes of the "Pay-As-You-Go" provisions  
of Title XIII of the Omnibus Budget Reconciliation Act of 1990.

COMMENTS: The attached Secret Service testimony is for a joint hearing  
Thursday before the House Ways and Means Committee's Subcommittee on  
Social Security and the House Judiciary Committee's Subcommittee on  
Immigration, Border Security, and Claims. Please respond with any  
comments by Noon tomorrow - Wednesday, September 18th. Thank you.

DISTRIBUTION LIST

AGENCIES:  
110-Social Security Administration - Diane B. Garro - (202) 358-6030  
114-STATE - Nicole Petrosino - (202) 647-1794  
061-JUSTICE - Daniel Bryant - (202) 514-2141  
021-Central Intelligence Agency - b(3)50 USC 3507  
025-COMMERCE - Michael A. Levitt - (202) 482-3151  
029-DEFENSE - Samuel T. Brick Jr. - (703) 697-1305  
030-EDUCATION - Jack Kristy - (202) 401-8313  
049-Federal Trade Commission - Ted Cruz - (202) 326-3683  
052-HEALTH & HUMAN SERVICES - Sondra S. Wallace - (202) 690-7773  
129-VETERANS AFFAIRS - John H. Thompson - (202) 273-6666

EOP:  
Edward H. Chase  
Richard M. Russell  
WHGC LRM  
Eva Kleederman  
Brooke Dickson  
Daniel J. Chenok  
Diana L. Meredith  
Christine M. Burgeson

Matthew Kirk  
Danielle M. Simonetta  
Brian C. Conklin  
Karen N. Blank  
NSC LRM  
OSTP LRM  
OVP LRM  
NEC LRM  
OHS LRM  
Larry R. Matlack  
Jack A. Smalligan  
Kenneth L. Schwartz  
Alan B. Rhinesmith  
Stephen S. McMillin  
Randolph M. Lyon  
Anne R. Stauffer  
James Boden  
Mark J. Schwartz  
Anne Gable  
Thomas Reilly  
Melany Nakagiri-Yeung  
David J. Haun  
Toni S. Hustead  
Kathryn B. Stack  
Siobhan Murphy  
Cameron M. Leuthy  
Glenn R. Schlarman  
Philip J. Perry  
John F. Wood  
Matthew J. Schneider  
Lauren C. Lobrano  
Diana L. Schacht  
Douglas Pitkin  
J. Michael Daniel  
Ellen J. Balis  
Lauren Wittenberg  
Joseph F. Lackey Jr.  
Ingrid M. Schroeder  
Richard E. Green  
Joanne Cianci Hoff  
James J. Jukes  
Karen F. Lee  
Benjamin Powell  
Alexandra Gianinno  
Khushali Parikh Shah  
Joseph G. Pipan  
Lauren E. Bloomquist  
Julie L. Haas  
LRM ID: LJM162      SUBJECT: TREASURY (Secret Service) Testimony on  
Preserving the Integrity of SSNs and Preventing Their Misuse by Terrorists

RESPONSE TO  
LEGISLATIVE REFERRAL  
MEMORANDUM

If your response to this request for views is short (e.g., concur/no

valrm@mail.va.gov @ inet

Message Copied

To:

---

Edward H. Chase/OMB/EOP@EOP  
Richard M. Russell/OSTP/EOP@EOP  
WHGC LRM  
Eva Kleederman/OMB/EOP@EOP  
Brooke Dickson/OMB/EOP@EOP  
Daniel J. Chenok/OMB/EOP@EOP  
Diana L. Meredith/OMB/EOP@EOP  
Christine M. Burgeson/OMB/EOP@EOP  
Matthew Kirk/WHO/EOP@EOP  
Danielle M. Simonetta/OMB/EOP@EOP  
Brian C. Conklin/WHO/EOP@EOP  
Karen N. Blank/OMB/EOP@EOP  
NSC LRM  
OSTP LRM  
OVP LRM  
NEC LRM  
OHS LRM  
Larry R. Matlack/OMB/EOP@EOP  
Jack A. Smalligan/OMB/EOP@EOP  
Kenneth L. Schwartz/OMB/EOP@EOP  
Alan B. Rhinesmith/OMB/EOP@EOP  
Stephen S. McMillin/OMB/EOP@EOP  
Randolph M. Lyon/OMB/EOP@EOP  
Anne R. Stauffer/OMB/EOP@EOP  
James Boden/OMB/EOP@EOP  
Mark J. Schwartz/OMB/EOP@EOP  
Anne Gable/OMB/EOP@EOP  
Thomas Reilly/OMB/EOP@EOP  
Melany Nakagiri-Yeung/OMB/EOP@EOP  
David J. Haun/OMB/EOP@EOP  
Toni S. Hustead/OMB/EOP@EOP  
Kathryn B. Stack/OMB/EOP@EOP  
Siobhan Murphy/OMB/EOP@EOP  
Cameron M. Leuthy/OMB/EOP@EOP  
Glenn R. Schlarman/OMB/EOP@EOP  
Philip J. Perry/OMB/EOP@EOP  
John F. Wood/OMB/EOP@EOP  
Matthew J. Schneider/OMB/EOP@EOP  
Lauren C. Lobrano/OMB/EOP@EOP  
Diana L. Schacht/OPD/EOP@EOP  
Douglas Pitkin/OMB/EOP@EOP  
J. Michael Daniel/OMB/EOP@EOP  
Ellen J. Balis/OMB/EOP@EOP  
Lauren Wittenberg/OMB/EOP@EOP  
Joseph F. Lackey Jr./OMB/EOP@EOP  
Ingrid M. Schroeder/OMB/EOP@EOP  
Richard E. Green/OMB/EOP@EOP  
Joanne Cianci Hoff/OMB/EOP@EOP  
James J. Jukes/OMB/EOP@EOP  
Karen F. Lee/OMB/EOP@EOP  
Benjamin Powell/OMB/EOP@EOP  
Alexandra Gianinno/OMB/EOP@EOP  
Khushali Parikh Shah/OMB/EOP@EOP  
Joseph G. Pipan/OMB/EOP@EOP

Lauren E. Bloomquist/OMB/EOP@EOP  
Julie L. Haas/OMB/EOP@EOP  
Kamela G. White/OMB/EOP@EOP

ATT CREATION TIME/DATE: 0 00:00:00.00  
File attachment <P\_JP08A003\_WHO.TXT\_1>

**Statement of Robert Bond**

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

**Before the Ways and Means Subcommittee on Social Security and the Judiciary  
Subcommittee on Immigration, Border Security and Claims**

**U.S. House of Representatives**

**September 19, 2002**

Mr. Chairman, I would like to thank you for the opportunity to address both subcommittees 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 Bureau of Investigation, the Department of State, 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 given primary authority for the investigation of access device fraud and parallel authority with other law enforcement agencies in identification fraud 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.

The burgeoning use of the Internet and advanced technology coupled with increased investment and expansion has led to fierce competition 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 utterance 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 fraud. 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 the victim's 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 and securities fraud.

## **IMPACT**

Identity theft, unlike many types of crime, 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. 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. With the assistance of the Secret Service, the Identity Theft and Assumption Deterrence Act was passed by Congress in 1998. This 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 battle the growing problem of identity theft. These protections included:

- Expanding the scope of the statute to include as victims those individuals whose identity information was stolen and whose primary loss is credit worthiness and reputation rather than financial loss;
- 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;
- Asset forfeiture provisions were enhanced to allow for the repatriation of funds to victims; and
- The closing of a significant gap 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 federal and state government 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.

The United States Sentencing Guidelines have also been amended since the passage of the 1998 Act to better address identity theft. Section 2B1.1 now provides an offense level of 12 in cases involving the possession of device-making equipment, the production of or trafficking in an unauthorized or counterfeit access device, the unauthorized transfer or use of any means of identification to unlawfully produce or obtain any other means of identification, or the possession of five or more means of identification that were lawfully produced from, or obtained by the use of, another means of identification.

The guidelines also provide a revised minimum loss rule for offenses involving counterfeit or unauthorized access devices. Specifically, a minimum loss amount of \$500 per access device is to 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, the guidelines now include grounds for an upward departure in identity theft cases in which the penalty range, which is largely based on financial loss, does not adequately reflect the seriousness of the offense. Specifically, courts may now consider whether the offense conduct harmed the victim's reputation or credit record, whether the victim suffered substantial inconvenience related to repairing that reputation or credit record, whether the victim was erroneously arrested or denied a job due to the theft, and whether the defendant produced or obtained numerous means of identification such that he or she 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 falls 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.

Given the relative ease with which criminals can steal the identities of others and the allure of enormous profits with few, if any, repercussions, relying on the current sentencing structure to deter the victimization of our citizens, is shortsighted. Recently, the Identity Theft Penalty Enhancement Act of 2002 was introduced in the Senate with

the intent 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, would provide for two (2) years imprisonment for aggravated offenses, in addition to the punishment associated with the related felony; committing the crime of identity theft in relation to specified felony violations, in addition to the punishment provided for such felony; and five (5) years imprisonment for the same the related felonies associated with terrorism. Additionally, the Act prohibits the imposition of probation for those convicted of such violations 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 society and the need to punish those engaging in criminal activity for personal or financial gain. The Secret Service supports these ideas and believes that it is another tool that law enforcement can utilize to the fullest extent in protecting our nation.

### **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 public documents 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 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 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.

It is quite probable 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.

## **TERRORISM**

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.

The Secret Service has also become involved in a collaborative effort with the intention of analyzing the potential for identity theft to be used in conjunction with terrorist activities through our liaison efforts with Operation Green Quest, Operation Direct Action, and FinCEN.

## **COORDINATION**

The Secret Service continues to attack identity theft 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 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 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, 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 or financial crimes. Consequently, our task forces devote considerable time and resources to the issue of identity theft.

### **OUTREACH EFFORTS**

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 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 desperate to restore their reputations and credit worthiness.

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 Federal Trade Commission (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; and
- 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.

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](http://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. 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.