AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 106–1025

IDENTITY THEFT

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

AUGUST 30, 2000

MONTEREY, CA

Serial No. J–106–103

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
73–465 WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512–1800 Fax: (202) 512–2250
Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

STROM THURMOND, South Carolina
CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
JON KYL, Arizona
MIKE DEWINE, Ohio
JOHN ASHCROFT, Missouri
SPENCER ABRAHAM, Michigan
JEFF SESSIONS, Alabama
BOB SMITH, New Hampshire

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
ROBERT G. TORRICELLI, New Jersey
CHARLES E. SCHUMER, New York

MANUS COONEY, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Minority Chief Counsel*

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

JON KYL, Arizona, *Chairman*

ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
MIKE DEWINE, Ohio

DIANNE FEINSTEIN, California
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin

STEPHEN HIGGINS, *Chief Counsel*
NEIL QUINTER, *Minority Chief Counsel and Staff Director*

CONTENTS

STATEMENT OF COMMITTEE MEMBER

	Page
Feinstein, Hon. Dianne, a U.S. Senator from the State of California	1

WITNESSES

Ahern, Michael E., Deputy Chief Inspector, Field Operations West, U.S. Postal Inspection Service, prepared statement	58
Baca, Leroy D., Los Angeles County Sheriff, prepared statement and attachments	4
Frank, Mari, identity theft victim, prepared statement and attachments	29
Kassin, Selene, identity theft victim, prepared statement	26
Klurfeld, Jeffrey A., Director of Western Regional Office, Federal Trade Commission, prepared statement and attachments	43
Vezeris, Jane, Deputy Inspector General, Social Security Administration, prepared statement	55

IDENTITY THEFT

WEDNESDAY, AUGUST 30, 2000

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY, TERRORISM,
AND GOVERNMENT INFORMATION,
COMMITTEE ON THE JUDICIARY,
Monterey Park, CA.

The subcommittee met, pursuant to notice, at 9:06 a.m., at the Sherman Block Sheriff's Headquarters Bureau, 4700 Ramona Boulevard, Monterey Park, CA, the Hon. Dianne Feinstein presiding.

OPENING STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Senator FEINSTEIN. I'd like to welcome all of you here, this morning, to the field hearing of the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information. I'm the ranking member of that committee.

The topic of this hearing is local and Federal response to identity theft.

In particular, I want to thank Sheriff Baca for joining me in hosting this hearing at the Los Angeles County Sheriff Headquarters, and Sheriff Baca will begin our testimony in just a moment, with an announcement that he has to make.

I'd also like to thank the impressive roster of witnesses, Jeffrey Klurfeld, who's director of the Western Regional Office of the FTC, Jane Vezeris, the Deputy Inspector General of the Social Security Administration, Michael Ahern, the Deputy Chief Inspector of Western Field Operations of the U.S. Postal Inspection Services, and also, two identity theft victims, Selene Kassin, and Mari Frank.

Identity theft is perhaps the signature crime of this new economy. Modern technology has made vast amounts of personal information obtainable at the click of a keyboard, or at the acquisition of a public document, leaving our personal information vulnerable to interception and misuse.

Now, what is identity theft? Identity theft occurs when one person assumes another's identity, and fraudulently uses their personal financial data, to acquire credit or products, again fraudulently, and to hide from their own true identity.

The documents can be a Social Security number, a birth date, a driver's license number, or other identifying information that enables them to obtain your credit cards, and then go out and use those credit cards.

Identity thieves can get personal information in a myriad of ways, stealing wallets and purses, containing identification cards, using personal information found on the Internet, stealing mail (including pre-approved credit offers and credit statements), fraudulently obtaining credit reports, or getting personal records at work.

An identity is stolen today every 60 seconds. As many as seven hundred thousand incidents of identity theft will occur this year.

The heaviest area in the United States for identity theft is right here, Los Angeles, and that's why we're holding this hearing here today, and to bring this information back to the Judiciary Committee.

The hearing is being recorded, and all of this will be included in the official transcripts of the hearings on this subject.

From 1997 to 1999, there was a 380-percent increase in the reporting of Social Security number misuse.

In a survey of a thousand Americans, by Impulse Research of Los Angeles, 42 percent of the respondents reported a member of their household had their personal identity or credit card information stolen.

Identity theft causes up to $3 billion in losses annually, from credit card fraud, alone.

We're going to hear from two victims today, who will describe the havoc to their lives caused by identity theft.

Now, identity theft, unlike other crimes, is an ongoing crime that can last for years.

The typical victim learns about the identity theft 14 months after it's occurred, sustains $18,000 in fraudulent charges, and spends a 175 hours over 2 years, restoring their clean credit and good name.

I'd like to tell you just about the one case of one person who is not testifying here today, but I happened to have met her before.

She was a victim of identity theft. Her name is Lynn Klinenberg. Her late husband, James Klinenberg, Dr. James Klinenberg was the chief of medicine and vice-president of professional services at Cedars-Sinai in Los Angeles.

If you're here, Lynn, would you stand, so people might be able to see you? Thank you, very much.

Her husband's Social Security number and mother's maiden name were obtained through a death certificate. Her husband died suddenly in December. His obituary was in the *Los Angeles Times*, as well as other places.

The thief went and got the death certificate, which looks like this, which is a public record. On that death certificate, was her husband's Social Security number and her mother's maiden name.

Mrs. Klinenberg didn't fill out that death certificate, others did. But this information was then used to access Mrs. Klinenberg's bank account, and receive credit cards in her late husband's name.

Shortly after her husband's death, these criminals attempted to wire transfer thousands of dollars from her family's bank account to banks in New York and Pittsburgh.

Her husband's name appeared on a credit card in Denmark and was used to order $25,000 in diamonds and Rolex watches, fraudulently.

Now, that's one example. Another example that we will hear about, are people using this information to go out and stalk a victim by locating their home address and finding out where they are.

I have also found that the Social Security number has become a prime source for obtaining information, to go ahead with a crime of identity theft.

So, our goal today to see how the Federal Government might be able to help, to put the clamps on identity theft, to make it harder to traffic in personally identifiable information, how law enforcement can increase the prosecution and investigation of identity theft, and how individuals can take preventive steps to protect themselves from identity thieves.

First, we can cut down on the widespread trafficking, and use of Social Security numbers, and I have a bill to do just that.

Social Security numbers have become the prime tool, used by identity thieves, to capture victims' personal information, and to set up fraudulent credit card accounts.

Today, on the Internet, an identity thief can buy another person's social security number for as little as twenty-five dollars ($25), no questions asked. This is simply wrong.

I have introduced the Social Security Number Protection Act, which is endorsed by the Clinton-Gore administration.

This bill would prohibit the sale of a person's Social Security number, without their consent, except for a narrow number of circumstances, such as law enforcement, national security, or public health purposes.

I've also introduced the Identity Theft Prevention Act. This bill, which is endorsed by the Federal Trade Commission and my Senate colleagues, John Kyl and Charles Grassley, offer a number of concrete practical measures, to cut down criminal access to personal information, and assist victims.

For example, identity thieves often intercept bank statement or credit card statements, and then redirect the account to another address.

This bill would require credit issuers to notify the original card holders of their original address of any address change request.

Therefore, cardholders would know right away, any time a thief is trying to shift the address of their account.

In addition, the bill would develop standardized forms for victims to report identity theft to bank credit bureaus and retail stores.

Right now, identity theft victims typically have to fill out a new fraud report for each store with a fraudulent charge.

Creating a standardized form could save many victims literally hundreds of hours of time of filling out what are redundant reports.

Sheriff Baca will head off the hearing today, with testimony about a new project, an innovative and ground-breaking Los Angeles County Identity Theft Strike Force.

I will leave it to him to describe the program, but I think he has developed a model that's worth emulating around the country, and when Congress convenes, I'm giving serious consideration to introducing legislation, authorizing $15 million to create identity theft strike force pilot projects, around the country.

So, I look forward to this hearing today, and I'd like to introduce the first panel.

Let me begin with Sheriff Baca. He is the thirtieth Sheriff of Los Angeles County.

He commands the largest Sheriff's Department in the world, supervising more than thirteen thousand sworn civilian personnel.

He's had an extraordinarily successful career in the Los Angeles Sheriff's Department, where he started as a Deputy Sheriff Trainee in 1965, rising to Captain in 1981 and Chief in 1992. He was sworn in as Sheriff in 1998.

His record is one of effective innovation. As a Chief of the Court Services Division, he directed the strategy that led to the merger of the Sheriff's Department and the Marshal's Department.

The merger saved the taxpayers of Los Angeles $14 million a year.

With the Sheriff Department's identity theft team, Sheriff Baca is again showing leadership. I look forward to his testimony in this area.

And the remaining two speakers of the first panel are identity theft victims, Mari Frank and Selene Kassin.

Let me just quickly tell you a little bit about them. Selene will describe in her testimony her personal encounter with identity theft.

She had her identity stolen by a thief who had just her Social Security number, who used her identity to obtain numerous credit cards.

Selene only found someone was living as her from a letter from a credit card company, asking if she tried to open up a new account.

And the second person is Mari Frank. Mari is an Orange County attorney, who has been a victim of identity theft on two separate occasions.

Since her first traumatic encounter in 1996, she's devoted much of her time and energy, teaching others how to protect themselves.

She is a co-author of the "Identity Theft Survival Kit," and is an Orange County, California Sheriff Reserve, for the High Tech Crime Unit.

So, let's begin right now with the first panel, and I'd like to present Sheriff Baca of Los Angeles County.

PANEL CONSISTING OF LEROY D. BACA, LOS ANGELES COUNTY SHERIFF, LOS ANGELES, CA, MARI FRANK, IDENTITY THEFT VICTIM; AND SELENE KASSIN, IDENTITY THEFT VICTIM

STATEMENT OF LEROY D. BACA

Sheriff BACA. Thank you very much Senator, and good morning. Welcome to the Los Angeles County Sheriff's Department Headquarters Unit, Sherman Block Administration Building.

I would like to open my remarks by piggybacking on the things that you've described earlier, Senator, and I appreciate the thoroughness under which you have approached this problem.

Prior to your testimony here, in opening up for our testimony, the Los Angeles County Sheriff's Department was well aware that there was an identity theft problem that needed to be addressed in a more concerted fashion.

So, in order to do this, approximately a year and a half ago, we researched this issue in depth, and implemented the best ideas from victim advocates, the public and private sector.

We trained our department as to the needs of the victims, and established a cutting-edge reporting procedure, that would centralize the tracking.

As you identified earlier, there's apparently a reporting deficiency, in terms of how we can get victims who are multiple targets from various suspects.

How can we get them to report things in a fashion that doesn't cause the victim any more agony than they already have by virtue of being a victim?

So, what we did, is we put together a guide for law enforcement officers to follow, when they're dealing with victims of this type of crime.

Furthermore, we put together a——

Senator FEINSTEIN. I'd like to ask that that be made part of the record.

Sheriff BACA. Yes, and I will present you with a complete packet, that will include this information.

Senator FEINSTEIN. Thank you.

Sheriff BACA. Second, the idea of how the department would respond to an identity theft report, what are the actual things that we will do, in order to ensure that the victim's circumstances are fully investigated?

We developed an informational brochure for victims of identity theft, as well.

Now, in producing this information, the logical outgrowth is that the public now is more informed, as to what they can do, and what will law enforcement do for them.

Consequently, we have seen a dramatic increase in this type of offense being reported to us.

For example, we have encountered, when we started this program, two hundred and seventy-three victims.

This was in 1999, and we started the program around July. So, at about a 6-month period of time.

Just opening up the first 4 months of this year, the year 2000, we have already 645 cases reported to us, which is a net increase of approximately 136 percent.

Recognizing these numbers and these statistics are, are the early reporting of what our experiences have been, it still clearly indicates that this is a problem that will only grow.

The encouraging part of what is going on with your inquiry to local law enforcement about the problem, is that the State of California recognizes that there is a need for more things to be done, as well.

For example, when we talked about training and public awareness, and then of course prevention, it's key to identify a central tracking mechanism and that, therein the Los Angeles County Sheriff's Department created the unit that is responsible for identity theft investigations.

There, there, there, it's a team approach. There are four investigators and a supervising lieutenant, that are responsible for this highly specialized task force.

Undoubtedly, procedures had to be established, and I have copies of that data for you.

Not only do we have to have internal departmental procedures, but the State of California's peace officer and standards and training offices now have a 40-hour course to train law enforcement officers on how to do these type of investigations.

The Sheriff's Department was privileged to participate in the, President Clinton's National Summit on Identity Theft, in Washington, DC, and at this point, the Federal Trade Commission has been working closely with the Los Angeles County Sheriff's Department, in a regional identity theft effort.

Cases that are reported to us, undoubtedly can affect the Federal Trade Commission, as well.

We have a new office facility in the city of Bellflower, that is capable of receiving additional investigative resources from the Federal Government.

Moreover Senator, excuse me, moreover Assembly Member and Speaker, Robert Hertzberg, has authored an Assembly Bill 1949, to fund a multiple agency task force team in the State of California.

I support wholeheartedly your bill, Senate Bill 2328, which is the Identity Theft Prevention Act, as well as your Senate Bill 2699, the Social Security Number Protection Act.

Your effort in ensuring that these privileged and confidential pieces of information are not available in such a open fashion, as through the Internet, is a step in the right direction, to guarantee that victims can be protected properly, sought out victims, that is by very, very highly skilled offenders who will prey on information, and then from the information, prey on the victims themselves.

I think that what I believe is necessary for us to go forward in Southern California is that we need to combine more Federal, State and local resources together.

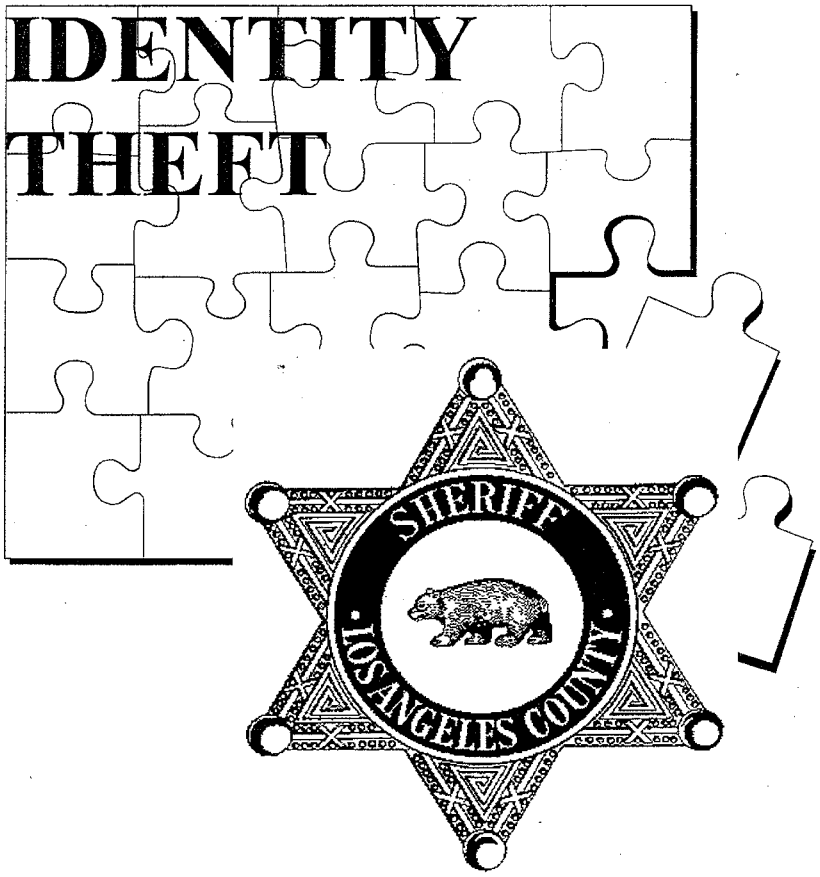
You will hear testimony from representatives of other agencies.

As I close, I would like to recommend to you that a full-time investigator from the following federal agencies be assigned to the Sheriff's Department Task Force: a member of the U.S. Postal Inspection Service; a member of the U.S. Secret Service; a member of the Office of Inspector General for Social Security and a member of the U.S. Treasury Department, Office of Tax Enforcement.

I will also be recommending to the Governor and State officials that the California Department of Health Services, Offices of Vital Records, be assigned to this task force, and a member of the California Department of Justice.

Thank you, very much.

[The prepared statement and attachments of Mr. Baca follow:]



PIECING IT TOGETHER

Los Angeles County Sheriff's Department 08-30-00

County of Los Angeles
Sheriff's Department Headquarters
4700 Ramona Boulevard
Monterey Park, California 91754-2169

LEROY D. BACA, SHERIFF

August 30, 2000

The Honorable Dianne Feinstein
United States Senate
11111 Santa Monica Boulevard
Santa Monica, California 90025

Dear Senator Feinstein:

Identity theft and its attendant fraud and larceny has become a very serious situation throughout the country which ruins people's lives and challenges law enforcement resources. Each identity theft case is not just one case but many and affects several agencies with enforcement and regulatory responsibilities. Frequently these financial predators commit multiple crimes that span city, county, state and even international boundaries. As a result, both victims and police agencies are subject to complex and confusing processes for investigation and prosecution.

The Los Angeles County Sheriff's Department began to address identity theft as a unique criminal activity in July 1999. Our research indicated a 42% increase in these cases from 1998 to 1999, and we project over 1,800 cases in our jurisdiction alone for the year 2000 (Attachment #1). Nationally, it is estimated that 1 in 4 Americans will be victimized by this crime sometime in their lifetime.

Sheriff's Department personnel developed a victim outreach protocol for field deputies to assist victims in reporting the circumstances to law enforcement and financial institutions. Information pamphlets were created to provide process information for both police officers and victims. (Attachments #2,3,4). A public awareness and prevention campaign was implemented and key liaisons with the private sector such as computer manufacturers, telecommunications providers and other trade groups were established.

In April the Sheriff's Department increased staffing dedicated to identity theft investigations to four deputies supervised by a lieutenant. They developed the first training program in the country for identity theft investigations with the California Commission on Peace Officers Standards and Training (Attachment #5). The concept of regional identity theft task forces

was developed and presented to California State Assembly Speaker Robert Hertzberg. This effort resulted in California Assembly Bill 1949 to provide funding to implement Regional Identity Theft Task Forces in California (Attachment #6).

The Department secured office space in June 2000 with the assistance of the City of Bellflower. This facility has the capacity to provide a modern, high-tech working environment for personnel for the various local, state and federal law enforcement and regulatory agencies that will facilitate a collaborative effort.

Currently, the Sheriff's Department Identity Theft Unit vigorously investigates identity theft and related fraud issues that have a nexus to Los Angeles County. With the team concept utilizing the resources of other governmental agencies, we have been able to target identity thieves, receivers of stolen property, and those misusing the Postal Service and Social Security, driver's license and other personal information.

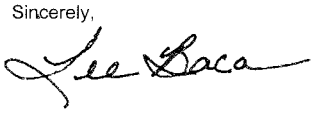
I am well aware of the limited nature of resources, but the growing magnitude of this matter demands dedicated full-time investigators to combat the problem. We have devoted such resources but we are limited in our ability to navigate the myriad federal and out of state investigative requirements in a timely and effective manner. Many of these cases move at the speed of E-Commerce. Although we receive assistance as needed on a case-by-case basis from various law enforcement and regulatory agencies, what is needed is a full-time commitment from the federal and state agencies who themselves have the resources to investigate financial crimes on a regional or national level.

I am therefore asking you to convince the heads of the United States Attorney's Office, the United States Postal Inspection Service, the United States Secret Service, the Office of the Inspector General for Social Security, the Internal Revenue Service, the California Department of Health Services Office of Vital Records, the California Department of Justice and the California Highway Patrol to dedicate a full-time representative to our strike force.

I appreciate and support your efforts to address this escalating problem which victimizes our citizens nationwide. Senate Bills 2328 (The Identity Theft Prevention Act) and 2699 (The Social Security Number Protection Act) you have introduced will provide valuable tools in the deterrence and investigation of identity theft.

I believe that by working together in a coordinated local, state, and federal effort we will have a significant impact on the economic terrorists that prey upon our financial system and citizens.

Sincerely,



LEROY D. BACA
SHERIFF

Attachment #1
Workload and Statistics

	2nd Trimester (05/01/1999-08/22/1999) 1999	**2nd Trimester (05/01/2000-08/22/2000) 1999**	% Increase
Cases Received by Forgery/Fraud Detail	273	645	136%
Cases Assigned	87	398	357%
Felony Filings	7	28	300%
Search Warrants Executed	0	14	1400%
Active Investigations	18	317	1661%

- Cases are solvable but are extremely labor intensive (**avg low end 60 man hrs** to 1000's of hrs). One search warrant to a location with 6 investigators/deputies X 6 hrs= 36 hours alone (search warrant briefing, entry, evidence collection, cataloging, booking of suspect, property, and evidence). Many times we wait days, weeks, or months for bank/credit documents.

Attachment #2
Field Operations Directive

COUNTY OF LOS ANGELES

SHERIFF'S DEPARTMENT

OFFICE CORRESPONDENCE

DATE March 13, 2000
FILE NO.

FROM: WILLIAM T. SAMS, CHIEF
CURTIS L. SPEARS, CHIEF
KENNETH L. BAYLESS, CHIEF
FIELD OPERATIONS REGIONS

HELENA ASHBY, CHIEF
DETECTIVE DIVISION

TO: ALL UNIT COMMANDERS
FIELD OPERATIONS REGIONS
DETECTIVE DIVISION

SUBJECT: FIELD OPERATIONS DIRECTIVE 00-01

IDENTITY THEFT PROCEDURES

PURPOSE

The purpose of this Directive is to provide additional procedures for Sheriff's Station personnel when investigating and processing identity theft crime reports.

BACKGROUND

Identity theft is a growing crime affecting many citizens around the country. Since credit cards are more difficult to alter and manufacture, criminals have taken to stealing the personal information of others to obtain credit, goods, and services. As a result, Penal Code Section 530.5 was enacted on January 1, 1998 (1997 Chapter 768). Prior to enactment of this legislation, only the creditor was the victim. Now the person whose information was used is also a victim of credit fraud.

Penal Code Section 530.5 provides that every person who willfully obtains personal identifying information of another person without the authorization of that person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, or medical information in the name of the other person without the consent of that person, is guilty of a public offense.

Personal identifying information, as used in this section means the name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, or credit card

number of an individual person.

Currently, some identity theft cases are investigated by Sheriff's station detectives, while others are assigned to the Forgery/Fraud Detail. Many of these cases are reported as grand thefts or under other statistical codes. As a result, it is difficult to assess the true number of cases reported to the Department.

DEPUTY RESPONSIBILITIES

When presented with the crime of identity theft, deputies shall take an incident report listing "Identity Theft, 530.5 PC" on the Classification Line, from victims that reside within the Department's jurisdiction. While the Department may investigate the 530.5 PC violation, this does not necessarily mean that it will handle the entire case. If the suspect(s) are committing other crimes in the name of the victim, in other jurisdictions, those respective law enforcement agencies are responsible for writing an incident report and investigating the separate offenses.

For example, a victim resides in Lennox Station's area and discovers that someone has used their personal identifying information to apply for a credit card, and the card was delivered to an address in Beverly Hills. The card is subsequently used to make purchases in Beverly Hills.

In this scenario, the Sheriff's Department (Lennox Station) would take a 530.5 PC report. The Beverly Hills Police Department would be responsible for the illegal use of the credit card in its jurisdiction and take a report for violation of Penal Code Section 484g (Using Access Card Obtained Without Consent of Cardholder or Issuer). Conversely, if the victim resided in Beverly Hills and their personal identifying information was used illegally to obtain and use a credit card in Lennox Station's area, the Beverly Hills Police Department would take a 530.5 PC report and Lennox Station, the 484g PC report.

A 530.5 PC report, should contain at least one incident of fraudulent activity (e.g., Visa Card account number 1234 5678 9012 3456 applied for in the victim's name and the victim said they never applied for such card).

Deputies shall advise the victim to call the three credit bureaus (Transunion [800] 680-7289, Equifax [800] 525-6285, and Experian [888] 397-3742) and have a "Fraud Alert" placed on their account. This alert usually lasts for 90 days, unless accompanied by a copy of a police report. The incident report shall

reference this notification.

Deputies shall also tell the victim they are entitled to a free copy of their credit report from all three bureaus if they are a victim of fraud. They should examine each report as some activity may show on one report and not the other. Different credit bureaus occasionally receive reports from different sources.

If the victim has made reports to other agencies (e.g., United States Secret Service, United States Postal Service, California Department of Motor Vehicles, other law enforcement agencies, etc.), those reports shall be referenced in the Department Incident (first) Report.

Deputies shall issue the victim a copy of the Department's *Victim's Guide to Identity Theft* and reference it in the first report. Copies of the guide can be obtained from the Sheriff's Data Network, in Microsoft Outlook, at the following address:

Public Folders/All Public Folders/Field Operations Info./Forgery Fraud Information

WATCH SERGEANT/FIELD SUPERVISOR RESPONSIBILITIES

All approved incident reports, which contain the elements of identity theft and are assignable to station detectives per the Case Assignment and Reporting Manual, shall have a Special Request Distribution (SRD) to Commercial Crimes Bureau, Forgery/Fraud Detail. All other forgery/fraud types of crimes shall be assigned and distributed as delineated in the Case Assignment and Reporting Manual.

STATION DETECTIVE BUREAU RESPONSIBILITIES

If an approved incident report is assigned to station detectives (e.g., a suspicious circumstances report) and later found to contain the elements of identity theft, the station detective bureau shall ensure the Los Angeles Regional Crime Information System (LARCIS) is updated to reflect this. Additionally, if the case remains assigned to station detectives, the Investigating Officer (IO) shall SRD a copy of the report to the Forgery/Fraud Detail.

If, after the preliminary investigation by the IO, a case appears to contain the elements of crimes assignable to the Forgery/Fraud Detail, the IO may refer it there for handle.

Questions may be directed to the Forgery/Fraud Detail at (562) 946-7217 or Field Operations Support Services at (323) 526-5765.

Original Signed

WILLIAM T. SAMS, CHIEF
FIELD OPERATIONS REGION I

Original Signed

CURTIS L. SPEARS, CHIEF
FIELD OPERATIONS REGION II

Original Signed

KENNETH L. BAYLESS, CHIEF
FIELD OPERATIONS REGION III

Original Signed

HELENA ASHBY, CHIEF
DETECTIVE DIVISION

WTS:CLS:KLB:HA:RDE:DAW:DS:daw/ds

Attachment #3
Victim's Guide to Identity Theft

Resources

Credit Reporting Bureaus:

Equifax: Roosevelt Blvd, St. Petersburg FL 33716-2202
- ✓ Report Fraud: Call (800) 290-8749 and write to address above.
- ✓ Order a credit report: (800) 685-1111.
- ✓ Opt out of pre-approve offers of credit; (888) 5OPTOUT or (888) 567-8688.

Experian (formerly TRW): PO box 1017, Allen, TX 75013
- ✓ Report Fraud: Call (800) 301-7195 or (888) 397-3742 and write to address above.
- ✓ Order a credit report: (888) 397-3742.
- ✓ Opt out of pre-approved offers of credit and marketing lists: (888) 567-8688

Trans Union: PO Box 390, Springfield, PA 19064
- ✓ Report Fraud: (800) 680-7289
- ✓ Consumer Relations: (800) 916-8800 and write to Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92834-6790
- ✓ Order Credit Report: (888) 680-7293

Remember, if you have been the victim of credit fraud (15 USC §1681j(b)) or are denied credit (15 USC §1681j(c)(3)) you are entitled to a free credit report. If you are a victim of fraud, be sure to ask the credit bureaus for free copies. They will often provide them.

Social Security Administration
- ✓ Report Fraud: (800) 269-0271
- ✓ Order your Earnings and Benefits Statement: (800) 772-1213

To remove your name from mail and phone lists:
- ✓ Direct Marketing Association
  - Mail Preference Service, PO Box 9008, Farmingdale, NY 11735
  - Telephone Preference Service, PO Box 9014, Farmingdale, NY 11735

To report fraudulent use of your checks:
- ✓ CheckRite: (800) 766-2748
- ✓ CrossCheck: (800)843-0760
- ✓ Chexsystems: (800) 428-9623
- ✓ Equifax: (800) 437-5120
- ✓ International Check Svcs: (800) 526-5380
- ✓ SCAN: (800) 262-7771
- ✓ Telecheck: (800) 710-9898

Other Useful Resources:
- ✓ Federal Government Information Center: Call (800) 688-9889 for help in obtaining government agency phone numbers.
- ✓ Federal Trade Commission (877) FTC-HELP for help in any type of consumer complaint (105 PL 318,112 Stat.3007 Section 5)(specifically identity theft and referrals to local law enforcement). FTC Consumer's Page www.consumer.gov/idtheft

Laws

Federal

Identity Theft and Assumption Deterrence Act Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998)
www.ftc.gov/os/statutes

Fair Credit Reporting Act (FCRA) 15 U.S.C. § 1681 *et seq.*
www.ftc.gov/os/statutes

State of California

Unauthorized Use of Personal Identifying Information 530.5 PC

Useful Internet Locations

Federal Trade Commission www.ftc.gov

California Department of Consumer Affairs www.dca.ca.gov

Los Angeles County Department of Consumer Affairs http://consumer-affairs.co.la.ca.us

Type "Identity Theft" into your web browser

This guide was adapted with permission from the Privacy Rights Clearinghouse, San Diego, California.

SOMEONE IS USING YOUR IDENTIFYING INFORMATION (NAME, DATE OF BIRTH, SOCIAL SECURITY NUMBER, ETC.) TO OBTAIN GOODS, SERVICES, CREDIT, AND/OR OPEN FRAUDULENT BANK ACCOUNTS.

YOU ARE A VICTIM OF...

Identity Theft

What to Do if It Happens to You

Los Angeles County Sheriff

FORGERY/FRAUD DETAIL

Forgery/Fraud Detail
Commercial Crimes Bureau
11515 South Colima Road M104
Whittier, California 90604
(562) 946-7212

This guide provides victims of identity theft with the major resources to contact. Victims themselves have the ability to assist greatly with resolving their case. It is important to act quickly and assertively to minimize the damage.

Rev. 08-31-99 jmd

*In dealing with the authorities and financial institutions, **keep a log** of all conversations, including dates, times, names, and phone numbers. Note the time spent and any expenses incurred. Confirm conversations in writing. Send correspondence by certified mail (return receipt requested). Keep copies of all letters and documents.*

Once you discover you are a victim of identity theft you should notify the following:

1. Credit bureaus. Immediately call the fraud units of the three credit reporting companies– Experian, Equifax, and Trans Union. Report the theft of your credit cards or numbers. The phone numbers are provided at the end of this brochure. Ask that your account be flagged. Also, add a victim's statement to your report, up to 100 words. ("My ID has been used to apply for credit fraudulently. Contact me at (*your telephone number*) to verify all applications.") Be sure to ask how long the fraud alert is posted on your account, and how you can extend it if necessary. *Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter. Ask the credit bureaus in writing to provide you with a free copy every few months so you can monitor your credit report.*

Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Ask the credit bureaus to remove the inquiries that have been generated due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months in order to alert them to the disputed and erroneous information (two years for employers).

2. Creditors. Contact all creditors immediately with whom your name has been used fraudulently-- by phone **and** in writing. Get replacement cards with new account numbers for your own accounts that have been used fraudulently. Ask that old accounts be processes as "account closed at consumer's request." (This is better than "card lost or stolen" when this statement is reported to credit bureaus, it can be interpreted as blaming you for the loss.) Carefully monitor your mail and credit card bills for evidence of new fraudulent activity. Report it immediately to credit grantors.

Creditors requirement to report fraud. You may be asked by banks and credit grantors to fill out and notarize fraud affidavits, which could become costly. The law does not require that a notarized affidavit be provided to creditors. A written statement and supporting documentation should be enough (unless the creditor offers to pay for the notary).

3. Law Enforcement. Report the crime to the law enforcement agency with jurisdiction in your case. Give them as much documented evidence as possible. Get a copy of your police report. Keep the report number of your police report handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report to verify the crime. Some police departments have been known to resist writing reports on such crimes. Prior to January 1st, 1998, the creditors (credit card companies, banks, etc.) were the only "legal" victims of Credit Fraud/Identity Theft. California Penal Code Section 530.5 went into effect on January 1st, 1998, thus giving legal standing to individual victims. Some police departments have not yet received training in the new laws of Identity Theft. Be persistent!

4. Stolen Checks. If you have had checks stolen or bank accounts set up fraudulently, report it to the check verification companies. Put stop payments on any outstanding checks that you are unsure of. Cancel your checking and savings accounts and obtain new account numbers. Give the bank a secret password for your account (not your mother's maiden name).

5. ATM Cards. If your ATM card has been stolen or is compromised, get a new card, account number, and password. Do not use your old password. When creating a password, don't use common numbers like the last four digits of your social security number or your birth date.

6. Fraudulent change of address. Notify the local Postal Inspector if you suspect an identity thief has filed a change of address with the post office or has used the mail to commit credit or bank fraud. Find out where the fraudulent credit cards were sent. Notify the local Postmaster for the address to forward all mail in your name to your own address. You may also need to talk to the mail carrier.

7. Social Security number misuse. Call the Social Security Administration to report fraudulent use of your social security number. As a last resort, you might want to change the number. The SSA will only change it if you fit their fraud victim criteria. Also order a copy of your Earnings and Benefits Statement and check it for accuracy.

8. Passports. If you have a passport, notify the passport office in writing to be on the lookout for anyone ordering a new passport fraudulently.

9. Phone Service. If your long distance calling card has been stolen or you discover fraudulent charges on your bill, cancel the account and open a new one. Provide a password which must be used anytime the account is changed.

10. Driver License number misuse. You may need to change your driver's license number if someone is using yours as identification on bad checks. Call the state office of the Department of Motor Vehicles (DMV) to see if another license was issued in your name. Put a fraud alert on your license. Go to your local DMV to request a new number. Also, fill out the DMV's complaint form to begin the fraud investigation process. Send supporting documents with the complaint form to the nearest DMV investigation office.

11. False civil and criminal judgements. Sometimes victims of identity theft are wrongfully accused of crimes committed by the imposter. If a civil judgement has been entered in your name for actions taken by your imposter, contact the court where the judgement was entered and report that you are a victim of identity theft. If you are wrongfully prosecuted for criminal charges, contact the state Department of Justice and the FBI. Ask how to clear your name.

Attachment #4
Field Deputy's Guide to Identity Theft

incur any charge, forfeiture, or penalty, or whereby any benefit might accrue to the party personating, or to any other person.

PC§ 148.9 (a) *Giving False Identification*
Any person who falsely represents or identifies himself or herself as another person or as a fictitious person to any peace officer listed in Section 830.1 or 830.2, upon a lawful detention or arrest of the person, either to evade the process of the court, or to evade the proper identification of the person by the investigating officer is guilty of a misdemeanor.

In almost any instance when a suspect commits the crime of False Personation of Another to a peace officer, 529.3PC, he also commits a violation of 148.9PC. However, one can easily commit a violation of 148.9 without violating 529.3.

The key distinction between 148.9 and 529.3 is 529.3 requires *an additional act beyond falsely representing yourself as another and the act has to be done with the required intent*. If an individual gives false identification to a peace officer and the information pertains to a real person (living or dead), and the person commits an additional act beyond the impersonation, with the intent to either: 1) subject the impersonated individual to civil or criminal liability, financial obligation, or charge, forfeiture or penalty, or 2) obtain a benefit for himself, he is guilty of 529.3PC. Providing a false name and DOB will not be enough. Additionally, the person being impersonated has to be a *real person.*

Providing a false driver's license doesn't add anything to the equation. However, signing a written promise to appear would be an additional act, which if done by the person falsely personated, might subject the person to prosecution or to pay a sum of money.

The main difference between 529.3PC and 530.5PC is that in a 530.5 the suspect uses the victims information to *obtain credit, goods, or information to obtain, or attempt to obtain credit, goods, or services*. In a 529.3, the suspect impersonates the victim so the victim might become liable to any suit or prosecution, or to pay any sum of money, or incur any charge, forfeiture, or penalty, or whereby any benefit might accrue to the party personating, or to any other person.

USEFUL PENAL CODES SECTIONS:

(Refer to P. C. for exact wording and meaning of sections)
368(d) Theft or embezzlement from elder/dependant adult, by caretaker
470 Forgery of Check Endorsements, Fictitious Checks, Documents, Food Stamps, Lottery Tickets, By Altering Checks. Uttering, (i.e.; merely passing item with intent to Defraud is sufficient for arrest)
470a Forgery/Counterfeiting of CDL or ID card to facilitate forgery
470b Display/Possess forged CDL to facilitate forgery
475 Possessing, receiving or uttering forged notes (check), etc.
476 Make, pass, utter or publish with intent to defraud any other person, or who, with the like intent, attempts to pass, utter, or publish, or who has in his or her possession, with like intent to utter, pass, or publish any fictitious or altered bill, note, or check
484(a) Theft defined
484d Definition of access card terms
484e(a) Selling , transferring, conveying access card
484e(b) Acquisition of 4 or more access cards
484e(c) Acquisition of access card with intent to use
484e(d) Acquires or retains possession of access card Information without permission
484f(a) Forgery of Access card. Make, alter, emboss utter counterfeit card
484f(b) Forge name of another to access card or sales slip
484g Fraudulent use of access card or account info.
484i Access card, counterfeiting
484j Publishing access card information with intent to defraud
485 Misappropriate lost property. Petty/Grand Theft
502.7 Obtain phone service by fraud
529 False Personation of another
530.5 Identity theft.
532(a) Theft by false pretenses
532a(1) False financial statement

Additional phone numbers to contact:
Social Security Administration Fraud Hotline (800)269-0271
Federal Trade Commission Hotline (877)ID-THEFT
Federal Government Information Center (To help in obtaining government agency phone numbers):
(800)688-9889

A Field Deputy's Guide for Identity Theft, 530.5PC

COMMERCIAL CRIMES BUREAU
Forgery/Fraud Detail
11515 South Colima Road, Room M-104
Whittier, California 90604
(562) 946-7217 - FAX (562) 944-8741

This Field Deputy Guide provides information and procedures for Deputy personnel when investigating the crime of Identity Theft, 530.5PC.

For additional information on Identity Theft Procedures, see Field Operations Directive 00-01. It was authored to establish reporting procedures for the criminal offense of Identity Theft. Additionally, the Directive can be retrieved in Microsoft Outlook at the following address:
Public Folders/All Public Folders/Field Operations Info./Field Operations Directives /2000

Questions may be directed to the Forgery/Fraud Detail at (562)946-7217.

TO REPORT IN-CUSTODIES AFTER HOURS AND ON WEEKENDS, CALL THE SHERIFF'S HEADQUARTERS BUREAU AT: (323) 526-5541

Authored: May, 2000

Identity theft is a growing crime affecting many citizens around the country. It continues to be a major problem for banks and access card companies. Since credit cards are more difficult to alter and manufacture, criminals have taken to stealing the personal information of others to obtain credit, goods, and services. As a result, Penal Code Section 530.5 was enacted on January 1, 1998 (1997 Chapter 768). Prior to enactment of this legislation, only the creditor was the victim. Now the person whose information was used is also a victim of credit fraud.

The victim's information is stolen and misused, in much the same way as a burglary victim's property is stolen from his home. This is an information crime: what is taken is personal identifying information and what is harmed is the victim's financial reputation. The jurisdiction for the crime of Identity Theft, *is where the impersonated victim resides*. Penal Code Section 530.5 provides that every person who willfully obtains personal identifying information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, or medical information in the name of the other person without the consent of that person, is guilty of a public offense.

Personal Identifying information, as used in this section means the name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, saving account number, or credit card number of an individual person.

DEPUTY RESPONSIBILITIES

When presented with the crime of identity theft, for victims who reside within the Department's jurisdiction, deputies shall take an incident report listing "Identity Theft, 530.5PC" on the Classification Line. The stat code is 112. While the Department may investigate the 530.5 PC violation, this does not necessarily mean it will handle the entire case. If the suspect(s) are committing other crimes in the name of the victim, in other jurisdictions, those respective law enforcement agencies are responsible for writing an incident report and investigating the separate offenses.

For example, a victim resides in Norwalk Station's area and discovers someone has used their personal identifying information to apply for a credit card, and the credit card was delivered to an address in Anaheim. The card is subsequently used to make purchases in Anaheim.

In this scenario, The Sheriff's Department (Norwalk Station) would take a 530.5PC report, regardless of where the issuing bank is located. The Anaheim Police Department would be responsible for the illegal use of a credit card in its jurisdiction and take a report for violation of Penal Code Section 484g (Using Access Card Obtained Without Consent of Cardholder or Issuer). Conversely, if the victim resided in Anaheim and their personal identifying information was used illegally to obtain and use a credit card in Norwalk Station's area, the Anaheim Police Department would take a 530.5PC report and Norwalk Station, the 484g PC report.

A 530.5 PC report, should contain at least one incident of fraudulent activity (e.g., Visa Card account number 1234 5678 9023 3456 applied for in the victim's name and the victim said they never applied for such card).

Deputies shall advise the victim to call the three credit bureaus (Transunion 800-6807289, Equifax 800-2908749 and Experian 888-3973742) and have a "Fraud Alert" placed on their account. This alert usually lasts for 90 days, unless accompanied by a copy of a police report. The incident report shall reference this notification.

Deputies shall also tell the victim they are entitled to a free copy of their credit report from all three bureaus if they are a victim of fraud. They should examine each report as some activity may show on one report and not the other. Different credit bureaus occasionally receive reports from different sources. Deputies should instruct the victim to register their complaint with the Federal Trade Commission at (877)ID-THEFT, so their information is placed into a national database.

If the victim has made reports to other agencies (e.g., United States Secret Service, United States Postal Service, California Department of Motor Vehicles, other law enforcement agencies, etc.), those reports shall be referenced in the Departmental Incident (First) Report.

Deputies shall issue the victim a copy of the Department's *Victim's Guide to Identity Theft* and reference it in the first report. Copies of the guide can be obtained from the Sheriff's Data Network, in Microsoft Outlook, at the following address:
Public Folders/All Public Folders/Field Operations Info./ Forgery Fraud Information

ADDITIONAL SCENARIOS:

1. A victim who resides in Lennox Station area, becomes aware she has a warrant for her arrest for a drug possession charge out of Los Cerritos Court. The victim asserts she is not the subject of the warrant. An unknown suspect used her name and birth date when she was arrested in Lakewood for drug possession. The suspect was fingerprinted when arrested, giving the victim a CII record.

The victim needs to make a False Personation of Another report, 529.3PC, at Lakewood Sheriff's Station (or the arresting law enforcement agency). She needs to contact Los Cerritos Court and report they are the victim of a false personation. If she is wrongfully prosecuted for the criminal charge, they need to contact the state Department of Justice (DOJ) and the FBI to clear their name. The victim may be required to present her fingerprints for comparison to clear her name. DOJ needs to be contacted by the arresting agency and the CII record updated.

2. A victim who lives in Long Beach receives notification in the mail from DMV, that his driver's license is now suspended for a citation received in Carson which was not paid to Compton court. The citation was received by an imposter using the victim's information.

The victim needs to make False Personation of Another report, 529.3PC, at Carson Station. Carson Station will investigate the allegation to clear the citation and notifies the court. The victim needs to contact Compton Court and the DMV to report he is the victim of a false impersonation. He needs to have DMV check if the imposter obtained a new license using the victim's name. After clearing the case with the court, the victim needs to take the court record to the DMV to clear his license.

3. A victim who lives in El Monte discovers someone impersonated them and obtained telephone service in Lynwood using the victims name and social security number.

The victim needs to make an Identity Theft report, 530.5PC, at El Monte Police Department (where they reside), and an additional report of Obtaining Phone Service by Fraud, 502.7(a)(5)PC to Century Station (Servicing Lynwood) for where the services were fraudulently obtained.

4. A victim who lives in Cerritos is receiving state disability for injuries obtained at work. Using the victim's name and social security number, an unknown suspect is working in Dallas, Texas using the victim's information and the wages are being reported to Social Security. The victim is notified that their state disability benefits are being ceased, and they owe the state money since it was discovered they are receiving pay and working in Dallas, Texas.

The victim needs to make an Identity Theft report, 530.5PC, to Cerritos Station and also report the incident to Dallas Police Department, Social Security and the State of California Employment Development Department.

PC§ 530.5 vs. 529.3 vs. 148.9

PC§ 530.5 *Identity Theft*
Every person who willfully obtains personal identifying information, as defined in subdivision (b), of another person without the authorization of that person, and uses that information to obtain, or attempt to obtain, credit, goods, or services in the name of the other person without the consent of that person is guilty of a public offense.

PC§ 529.3 *False Personation of Another*
Every person who falsely personates another in either his private or official capacity, and in such assumed character either: Does any other act whereby, if done by the person falsely personated, he might, in any event, become liable to any suit or prosecution, or to pay any sum of money, or to

Attachment #5
Overview of LASD Efforts and Accomplishments

The Pilot Project

- Department wide education and training
- Education Training of Field Operations Units (20 Patrol Stations)
    - Full service approach similar to STOP Program
    - Victim's Guide for Identity Theft
    - Field Deputy's Guide for Identity Theft
    - Field Operations Directive
- Public awareness and prevention campaign
- Centralized tracking
- Public-Private Partnerships
- Liaisons with local, state, and federal agencies
    - Bellflower
    - Postal, DMV, CHP, SSA, Secret Service
- Handling of Cases
- Proposed legislation to fund multi-agency multi-jurisdictional teams statewide (Hertzberg AB 1949)
- Assistance to the California Commission on Peace Officer Standards and Training for curriculum development for a 40 hour class for investigators for Identity Theft
- Participated in President's National Summit on Identity Theft in Washington DC
- Lead referral agency for FTC for Identity Theft cases in the Region
- Opening of new office facility in Bellflower California

County of Los Angeles
Sheriff's Department Headquarters
4700 Ramona Boulevard
Monterey Park, California 91754-2169

LEROY D. BACA, SHERIFF

July 23, 2000

Michael Kochmanski
Special Agent in Charge
Internal Revenue Service Criminal Division
P.O. Box 12699
Santa Ana, California 92712

Dear Mr. Kochmanski:

I am writing this letter to tell you about a multi-jurisdictional law enforcement problem that plagues your agency in Los Angeles County. Identity theft has risen to epidemic proportions. As you are aware, each identity theft case is not just one case, but many, and affects many agencies with enforcement and regulatory responsibilities to our constituents.

In July 1999, I detailed investigators to quantify the problem as it relates to the Los Angeles County Sheriff's Department. Our Department alone has documented a 42 percent increase from 1998 to 1999. We project over 1,600 cases in our jurisdiction alone for the year 2000. Our team researched the issue, and developed and implemented a training program. They have implemented a public awareness and prevention campaign and formed key liaisons with the private sector (computer manufacturers, telecommunications providers, and other trade groups). They work with the California Commission on Peace Officers Standards and Training on statewide training curriculum.

After further research of Department statistics, the team identified the Lakewood regional area as having the highest relative incidence of fraud related activity. With the assistance of the City of Bellflower, the team secured office space and other resources. The office is scheduled to be operational June 1, 2000.

The team will vigorously investigate identity theft and related fraud issues that have a nexus to Los Angeles County. With the team concept, we will be able to target both the identity

thieves, the receivers of stolen property, and those misusing the Postal Service, Social Security, and driver's license information.

We are all aware of the limited nature of resources. With that in mind, our Department has detailed three investigators and a lieutenant to the issue. We cordially invite you to detail an investigator from your agency full time to this team. We are aware that Special Agent Jennifer Mullins from your agency investigate these types of crimes. Please feel free to have your investigator bring their existing cases, as we are likely to have active investigations of the same suspects. This team will enable your investigator to coordinate and investigate cases, and compile suspect information on a countywide basis. Additionally, as part of this team, your investigator will have access to COPS deputies and our criminal data resources.

For further information regarding this matter, please contact Lieutenant Jack Jordan or Detective Joseph Dulla of our Forgery/Fraud Detail at telephone number (562) 946-7217.

Sincerely,

LEROY D. BACA, SHERIFF

William G. Graves, Captain
Commercial Crimes Bureau

County of Los Angeles
Sheriff's Department Headquarters
4700 Ramona Boulevard
Monterey Park, California 91754-2169

LEROY D. BACA, SHERIFF

July 23, 2000

Randy DeGasperin
Postal Inspector
United States Postal Inspection Service
300 North Long Beach Boulevard
Long Beach, California 90802-2427

Dear Mr. DeGasperin:

I am writing this letter to tell you about a multi-jurisdictional law enforcement problem that plagues your agency in Los Angeles County. Identity theft has risen to epidemic proportions. As you are aware, each identity theft case is not just one case, but many, and affects many agencies with enforcement and regulatory responsibilities to our constituents.

In July 1999, I detailed investigators to quantify the problem as it relates to the Los Angeles County Sheriff's Department. Our Department alone has documented a 42 percent increase from 1998 to 1999. We project over 1,600 cases in our jurisdiction alone for the year 2000. Our team researched the issue, and developed and implemented a training program. They have implemented a public awareness and prevention campaign and formed key liaisons with the private sector (computer manufacturers, telecommunications providers, and other trade groups). They work with the California Commission on Peace Officers Standards and Training on statewide training curriculum.

After further research of Department statistics, the team identified the Lakewood regional area as having the highest relative incidence of fraud related activity. With the assistance of the City of Bellflower, the team secured office space and other resources. The office is scheduled to be operational June 1, 2000.

The team will vigorously investigate identity theft and related fraud issues that have a nexus to Los Angeles County. With the team concept, we will be able to target both the identity

thieves, the receivers of stolen property, and those misusing the Postal Service, Social Security, and driver's license information.

We are all aware of the limited nature of resources. With that in mind, our Department has detailed three investigators and a lieutenant to the issue. We cordially invite you to detail an investigator from your agency full time to this team. We are aware that Inspector Mark Zito from your agency investigates these types of crimes. Please feel free to have your investigator bring their existing cases, as we are likely to have active investigations of the same suspects. This team will enable your investigator to coordinate and investigate cases, and compile suspect information on a countywide basis. Additionally, as part of this team, your investigator will have access to COPS deputies and our criminal data resources.

For further information regarding this matter, please contact Lieutenant Jack Jordan or Detective Joseph Dulla of our Forgery/Fraud Detail at telephone number (562) 946-7217.

Sincerely,

LEROY D. BACA, SHERIFF

William G. Graves, Captain
Commercial Crimes Bureau

County of Los Angeles
Sheriff's Department Headquarters
4700 Ramona Boulevard
Monterey Park, California 91754-2169

LEROY D. BACA, SHERIFF

July 23, 2000

Steve Barry
Supervising Special Agent
Social Security Administration Office of the Inspector General
Investigations 6340 security Boulevard, First Floor
Baltimore, Maryland 21235

Dear Mr. Barry:

I am writing this letter to tell you about a multi-jurisdictional law enforcement problem that plagues your agency in Los Angeles County. Identity theft has risen to epidemic proportions. As you are aware, each identity theft case is not just one case, but many, and affects many agencies with enforcement and regulatory responsibilities to our constituents.

In July 1999, I detailed investigators to quantify the problem as it relates to the Los Angeles County Sheriff's Department. Our Department alone has documented a 42 percent increase from 1998 to 1999. We project over 1,600 cases in our jurisdiction alone for the year 2000. Our team researched the issue, and developed and implemented a training program. They have implemented a public awareness and prevention campaign and formed key liaisons with the private sector (computer manufacturers, telecommunications providers, and other trade groups). They work with the California Commission on Peace Officers Standards and Training on statewide training curriculum.

After further research of Department statistics, the team identified the Lakewood regional area as having the highest relative incidence of fraud related activity. With the assistance of the City of Bellflower, the team secured office space and other resources. The office is scheduled to be operational June 1, 2000.

The team will vigorously investigate identity theft and related fraud issues that have a nexus to Los Angeles County. With the team concept, we will be able to target both the identity

thieves, the receivers of stolen property, and those misusing the Postal Service, Social Security, and driver's license information.

We are all aware of the limited nature of resources. With that in mind, our Department has detailed three investigators and a lieutenant to the issue. We cordially invite you to detail an investigator from your agency full time to this team. We are aware that Special Agent Scott Johnson and Special Agent Chris Castellanos from your agency investigate these types of crimes. Please feel free to have your investigator bring their existing cases, as we are likely to have active investigations of the same suspects. This team will enable your investigator to coordinate and investigate cases, and compile suspect information on a countywide basis. Additionally, as part of this team, your investigator will have access to COPS deputies and our criminal data resources.

For further information regarding this matter, please contact Lieutenant Jack Jordan or Detective Joseph Dulla of our Forgery/Fraud Detail at telephone number (562) 946-7217.

Sincerely,

LEROY D. BACA, SHERIFF

William G. Graves, Captain
Commercial Crimes Bureau

Senator FEINSTEIN. Thanks, very much, Sheriff. I'll hold my questions, and give an opportunity for the two victims to testify.

Let's begin with Selene, would you——

Ms. KASSIN. OK, sure, thanks.

Senator FEINSTEIN [continuing]. Begin your testimony, please?

STATEMENT OF SELENE KASSIN

Ms. KASSIN. Thank you, Senator.

I produced a documentary called "Stolen Identity, Crime of the Millennium," which was inspired by my own experience of having my identity stolen.

The person who stole my identity did not know me. They did not know my age or my mother's maiden name. They did not know my driver's license number. They did not even know what I looked like.

In fact, she changed all these statistics to match her own. All this person knew that stole my identity was my Social Security number.

Having my identity stolen and recovering my identity was traumatic, scary and surreal.

I felt I was victimized once by a perpetrator, and again by the system.

I found out someone was living as me, from a letter from a credit card company, asking if I tried to open up a new account.

When I called the credit bureaus, I found a new address, phone number, driver's license number and numerous new credit cards.

I called and I went to several police stations, and I was refused help.

The police told me they would take a courtesy report, but not to expect an investigation, and the burden of proof was on me.

I called the police to see if they could tell me whom the phone line belonged to, that was listed on my credit report. They said they couldn't. I found out it belonged to me.

So, I called the phone company to have them disconnect the phone line. They said they would have to notify the other Selene in writing first.

The other Selene, the person who stole my identity, called them and was more convincing than I was, in proving my own identity.

They believed her and didn't believe me, and subsequently closed the fraud file.

I called the credit, I'm sorry, I called the credit card companies and I begged them to send me the documents that were forged in my name, and they did send them, but they sent them to her.

As quickly as I would close the accounts, she would open new ones. I called the credit bureaus to ask why they opened new accounts when I had it flagged. They had no answer.

My story is not typical, because I was fortunate enough to finally receive help from police.

After several months of persistence, I was able to get enough evidence by myself that Detective Edholm of the Beverly Hills Police Department arrested her.

She had a prior criminal record. I was told she would not be released on bail, but she was. I was notified several weeks later, that someone tried to take out a loan, in my name.

The identity thief was sentenced to 18 months. She served 9 months, and is now out on parole. The parole officer warned me that she could do it, all over again.

The shocking thing about being a victim of stolen identity is you're often met with disbelief. People think stealing your identity cannot be that easy, that the police could not refuse to help you, and that if your identity was stolen, there has to be a remedy, to not only get it back, but also to prevent it from happening again.

Because many of these aspects are not easy to digest as true, I was inspired to produce a documentary to give a voice to the victims that were often silenced by the current laws.

The documentary "Stolen Identity, Crime of the Millennium" provides candid testimony from the victims themselves, that this crime exists and to what extent.

It's currently being distributed by Aames Multimedia, Chatsworth to schools, universities, and law enforcement agencies, nationwide.

While producing the documentary, I was astonished to learn that identities were being stolen, not only to obtain cash and credit cards, but to commit serious crimes in the name of an unsuspecting victim.

I want to share some of their devastating stories, as they've tried to recover their identity and clear their names.

One victim best described his battle in just a few words. It's war, and I'm the enemy.

It's hard to believe that the crime of stolen identity exists, because it's nearly invisible to its victims.

You don't see it happening to you, you wake up one day and all of the sudden you could be facing jail time.

Rochelle, the school teacher, finds out she's been denied car insurance. When she calls to find out why, she finds out she has three driver's licenses that had been, that have been made out in her name. She also finds out she has an arrest warrant out for her.

When she inquires with the DMV, they're suspicious, but they're suspicious of her. When she goes to the police, they refuse to help her.

So, she goes to court with documents proving her identity, but the judge doesn't believe her.

The story is typical. The first response that most victims face, when confronting the law is, you're guilty, and the burden of proof is on the victim.

Victims generally have the responsibility of retrieving their identity, on their own, even if law enforcement is contacted.

The victims also have to endure an emotionally-draining, costly, and time-consuming experience, of clearing their own name.

I met Linda, a college student over many months, as she tried to prove her identity.

She found, found out her identity was stolen, when the police showed up at her door with a bench warrant. She was charged with being under the influence of PCP.

She had to live with the terror of going to jail, as she endured months of court appearances. She tried to prove her innocence, with her fingerprints. She had to have her fingerprints done 5 times, and they still did not prove her innocence.

Finally, months later, in yet another court proceeding, she is told to undress, so that she could be examined for a distinguished tattoo, in the end, which would clear her name.

She now carries the wrong person's certificate for the rest of her life, and she has to worry about a police officer knocking on her door, for something she didn't do, because the identity thief and her now share the same name.

Stolen identity is an epidemic that attacks silently and indiscriminately. It's just a matter of time before you, or someone you know, will have their identity stolen.

The crime of stolen identity is in dire need of a solution, and I support both of your bills, and I think it's a very important step.

Senator FEINSTEIN. Thanks, very much, Selene.

Ms. KASSIN. Sure.

[The prepared statement of Selene Kassin follows:]

PREPARED STATEMENT OF SELENE KASSIN

I produced a documentary called Stolen Identity: Crime of the Millennium inspired by my own experience of having my identity stolen. The person who stole my identity did not know me. They did not know my age or mother's maiden name. They did not know my driver's license number. They did not even know what I looked like. (In fact she changed all these statistics to match her own.) All this person knew that stole my identity was my social security number. Having my identity stolen and recovering my identity was traumatic, scary and surreal. I felt I was victimized once by the perpetrator and again by the system.

I found out Someone was living as me from a letter from a credit card company asking if I tried to open up a new account. When I called the credit bureaus, I found a new address, phone number, driver's license number and numerous new credit cards. I called and went to several police stations and I was refused help. The police told me they would take a courtesy report—but not to expect any investigation—and the burden of proof was on me.

I called the police to see if they could tell me whom the phone line belonged to that was listed on my credit report. They said they couldn't. I found out it belonged to me. So, I called the phone company to have them disconnect the phone line. They said they would have to notify the other "Selene" in writing first. The "other selene" the person who stole my identity called them and was more convincing than I was in proving my own identity.

They believed her and didn't believe me. And Subsequently closed the fraud file. I called the credit card companies and begged them to send me the documents that were forged in my name. . . . And they did send them. But they sent them to her. As quickly as I would close the accounts she would open new ones. I called the credit bureaus to ask why they opened new accounts when I had it flagged. They had no answer.

My story is not typical, because I was fortunate enough to finally receive help from the police. After several months of persistence, I was able to get enough evidence by myself that Detective Edholm of the Beverly Hills Police Dept. arrested her. She had a prior criminal record. I was told she would not be released on bail. But, She was. I was notified several weeks later that someone tried to take out a loan in my name. The identity thief was sentenced to 18 months. She served 9 months and is now out on parole. The parole officer warned me that she could do it all over again.

The shocking thing about being a victim of stolen identity is you are often met with disbelief. People think stealing your identity cannot be that easy. That the police could not refuse to help you. And that if your identity was stolen, there has to be a remedy to not only get it back but also prevent if from ever happening again.

Because many aspects of the crime are not easy to digest as true, I was inspired to produce a documentary to give a voice to the victims that were often silenced by the current laws. The documentary: Stolen Identity: Crime of the Millennium provides candid testimony from the victims themselves that this crime exists and to what extent. It is currently being distributed by Aims Multi-Media in Chatsworth to schools, universities and law enforcement agencies nation-wide.

While producing the documentary, I was astonished to learn that identities were being stolen to not only obtain cash and credit cards, but to commit serious crimes in the name of an unsuspecting victim.

I want to share some of their devastating stories as they tried to recover their identity and clear their names. One victim best described his battle in just a few words. "It is war, and I am the enemy."

It is hard to believe the crime of stolen identity exists because it is nearly invisible to its victims. You don't see it happening to you. You wake up one day and all of a sudden you could be facing jail time.

Rochelle, a schoolteacher finds out she has been denied car insurance. When she calls to find out why—she finds out her driver's license has been revoked for a year. She owes an outstanding fine and there is a warrant out for her arrest. She also finds out there are three driver's licenses being used with her name and someone else's picture on it. When she inquires with the DMV, they are suspicious . . . of her. When she goes to the police—they refuse to help her. So she goes to court with documents proving her identity. But the judge doesn't believe her.

This story is typical. The first response that most victims face when confronting the law is "you're guilty." And the burden of proof is on the victim. Victims generally have the responsibility of retrieving their identity on their own, even if law enforcement is contacted. The victims also have to endure an emotionally draining, costly and time-consuming experience of clearing their own name.

I met Linda, a college student over many months as she tried to prove her identity. She found out her identity was stolen when the police showed up at her door with a bench warrant. She was charged with being under the influence of PCP. She had to live with the terror of going to jail as she endured months of court appearances. She tried to prove her innocence with her fingerprints. She had to have her fingerprints done five times. And they still did not prove her innocence. Finally, months later in yet another court proceeding. She is told to undress so that she could be examined for a distinguished tattoo that in the end would clear her name. She now has to carry a wrong person's certificate for the rest of her life. And she still has to worry about a police officer knocking on her door for something she didn't do because the identity thief and her now share the same name.

Stolen identity is an epidemic that attacks silently and indiscriminately. It is just a matter of time before you or someone you know will have their identity stolen. The crime of stolen identity is in dire needs of a solution. This hearing is an important step in resolving this problem.

Senator FEINSTEIN. Appreciate the testimony.

Mari Frank.

STATEMENT OF MARI FRANK

Ms. FRANK. Senator Feinstein, I thank you so much for allowing me to come and address you today.

In May 1998, I appeared before this distinguished committee, when you were considering the Identity Theft and Assumption Deterrence Act of 1998.

I especially applaud you and Senator Kyl, for the work that you did in having that law passed and signed by the President, in 1998.

At that, when I was a victim, there was only one State in the country that had an identity theft statute, and that was Arizona.

And now, because of the, the new identity theft Federal bill that makes identity theft a crime, we have almost forty States that have identity theft statutes, and I, I really applaud you, for taking the lead on that.

When that bill was passed, it also established a central clearinghouse for the identity theft complaints within the Federal Trade Commission, and it was a very, very good positive step.

However, that, that bill only dealt with victims after they had been victimized. The two bills that you have are clearly for prevention, which is what we need right now.

I want to tell you a little bit about my story, and I'm also gonna go, after I tell my two stories, which I was just a victim again, last

month, I will also tell you then some of the important aspects of your bill, and how they will affect victims in the future.

I'm an attorney, and the author of the "Identity Theft Survival Kit." I'm also the co-author of "Privacy Piracy," which I just gave to you. As you remember, I gave you the, the kit when I was in Washington.

I'm also an Orange County Sheriff Reserve, and I sit on the High Tech Crime Task Force, with several of the Los Angeles Sheriff's Department's people.

And I want to applaud you for Joe Dulla, and all the people that you have, who have done so much, to really foster help for victims.

My expertise in identity theft was acquired by necessity. In restoring my own life, I was compelled to assist in the passage of State and Federal legislation, and create materials to help other victims.

Because the epidemic was growing so rapidly, those of us who had some understanding of the crime and its causes have been called upon to speak to the media, assist governmental agencies, and provide education to law enforcement and the financial industry.

I was greatly honored to speak at the White House on, in May 1999, to discuss consumer privacy and identity theft.

In August 1996, I received a call from a bank that I'd never heard of, asking me why I had not paid my $11,000 bill.

At first, I wanted to get off the phone and tell them they were crazy, but the woman then told me my, asked me if that was my Social Security number and if it was my proper birth date.

When my heart jumped into my throat, I answered, where did you send the bills? Where did you send the credit card?

And I was told that, after much arguing with the person, exactly where the bills were, the bills and the statements were sent, and it was sent to Ventura, CA, which is about 3½ hours away from my home.

I told her that it was fraud. She told me at that time, that she would erase it from fraud. However, it was then sent to collections, by the way.

I found out that my imposter had used my credit to obtain new credit cards, credit lines, services and cash advances, all over $50,000.

She also got a red convertible Mustang in my name. She had driven almost 3 hours to get my business cards, and parade as an attorney, up in Ventura, CA.

She had rented a car and had totaled it, and I was being sued by Thrifty Rental Car Agency.

My impersonator was assuming my entire identity, not only my personal identity, but my professional identity, as well, and I was afraid I was going to be disbarred from the State of California.

It took me over 500 hours, and more than 10 frustrating months, to regain my credit. I have over five boxes of, overstuffed banker's boxes, filled with correspondence from credit reporting agencies, credit card agencies, the IRS, the Social Security Administration, the Postal authorities, the State Bar of California, on and on, and on.

In 1996, according to State and Federal law, I wasn't considered the victim, until I found a peace officer who, himself, had been a peace officer for over 20 years, and he was a victim of identity theft.

He sent a Lieutenant out to the home and this woman, indeed had said that she knew me, although she did not, and she said that I used to live with her, and she was getting mail to me there, and she always sent it back.

We found out that this woman was on probation for shoplifting, she was arrested, let out on bail, and continued to accept fraudulent cards, and pre-approved offers.

And I just want to show everybody, what exactly happened here, because it will show how the financial industry facilitated this crime.

I've got handouts for you, and if you'll look, this is a copy of the original application that, by the way, it took me pulling teeth to get from the Bank of New York, Delaware.

If you'll look where it says, "Tracy Lloyd." Tracy Lloyd is my imposter who was convicted. She put, as you notice here, she'd crossed out one line through her name, put my name, and she did put my Social Security number, although I did erase it for you, while here today.

Senator FEINSTEIN. Good.

Ms. FRANK. Unfortunately, you see how old I am, because that was my proper birth date, and she had the spelling of my address of my office spelled wrong. She said, she had other things on here that were wrong, but notice she had her proper address.

Now, she has a much nicer handwriting than I do, she sent this card in, and she sent this application in, which you notice was not even a pre-approved offer, and she got a $10,000 credit card. She used this to get other credit cards.

Now, the important thing to note is that when she got this credit card, you have to question, who was processing this credit card with the credit card company?

Why did they not question the fact that she just crossed off a name? When they pulled my credit report, to see if they were going to issue a credit line of $10,000, they would have looked at my credit report, and if they were cautious, they would have compared and seen that there was a different address on there.

That should have been some kind of clue. They did nothing about that. Instead, Senator Feinstein, they sent her a credit card.

Immediately after that, when that credit card was sent in, and I don't know if all of you notice, but when your credit card, a new credit card is sent in to the credit reporting agencies, then what they do, is they consider themselves reporting agencies, and what they do, is they just change the address to the new address on the new card.

So, if you'll turn the paper over, you will then see what happened. Once, she got that first card, it started the whole craziness, and what she did, what happened then was the credit reporting agencies, which I don't know if all of you know this, but they sell your name and your financial information and your profile on promotion. At that time, I didn't know that.

So, because I had pristine credit, and a new credit card was just issued, they sold my name on promotion to many, many different credit card companies.

This is an example of a pre-approved offer. If you look at this, now she says she's making $300,000 a year. I wish.

By the time she did this, she was not only doing this to me, but to other people, and she probably was making $300,000 a year.

Notice she says she's an attorney with Steve Kuhn and Associates. That's not true. I have my own law office. So, that was a mistake.

She has an address now. Now, she's being sent Mari Frank in Ventura, CA, when in fact, Mari Frank lives in Laguna Niguel, CA.

So now, the pre-approved offer is going to her. Not only was there this pre-approved offer, but there were dozens and dozens like candy, coming to her door.

Also, if you'll notice, she wants to use this as a credit line. She got a $15,000 credit line from this.

If you notice, on the bottom, she says she wants to use it right away to pay off her Capital One account.

So, what she did was, for a period of 10 months, she was using credit line to pay off different credit cards.

So, because she didn't have any of my own credit cards, I had no idea this was going on. I'm getting my different credit card bills every month, and there's no fraud. So, there was no way for me to know.

So, this is an example of the kinds of things you're addressing in your bill, about address changes, and the less than cautious approach. So——

Senator FEINSTEIN. Mari, I'm going to, I neglected to tell everyone, if they could really confine their initial remarks to 5 minutes.

Because, before the Sheriff has to leave——

Ms. FRANK. OK.

Senator FEINSTEIN [continuing]. I'd really like some of the Federal officials to be able to testify as well.

Ms. FRANK. OK.

Senator FEINSTEIN. And I need to ask him some questions.

Ms. FRANK. Okay, I just want to briefly tell my second identity theft victimization, that happened last month.

Senator FEINSTEIN. OK.

Ms. FRANK. I came back from a trip to New York, I had my AmEx card in my wallet, and I had $9,000 worth of fraudulent charges.

I was a victim of skimming. For those, if you don't know what skimming is, skimming is when someone takes a credit card, and slides it through a little skimmer, they may have it in their pocket, when you go to a restaurant, and they download that information, and have a new card.

And, in fact, the person who charged $9,000 at two different dealerships, had a name of Michael Brown, supposedly.

So, I was the victim again. It took me, again, hours to clean up, and the credit reporting agencies were very difficult to work with, and Experian, for example, didn't even have a human answering the phone, and didn't get me my credit report for 20 days.

So, I have all of this in my testimony, and I can answer questions, and I also reflect on here, all of the things that you're doing, I am showing why it's so important.

So, I just want to tell you, I honor you, and thank you for both of the bills, and I support them strongly.

[The prepared statement of Mari Frank follows:]

PREPARED STATEMENT OF MARI J. FRANK

Senator Feinstein and honorable members of this committee, thank you for the opportunity to address you today. In May of 1998, I appeared before this distinguished committee when you considered the Identity theft and Assumption Deterrence Act of 1998. I especially applaud Senator Kyl and Senator Feinstein for their leadership and efforts in the passage of that law. By making Identity theft a federal crime, it helped to educate states to also make Identity theft a crime. We now have almost 40 states that have enacted statutes—only Arizona had a statute when I became a victim. The federal legislation also established a central clearinghouse for identity theft complaints within the Federal Trade Commission. There is now a toll free number for consumers to call (1–877–IDTHEFT) and a web site of information at *www.consumer.gov/idtheft.* I am grateful that congress focussed on law enforcement's role and allocated more resources, and I am pleased that the Federal Trade Commission is providing education to victims after they find out about their evil twin, but that Act did nothing to prevent the crime from occuring.

When I testified on that bill, I brought to your attention how the credit reporting agencies and the credit grantors were facilitating the crime of identity theft. I demonstrated how certain practices in the financial industry made the social security number easily accessible to fraudsters (it is the key to identity theft), and continued with procedures that failed to verify identity and address changes. Thank you for listening to those concerns and addressing those issues in Senate Bill S. 2328, The Identity Theft Protection Act of 2000, and in Senate Bill S. 2699 The Social Security Number Protection Act of 2000. In my testimony today, I will tell you about real life examples that clarify the need for these bills that you are now considering.

My written testimony will give you a brief overview of my own identity theft nightmares; provide you with insights that I have gained after hearing from thousands of victims; indicate why the bills we are considering today are so critical; share a few helpful tips for consumers to protect themselves, and provide some measures to take if one's identity is stolen.

I am an attorney, the author of the Identity Theft Survival Kit (Porpoise Press, 1998), Privacy Piracy (Office Depot 1999—co-authored with Beth Givens, the Director of the Privacy Rights Clearinghouse), and an Orange County, California Sheriff Reserve for the High Tech Crime Unit. My expertise in Identity Theft was acquired by necessity.

In restoring my own life, I was compelled to assist in the passage of state and federal legislation, and create materials to help other victims. Because this epidemic grew so rapidly, those of us who have an understanding of the crime and its causes have been called upon to speak to the media, assist governmental agencies, and provide education to the financial industry and law enforcement. I was greatly honored to address members of congress and the financial industry on May 4, 1999, when I spoke at the White House on Consumer Privacy. I shared my story and offered solutions.

In August 1996, I received a call from a bank that I had never heard of asking me to pay an $11,000 bill to them. I was about to hang up, when the woman asked if she had my correct social security number, birth and other identifying information. Upon hearing her tell me my personal and financial information, my heart leaped into my throat. I asked where the company had sent the credit card and billing statements.

She gave me an address four hours from my home in a city I had never been. I found out that my impostor had used my credit to obtain all new credit cards, credit lines, services, and cash advances of over $50,000. She also had purchased a red convertible mustang using my name, had rented a car and totaled it and I was being sued by the rental car agency. My impersonator was also assuming my professional identify by using my name on business cards indicating that she was a licensed California attorney.

It took me over 500 hours and more than 10 frustrating months to regain my credit—I have 5 overstuffed bankers boxes filled with correspondence with credit reporting agencies, credit card companies, the IRS, the Social Security Administration, the Postal Inspector, the State Bar of California, and on and on. In 1996, according

to state law and federal law I was not considered the victim. Until I found a peace officer that was victim himself, I could not get a police report. Even though there are almost 40 states with Identity Theft statues, over half of the victims who contact my office cannot get law enforcement to issue a report.

Many law enforcement agencies are concerned that if a report is issued, a full investigation will be needed, and there are just not enough resources to investigate all the identity theft. Unfortunately, without a police report—it is impossible to clean up the mess.

Although prior to my stolen identity, I had pristine credit, after my evil twin abused my financial profile, I was considered a low life that didn't want to pay my bills. I was hounded by creditors and collection agencies and ignored by the Credit Reporting agencies. Victims call me every day telling me the same story.

I found out that my "identity clone"—who I never knew, had been working as a contract secretary in several law offices. She was able to access a copy of my credit report as well as those of other victims. Many law offices as well as car dealerships, realtors, banks, etc. have on line or fax subscriptions to order credit reports from the credit reporting agencies and resellers. So my impostor accessed the system, obtained my entire personal and financial profile, including my social security number, and took over my identity. Because I was tenacious, and the law enforcement agency in the city where she resided had empathy, she was arrested. Soon after she was released on bail, she continued to defraud others and me.

She stalked my family by phone; dumpster dived my garbage, stole my mail, and still drove around in the red convertible mustang purchased with my credit. A year later she was sentenced to a two month work furlough program and probation (still driving that car). A few months later she was apprehended committing identity theft again in a different state. Unfortunately, although the police took the case seriously, the district attorney and judge saw this as economic crime—the stepchild of the criminal justice system. Very few of identity theft cases are investigated—thus few impostors are prosecuted unless there is a great loss or a crime ring is involved.

Although I was victimized, I chose not to succumb to victim-hood. I created the kit that I wish I would have had—The Identity Theft Survival Kit with pre-written legal letters on diskette and step by step instructions.

I developed a web site with over 70 pages of free information to help other victims. Because of this outreach to victims, I receive at least 100 e-mails and calls a month from victims and frightened consumers across the country. They are still experiencing the same problems with financial industry as I did.

Before I go into those problems and how the two bills presented help focus on those concerns, it is important to know that no one is immune from this crime and that it can happen more than once to the same person. I receive calls from lawyers, doctors, homemakers, retired persons, teachers, students, judges, and even widows who tell me that their loved one who has died is a victim after death.

In early July, 2000 (last month) I gave a presentation on Identity Theft for Chase Manhattan Bank in New York City. I explained to them how a customer can become a victim of identity theft from "skimming" when, for example, a waiter takes credit card at the end of the meal, slides the card through a small 3" by 5" skimmer in his pocket, then processes the card at the register and returns the card to the cardholder smiling and gratefully accepting his tip. That evening, the fraudster downloads the information that he obtained from the back of the customer's card and sends it to make a new card with the duplicated metal strip of the customer's card on the fraudulent card.

When I returned to California after the program, I opened my American Express bill to find over $9,000 of fraudulent charges with my credit card still in my wallet.

Cleaning this mess only took me 7 hours. Amex promptly opened an investigation, but told me that they would not notify me of the results. They gave me the telephone numbers of the two car dealerships (where most of the fraud occurred) located in a California city that I had not visited. Upon calling the dealerships, I learned that the man who used my "card" was named Michael Brown and he lived at an address near the dealerships several hours from my residence.

So here I was victimized again. I called the fraud department of the three credit reporting agencies. After at least twenty minutes of pushing buttons and waiting, I finally was able to reach a human at Equifax and TransUnion. They told me to write to them concerning the fraud enclosing copies of my license and a utility statement. Within a week I received my credit reports—the fraud departments of those agencies provided no further referrals, assistance or suggestions. I fortunately knew what steps to take; however, most victims haven't a clue of what to do!

When I called Experian, even after pushing every button on my phone, I could not reach a live person. I was told by recorded message that I was to send a letter

referring to my fraud and I would receive a report within 10 days. After 20 days I received a form letter—just last week, stating that I needed to send $8.00—when in fact a credit report is free for victims of fraud. I had sent my mortgage statement, a copy of my driver's license and a utility bill. After a call to the number of the form letter, I waited 30 minutes until I relieved a live, but rude person who told me that I needed to send a recent phone bill to get my report and place a fraud alert on my file for more than 90 days—up to seven years. After demanding to speak to a supervisor, I was allowed to fax the phone bill, and he agreed to send my credit report by overnight mail once he found out I was to testify at this hearing. Most victims are overwhelmed when they call the credit bureaus. They don't know what to ask and receive virtually no assistance or reassurance from the credit reporting agencies. Although the Credit Bureaus claim that they have improved their assistance, my experience just this month, and the e-mails and phone calls I receive, tell me otherwise.

When I became a victim the first time, it was a total identity take over, obviously much worse then this recent skimming incident. My evil twin took advantage of a very easy system, which is illustrated by the attachments to this written testimony. My convicted impostor, Tracey Lloyd had received a promotional offer sent to her residence by The Bank of New York, Delaware. This started the "identity cloning" process. You can see from this document, that she crossed one line through her name, inserted mine, wrote in my social security number (which I have erased for obvious reasons) and added some other identifying information, much of which was not correct, and within two weeks she received a credit card at her address with my name with a credit limit of $10,000.

Whose fault was it that Tracey Lloyd was able to commit fraud? Why didn't the bank's personnel question the fact that the name associated with the address was crossed out and changed to an entirely different name on the application? Clearly the bank pulled my credit profile before issuing a card with such a $10,000 credit limit. Why did the bank issue the credit card to an address that was different from the address on the my credit report? Why didn't the bank question the fact that the name of the law office and the address on the application did not match the information on my credit report? If the bank had taken just a moment to verify and match, they would not have issued the card without further investigation. Because of their faulty procedures, I experienced identity theft hell!

Once the credit reporting agencies get news of a new credit card and a new address, they report the new address as the "current address" even though it may be a fraud address. In my case—and this still happens to thousands of victims each day—the new address was reported to the three agencies. This activity of a new card prompted the agencies to sell my name with the new address on promotion (I have since removed my name from the promotional lists by calling 1–888–5–OPTOUT). Then as you can see in exhibit two attached, my impostor received dozens of pre-approval offers (like candy to her door!) This offer from Security Pacific enabled her to get checks with a $15,000 credit line. The more credit cards she received, the more credible she was, and the more she could apply for. With my business cards and a false driver's license with her picture, she was transformed into a credit worthy professional with instant credit, while my reputation was being destroyed without my knowledge. She had been impersonating me for 11 months before I received that fateful call demanding money. Most victims don't find out about the identity fraud until they are denied credit or employment or a service. Other times they learn about the fraud when they receive a call from a bank or collection agency. Because of the insidious nature of this crime and the less than careful procedures of the credit grantors and credit reporting agencies, there is little a savvy consumer can do to avoid if an impostor wants to strike. For that reason, the Identity Theft Protection Act of 2000—S. 2328 provides some important safeguards.

ADDRESS CHANGES

In almost every case in which there is an identity takeover (not skimming or the use of a stolen valid credit card), there is always a change of address by the impostor, Holding creditors and credit reporting agencies accountable for verifying address changes is necessary to prevent fraud. The Act requires verification of address for:

1. Impostors who try to change the addresses for valid cards held by the victim or for potential impostors who try addressing their names as additional cardholders at a different address.

2. Potential new accounts by persons who apply for cards at a different address than the address listed for the consumer on his credit report.

FRAUD ALERTS

A fraud alert provides notice to creditors that the consumer must be called before credit is issued. It is a protection from impersonators opening new accounts without thee victim's knowledge. In many cases, even with a fraud alert, credit is issued—especially instant credit where a creditor only receives a credit score and does not see the alert. Also, hundreds of victims have told me that apartments, cell phones, and mortgages were issued in their names after a fraud alert is on file with the credit reporting agencies.

Credit reporting agencies will place a fraud alert on for 7 years. I believe it should be kept on permanently if the victim so wishes; however that is not permitted by the Credit Reporting Agencies.

S. 2325 by Senators Feinstein, Kyle and Grassley allows a consumer to place a fraud alert on a file, and requires that this alert be provided to all users who access the credit report. More importantly it provides penalties for creditors who extend credit without contacting the consumer to verify if credit was requested. If an impostor obtains credit after a fraud alert is on the file there would be sanctions allowable

DUTY TO INVESTIGATE AND THE ISSUANCE OF FREE CREDIT REPORTS

Identity theft victims and non-victims who are harmed by merged and mixed files (one consumer's bad credit appears on that of another with a similar name), there are disastrous results and ruined reputations. The best way to ascertain stolen identity (or other errors reducing a consumer's credit reputation) is to see one's credit report. Several states have already enacted laws to provide one free credit per year to consumers. All consumers should be able to review their credit reports at no cost once a year to reduce the cost of fraud.

SELLING PERSONAL INFORMATION INCLUDING SOCIAL SECURITY NUMBERS

Presently Credit Reporting Agencies are selling the credit header information to information brokers. The information includes personal identifying information such as the social security number. This number is the only identifier an impostor needs to steal your identity. We know of consumers who became victims when only their social security number was used—not even their correct name. Consumers right now do not have the right to opt-out of this information being sold. They only have the right to limit their financial profile form being sold without their permission. With no control over the sale of that personal information, on-line brokers are selling the social security number for as little as $20. This is a small investment for criminals who intend to use the information to defraud someone of thousands of dollars.

INDIVIDUAL REFERENCE SERVICE—DISCLOSURES

We are seeing a dramatic rise in cases of criminal identity theft. This occurs when an impersonator is arrested or convicted of a crime in the name of a victim. A victim of criminal identity theft often doesn't even friend out about the fraud until he is arrested or denied some benefit. We have helped victims who were denied employment due to criminal records that did not belong to them. Victims have been terminated from their jobs, lost custody of their children, been deported, lost their professional license, etc. Even when we finally ascertain the records and provide fingerprints and mug shots to clean up the criminal records, the information brokers have sold that information dozens of times to entities—so the information continues to proliferate. Presently, many of these victims cannot find out what information was sold, to whom it was sold, who to correct it and how to stop it from being sold erroneously again by others. This type of identify theft can last a lifetime and destroy a person's reputation forever.

S. 2328 addresses the need to hold the Individual Reference Services accountable. This bill would ensure that consumers could access the information compiled by the various information brokers to see if the information is correct. I suggest that the bill be amended to clarify the correction procedure and provide penalties for failure to correct in a timely manner. Presently I am helping a victim who has cleared his criminal records, yet the Individual Reference Service company claims it cannot provide a list of who purchased and received the erroneous information so that we can correct the file. This victim was unable to get employment until his story was told on Dateline NBC this past April, 2000.

SUMMARY OF PROBLEM

We are living in an easy credit society (11 billion pre-approved offers were sent out in 1999), where information is readily transferred in a nano-second on the Internet and that information is worth more than currency. In a matter of a few minutes, an impostor can purchase your social security number and apply for numerous credit cards on-line without your knowledge. The impersonator can get medical care, become a legal citizen, take over your professional status, steal money from your accounts, buy life insurance in your name, purchase a home and even be arrested with your identity. Anything you can do, your impersonator can do. We have even had victims tell us that ex-spouses have had friends assume their identity just to ruin their reputation.

So on a local and federal level; we need to work collaboratively. A victim in California may have an impostor in New York City who then sells the data to another criminal in Miami. The impostor could be part of a fraud ring using the mails, selling social security numbers, stealing identities in the workplace through the human resource departments or payroll departments. The crime is complex after it occurs. However if all businesses were more conscientious concerning the proper handling of our personal information, and were held accountable to safeguard that data with monetary sanctions, perhaps the situation would change. If the financial and governmental entities were required to verify and authenticate identities (before issuing credit or providing services, or booking criminals) our identity theft problem would be greatly reduced.

PROTECTING YOURSELF

No one can assure you that you won't become a victim since your information and the issuing of credit is beyond your control, however you can minimize your risk by:

1. Ordering your three credit reports from Equifax, TransUnion, and Experian twice a year to look for fraud accounts and inquiries, and mixed files with errors. Immediately correct anything suspicious and place a fraud alert on your file.

2. Shredding or disposing of all of your confidential information offline and online. Also shred confidential information in your computer and by using shredding software.

3. Don't give out personal information over the Internet or by filling out warranty information. Your personal information is the key, especially your social security number. Don't give out your social security number unless it is for some tax purpose. Ask for an alternative number. Presently companies can ask for your social security number, but you don't have to give it—they may deny you service.

For more free information go to *www.identitytheft.org; www.privacyrightrs.org;* and *www.consumer.gov/idtheft.*

DEALING WITH IDENTITY THEFT IF IT HAPPENS TO YOU

If you become a victim, go to the above web sites for specific guidelines, but here are the top three things to do:

1. Immediately contact the fraud department of the three credit reporting agencies to place a fraud alert and obtain your full reports at no charge. Carefully read these reports and identify false names, fraud addresses, fraud inquiries, and fraudulent account. (See the free form letter at *www.identitytheft.org*)

2. Once you receive your credit reports, make a police report listing all the fraud found on the credit reports and send a copy of the police report with a cover letter to each of the credit reporting agencies requesting that all the fraud accounts listed on the police report be removed within thirty days.

3. Write to all the fraudulent credit grantors (get the addresses from the Credit Reporting Agencies), your own credit grantors and banks to inform them of the fraud and get new passwords (never use your mother's maiden name), write the IRS, the Social Security Administration, the Postal Inspector, etc. (see the list of letters to write at *www.identitytheft.org*—The Identity Theft Survival Kit has all the letters on diskette and includes step by step instructions for who to call, what to say, and how to get what you need to regain your life.

Thank you all for the opportunity to testify about the multifaceted issues of identity theft. California is leading the states in number of identity theft reports and has also taken a lead in dealing with proposing solutions. As a former victim and an advocate, I am grateful for your legislative proposals and will be happy to provide you further information and assistance.

OFFER EXPIRES: 11/17/95

☑ YES! I also want a cash advance of $1,000 as soon as my account is opened. I understand that this amount will be charged against my available credit line as a cash advance.

YES! Please enroll me in the optional Payment Protection Credit Insurance Program. I have read all the details on this application and realize that coverage is not required to obtain credit. I also understand I may cancel at any time. I hereby authorize the premiums to be billed to my account.

Initial Here For Payment Protection:_____ Date:_____

~~Tracey Lloyd~~ Mari Joy Frank
293 Estrella St.
Ventura, CA 93003-1632

1199105819203 7

1LJ

This application must include all requested information. Please print clearly and sign in ballpoint pen.

SOCIAL SECURITY NUMBER	TIME AT PRESENT ADDRESS ([illegible]) YRS. (16) MOS.
DATE OF BIRTH 12 / 9 / 47 (must be 18 years of age or older)	HOME PHONE (805) 644-1535
PRIMARY RESIDENCE ☐ Own ☐ Parents ☐ Rent ☐ Other	CHECKING ☐ YES ☐ NO SAVINGS ☐ YES ☐ NO
PREVIOUS ADDRESS (if current address is less than 3 years) 28202 CABOT RD	CITY LAGUNA NIGEL STATE CA ZIP CODE 92677
EMPLOYER Self	BUSINESS PHONE (805) 639-4558
TIME WITH PRESENT EMPLOYER (10) YRS. ( ) MOS.	POSITION/ OCCUPATION Attorney / Mediator

ANNUAL HOUSEHOLD INCOME (BOTH APPLICANTS).* You may include pension, SSI, rental income and any other earnings. You do not need to include alimony, child support or separate maintenance if you do not wish to have it relied upon for this application.

$ 150,000.00 yr. SOURCE business income.

MONTHLY HOUSING PAYMENT $ 1,050	MY TOTAL MONTHLY CREDIT PAYMENTS ARE $ 1500.00 (excluding rent, mortgage, [illegible], etc.)

JOINT APPLICANT (if any) PRINT FIRST NAME, MIDDLE INITIAL, LAST NAME

DATE OF BIRTH (must be 18 years of age or older) / /	SOCIAL SECURITY NUMBER - -

X APPLICANT SIGNATURE Mari J. Frank DATE 10/13/95

X JOINT APPLICANT SIGNATURE (if any) DATE / /

Your 18.15%** variable introductory APR is good for the [illegible] from account open date. 1. If the assigned credit line is less than $1,000, a request for a cash advance will not be processed* 2. Minimum annual income required: $30,000. If your [illegible] is below that, please consider applying with a joint applicant. If your combined [illegible] is less than $30,000, but at least $12,000, your application may be processed for a [illegible]

Call or mail to accept your personal Private Reserve! To accept by phone, call (800) 356-3991. Please retain the letter for your records.

Exclusively For:	Reservation Number:	Offer Valid Until:	Immediate Cash Advance
Mari J. Frank 293 Estrella St. Ventura, CA 93003-1632	0180665 6303 I 02	August 30, 1996 JUL 19 1996	I would like an immediate cash advance of: ☐ $1,500 ☐ $2,000 ☐ $2,500 859815 JA Genuine security of PAYMENT PROTECTION just sign on the back of this Acceptance Certificate

Please make any name and/or address corrections above.

ABOUT YOU AND YOUR CREDIT REQUEST.

EMPLOYER Steven R. Kuhn & Assoc. OCCUPATION Attorney TOTAL HOUSEHOLD INCOME $ 300,000.00

BUSINESS PHONE (805) 643-1535 HOME PHONE (805) 641-9821 SOCIAL SECURITY NO.

SIGN HERE. I have read the important information about the Private Reserve Credit Line, Note 141963-300-00, on the reverse of the attached letter, and agree to its terms.

x Mari J. Frank 6-27-96

APPLICANT'S SIGNATURE DATE

UPON VERIFICATION AND ACCEPTANCE THE MINIMUM LINE AMOUNT WILL BE $2,500. THIS OFFER IS NOT TRANSFERABLE.

PLEASE PAY THE FOLLOWING ACCOUNTS WITH MONIES FROM MY PRIVATE RESERVE ACCOUNT.†

See Balance Transfer Information on reverse.

NAME AND BILLING ADDRESS OF FINANCIAL INSTITUTION	ACCOUNT NUMBER TO BE PAID	AMOUNT YOU WANT TRANSFERRED†
1. Capital One P.O. Box 85617 Richmond, VA 23276-0001	412174-1367552838	$ 585.58
		$

x Mari J. Frank

APPLICANT'S SIGNATURE DATE

9LA206

Senator FEINSTEIN. Thank you, thank you. Well, thank both of you, very much.

The testimony is very compelling, and I think everybody can see how it can happen to them.

As a matter of fact, you'd be interested to know, Mari, that my chief of staff in Washington was the victim one weekend. So it, it is happening.

Sheriff, let me, quickly ask you some questions, because I know you're busy, and I thank you very much for this, and being here.

This is the first strike force in the Nation, as far as I know. How many people are dedicated to it? How does it work? How much time does an investigation take?

Sheriff BACA. Let me introduce you to Lieutenant Jordan, if I may, Senator. He's the lead of that task force.

And would you please, as quickly as you can——

Senator FEINSTEIN. Lieutenant, welcome.

Lieutenant JORDAN. Good morning, Senator.

Sheriff BACA [continuing]. Answer her question.

Lieutenant JORDAN. There's four deputies assigned to the task force. There's a Lieutenant, me, and the way it works, is we work together with other law enforcement agencies.

We work together with the Highway Patrol, we work together with the Los Angeles Police Department.

Senator FEINSTEIN. And, now obviously, you cover the County, not the City.

But if, if someone has an identity theft, and they live in the county, they would then report it to the Sheriff's Department? And report it to your task force?

Lieutenant JORDAN. Yes. Sheriff Baca made a decision, about a year and a half ago, to assist the victim, so that they could report their theft of identity to the local sheriff's department substation.

Whether the crime occurred in Connecticut, they could go to a sheriff's station, say, in the city of Temple, report the crime and begin the process of recovering their identity.

Senator FEINSTEIN. Now I, I guess people from the city of L.A., still would go to the police department to report the crime, right?

Lieutenant JORDAN. Yes, based on, based on what the Sheriff did, then Gil Garcetti, the District Attorney, made a policy decision that the Los Angeles Police Department, and the Los Angeles County Sheriff's Department, would take those first reports.

Senator FEINSTEIN. Ah-hah. So, can someone from L.A. City go into a sheriff's department, and report it?

Sheriff BACA. Yes, we can cover each other's jurisdictions, to start the process.

So, a city resident can come to a sheriff's station and start a process, or a county resident go to a police station and start the process.

Ideally, it would be that if you reside in the City of Los Angeles, you can go to a police station. If you reside in sheriff's territory, you go to a sheriff's station.

But we are combining our effort, through this task force endeavor, and we believe that more can be done, if the staffs of both these departments were combined under one roof.

And of course, we're at the early stages of this task force effort, and that's why I'm recommending to you that we further increase the staffing, by bringing in these Federal agencies, as well.

This is not unprecedented. We do this with Asian crimes that we investigate, we do this with narcotics cases that we investigate, and there are even other specialty offenses, that occur in the jewelry business, that require us to have this collaboration between Federal, State and local municipal law enforcement.

And how long does it take for one of these cases to be investigated, by the way? The Senator asked that question.

Lieutenant JORDAN. They can take as little as 60 hours, and as much as a 1,000 hours.

Primarily, because that they cross jurisdictional lines, they cross county lines, State lines and Federal lines. We've even investigated cases that are crossing international borders.

Once you get into it, you see that it's like a spider web. It just keeps growing and growing.

Senator FEINSTEIN. Right, right. Now, and that's the interstate aspect of this. I think makes your request a legitimate request, Sheriff.

And we have Social Security here, and we have Postal Services here, and perhaps they can comment in their testimony, on this request.

Does LAPD assign officers to the strike force? Or are the four, you have four Sheriff's deputies.

Sheriff BACA. Sheriff's deputies. Currently, they're working independent of our team.

However, there is communication back and forth between the two offices. So, in effect, although we're not housed together, we are operating in a collaborative effort.

Senator FEINSTEIN. How many cases do you have at present, under investigation?

Lieutenant JORDAN. Currently, we have, as of today, approximately eighteen hundred and fifty cases, so far reported this year, to the L.A. County Sheriff's Department, alone.

Senator FEINSTEIN. How many, or I don't know if you have this broken down, but how many of them would you say are fraud, in terms of money, and how many of them are aimed at things like stalking and violence?

Lieutenant JORDAN. The majority of the ones that we receive, Senator, are the frauds, for money.

Senator FEINSTEIN. My finding is also that fraud represents the majority of cases right now. That's not to say that stolen personal information can't be used for a violent crime, but generally it's in this area of money fraud.

Lieutenant JORDAN. Exactly.

Senator FEINSTEIN. Right, OK.

Lieutenant JORDAN. Also, to piggyback, Senator, on one of the questions you asked earlier, one of the things that we're going to propose to the International Association of Chiefs of Police meeting at San Diego, later this year, is that all the chiefs of police, across the Nation, develop the same policy that Sheriff Baca started and that Gil Garcetti furthered, and that is to have the individual cit-

izen that lives in that jurisdiction, be able to walk into that local police station or sheriff's station and initiate that first report.

Senator FEINSTEIN. Right. Because, it's very difficult. All, all of the testimony that I've received, it's very difficult for people to get law enforcement to take them seriously.

And then second, it's difficult for people to really regain their identity. The Senate Judiciary Committee that received testimony in Washington from a young woman in San Diego County, who had her identity stolen. A year after she reported the theft, she went to Mexico on a vacation, and Customs wouldn't let her back into the United States.

And she was alone and she had to prove that she wasn't who Customs said she was, because the person committing this identity theft had a criminal record, and therefore, she was accused of having that criminal record.

So, a critical step in how government can, from a law enforcement point of view, really restore somebody's legitimate identity, across all of the lines that it has to be restored. Identity theft is not only local.

A victim has problems with events, like coming back into the country, if one's name happens to get on a list, because they think you're someone else.

Sheriff BACA. Well, exactly, and the testimony from the two victims that we heard addresses that point more succinctly, and that is they're like a football, where they're being moved one part of the field to the next part of the field.

And at some point, somebody has to say, we'll start it right here, and we were not gonna pass this off to another agency, because the victim, in terms of the dollar amount lost was in a bank out of State.

And that's the problem here. It's an international, national scope of the problem itself.

Senator FEINSTEIN. Sheriff, I hope you can say a little bit, for this testimony.

So, I'm going to not ask Selene and Mari questions right now, but move along, because I think it's important that this record be intact.

And let me just now welcome the second panel of witnesses. Jerry Klurfeld represents the Federal Trade Commission (FTC).

He's an independent law—well FTC is an independent law enforcement agency, charged by Congress with protecting American consumers from unfair methods of competition, and unfair and deceptive acts and practices in the marketplace.

Pursuant to the Identity Theft Assumption and Deterrence Act, the FTC is today the Federal Government's central repository, for identity theft complaints, and is charged with providing victim assistance.

Mr. Klurfeld is Regional Director of the Western Region of the FTC. He was appointed to this position, which embraces California, Arizona and Nevada, Hawaii, Colorado and Utah, in 1990.

Mr. Klurfeld, we'd like to hear from you, if you would.

PANEL CONSISTING OF JEFFREY A. KLURFELD, DIRECTOR OF WESTERN REGIONAL OFFICE, FEDERAL TRADE COMMISSION, JANE VEZERIS, DEPUTY INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION; AND MICHAEL E. AHERN, DEPUTY CHIEF INSPECTOR, FIELD OPERATIONS WEST, U.S. POSTAL INSPECTION SERVICE

STATEMENT OF JEFFREY A. KLURFELD

Mr. KLURFELD. Thank you, Senator.

I appreciate the opportunity to present the Federal Trade Commission's views on the important issue of identity theft, and describe to you the commission's efforts to help victims, alert industry and equip law enforcement, to deal with this heart-rending crime.

Senator, we applaud your efforts to combat this serious problem that injures so many consumers, and we also endorse your determined legislative efforts to protect the public against this pernicious problem.

As you aptly noted, this type of fraud, like so many types of fraud, is really opportunistic.

In my remarks today, I will discuss the growing phenomenon of identity theft, briefly, and the measures the commission has taken, to meet the goals of the Identity Theft Act.

The fear of identity theft has gripped the public as few commission, consumer issues have. This is in part because it seems to be widespread, and in part, because the consequences can be so devastating.

Consumers feel particularly vulnerable, knowing that no matter how careful they are, they may nonetheless become identity theft victims.

The Identity Theft Act addressed these concerns in several concrete ways. As, Senator you noted, it directed the Federal Trade Commission to establish the Federal Government's central repository for identity theft complaints, and to provide victim assistance and consumer education.

The identity theft clearinghouse, our toll-free hotline phone counselors and our consumer education campaign have helped the FTC begin to address the serious problems associated with identity theft.

As the commission staff has strived to meet the responsibilities of this act, we have learned much about the crime, its victims and its perpetrators.

Let me now address what our clearinghouse tells us about identity theft in California.

The Identity Theft Act recognized the importance of creating a single repository for identity theft complaints.

Accordingly, we established this clearinghouse to collect and consolidate these complaints. We are already seeing the fruits of this effort.

The data from these complaints are illuminating. The basic complaint data showed that the most common forms of identity theft reported by California consumers, during the first 9 months of operation were credit card fraud, approximately 50 percent of consumers reported this type of fraud, and this is where an account

is opened in their name, or there is a takeover of their existing credit card account.

Communication services and 28 percent reported this where the identity thief opened up telephone, cellular or other utility services in their name.

Bank fraud, approximately 17 percent reported that a checking or savings account had been opened in their name.

Fraudulent loans, representing about 10 percent, the victims and government documents or benefits, approximately 8 percent reported that the identity theft had obtained government documents, or benefits, such as a driver's license, or file documents, such as a tax return in their name.

Not surprisingly, the States with the largest populations account for the largest numbers of complainants and suspects, and Senator as you noted correctly, California is the State with the highest number of complainants.

About 60 percent of California victims calling us identify their age, and I can report that data to you later, if you wish.

Commission staff is also assessing the data on the monetary impact of this theft.

Some complainants provided estimates of the dollar amounts obtained by the thief, because they have received the resulting bills, or had been notified of the resulting bad debts.

California consumers reported a total monetary loss of approximately $18 million, and the range of dollar amounts reported by these consumers in California varies widely.

For example, 12 percent of complainants reported theft, totaling between $5,000 and $10,000, 16 percent of complainants reported theft of over $10,000.

The data also reveal information about the perpetrators. Almost 60 percent of the complainants provided some identifying information about the identity thief, such as a name, address or even a phone number.

Los Angeles was the most common location for suspects, reported by California consumers.

It was reported more than 3 times more often than the next most common location, which is Oakland.

Consumers also report the harm to their reputation or daily life.

The most common, non-monetary harm reported by consumers is damage to their credit report through derogatory, inaccurate information.

Forty-nine percent of California consumers reported that they were harmed in this matter. This negative credit information leads to the other problems, most commonly reported by victims, including loan denials, bounced checks, rejection of credit cards.

Identity theft victims also report repeated contacts by debt collectors for the bad debt incurred by the identity thief.

Many consumers reported that they have to spend significant amounts of time resolving the problems caused by identity theft.

The commission has made great strides in assisting consumers and law enforcement to combat identity theft, but recognizes that much remains to be done.

Earlier this year, the Identity Theft Prevention Act of 2000 was introduced in the Senate, and this would effectively address many

areas of identity theft vulnerability, and protect many consumers from becoming victims of this very serious crime.

The Federal Trade Commission strongly supports this legislation, and we'd like to thank you for the opportunity to participate in this important hearing. Thank you.

[The prepared statement of Jeffrey A. Klurfeld follows:]

PREPARED STATEMENT OF JEFFREY A. KLURFELD

Senator Feinstein, I am Jeffrey Klurfeld, Director of the Weston Regional Office of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on the important issue of identity theft and describe to you the Commission's efforts to help victims, alert industry, and equip law enforcement to deal with this harrowing crime. In my remarks today, I will discuss the growing phenomenon of identity theft, the measures the Commission has taken to meet the goals of the Identity Theft and Assumption Deterrence Act ("the Identity Theft Act"),[2] and what we see as the major challenge for the coming year in combating identity theft.

The fear of identity theft has gripped the public as few consumer issues have. This is in part because it seems to be widespread and in part because the consequences can be devastating. Consumers feel particularly vulnerable knowing that no matter how careful they are, they may nonetheless become identity theft victims.[3]

The Identity Theft Act addressed these concerns in several concrete ways. It directed the Commission to establish the federal government's central repository for identity theft complaint, and to provide victim assistance and consumer education. As the Commission staff have strived to meet the responsibilities of the Identity Theft Act, we have learned much about the crime, its victims and its perpetrators.

I. MEETING THE GOALS OF THE IDENTITY THEFT ACT

In earlier testimony before this Committee, the Commission describe the ways in which we have carried out our responsibilities under the 1998 Identity Theft Act.[4] We have continued to build on these achievements.

A. Centralized Complaint Handling—877 ID THEFT

The Commission established its toll-free telephone number, 1–877–ID THEFT (438–4338) to help consumers avoid or resolve identity theft problem. In addition to advising consumers, counselors enter consumer complaint information into the centralized Identity Theft Data Clearinghouse used to aid law enforcement and prevent identity theft.

The identity Theft hotline has been in operation since November 1, 1999. Calls answered have more than tripled in the last six months.[5] About two thirds of the calls are from victims, with the remaining calls coming from consumers who are looking for information on ways to minimize their risk of identity fraud.

The telephone counselors provide victims of identity theft with specific information about how to try to prevent additional harm to their finances and credit histories. Callers are advised to contact each of the three national consumer reporting agencies to obtain copies of their credit. reports and request that a fraud alert be placed on their credit reports.[6] Fraud alerts request that the consumer be contacted

---

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any Commissioner.

[2] Pub. L. No. 105–318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

[3] Data from the Identity Theft Clearinghouse, our central repository of identity theft complaints, bear out these fears. See discussion at pp.7–10.

[4] The Commission testified before this subcommittee on March 7, 2000. We also testified before this subcommittee in May 1998 in support of the Act. Following the passage of the Act the Commission testified again, in April 1999, before the House Subcommittee on Telecommunications, Trade and Consumer Protection and the Subcommittee on Finance and Hazardous Materials of the Commerce Committee. That testimony focused on identity theft in the financial services industry.

[5] The hotline received an averaged of more than 1000 calls per week in the month of July.

[6] The three national consumer reporting agencies are Equifax Credit Information Services, Inc., Experian Information Solutions, Inc., and Trans Union, LLC.

when new credit is applied for in that consumer's name.[7] The phone counselors also explain how to review carefully the information on credit reports to detect any additional evidence of identity theft. The counselors also inform callers of their rights under the Fair Credit Reporting Act,[8] and provide them with the procedures for correcting their credit reports. The counselors advise consumers to contact each of the creditors or service providers where the identity thief has established or accessed an account, and to follow up in writing by certified mail, return receipt requested. Consumers are also advised on how to take advantage of their rights under the Fair Credit Billing Act,[9] and the Truth in Lending Act,[10] which, among other things, limits their responsibility for unauthorized charges to fifty dollars in most instances. Consumers who have been contacted by a debt collector concerning debts incurred by the identity thief are advised of their rights under the Fair Debt Collection Practices Act,[11] which limits debt collectors' practices in the collection of debts.

In addition, the FTC phone counselors advise consumers to notify their local police departments, both because local law enforcement may be in the best position to catch and bring the perpetrator to justice and because a police report is among the best means of demonstrating to would-be creditors and debt collectors that a consumer is a genuine victim of identity theft. More than half the states have enacted their own identity theft laws, and our counselors, in appropriate circumstances, will refer consumers to other state and local authorities for potential criminal investigation or prosecution.

B. Outreach and Consumer Education

The FTC also reaches consumers through the Internet. The FTC's identity theft website—*www.consumer.gov/idtheft*—gives tips on how consumers can guard against identity theft, warns consumers about the latest identity theft schemes and trends, and provides access to consumer education materials on identity theft. This website has received more than 139,000 hits from November, 1999 through July, 2000. The site also links to a secure complaint form on which identity theft victims can enter the details of their complaints online, allowing consumers to contact the Commission at all times. After review by FTC staff, these complaints are entered into the Clearinghouse. To date we have received more than 1900 complaints through this electronic form. Further, the Federal Trade Commission has distributed nearly 100,000 copies of the comprehensive consumer guide: ID Theft: When Bad Things Happen to Your Good Name. Developed in consultation with more than a dozen federal agencies,[12] this booklet provides consumers with practical tips on how best to protect their personal information from identity thieves, summarizes the various federal statutes that protect consumer victims of identity theft, and details the victim assistance mechanisms available.[13]

C. Identity Theft Clearinghouse—Launched Online

The Identity Theft Act authorized the Commission to establish a central repository of consumer complaints about identity theft, and to refer appropriate cases to law enforcement for prosecution. The Identity Theft Complaint Database, which was activated in November 1999, provides law enforcement with specific investigative material and also allows our public and private sector partners to examine larger, trend-based information to determine ways to reduce the incidence of identity theft. Currently, the Clearinghouse contains data from consumers who contact the FTC through the toll free number or website. We are pursuing ways to collect complaint

---

[7] In addition to fraudulently acquiring accounts or loans, the identity thieves also may register a change of address in the victim's name, routing bills and other correspondence to a different address. In that way, it may take months for the victim to realize that their identity has been hijacked.

[8] 15 U.S.C. §§ 1681 et seq.

[9] 15 U.S.C. § 1666. The Fair Credit Billing Act generally applies to "open end" credit accounts, such as credit cards, revolving charge accounts, and overdraft checking accounts. It does not cover installment contracts, such as loans or extensions of credit that are repaid on a fixed schedule.

[10] 15 U.S.C. § 1601 et seq.

[11] 15 U.S.C. §§ 1692 et seq.

[12] These include: Department of Justice; Federal Bureau of Investigation; Federal Communications Commission; Federal Deposit Insurance Corporation; Federal Reserve Board; Internal Revenue Service; National Credit Union Administration; Office of the Comptroller of the Currency; Office of Thrift Supervision; Social Security Administration; United States Postal Inspection Service; United States Secret Service; United States Securities and Exchange Commission; and United States Trustee.

[13] The Federal Trade Commission expects to receive a second, and larger, printing of the booklet shortly. The Social Security Administration and the Federal Deposit Insurance Corporation have also printed and distributed When Bad Things Happen. The FTC has provided the booklet on zip disk to other agencies who are interested in printing additional copies.

data from other agencies and private sector entities to allow Clearinghouse users to see as much identity theft complaint data as possible.[14]

With a database as rich as the Clearinghouse should become, Commission staff can and do refer cases for potential prosecution. To maximize use of the data, the Commission now provides law enforcement partners with direct access to the Clearinghouse through Consumer Sentinel, a secure website for sharing complaints and other information with consumer protection law enforcers. Starting this month, law enforcement and appropriate regulatory offices can access the Clearinghouse through their desktop computers. This access will enable them to readily and easily spot identity theft problems in their own backyards and to coordinate with other law enforcement officers when the database reveals common schemes or perpetrators. The FTC staff will continue to comb through the data to spot cases for referral, but has also enabled others to use the data to ferret out the bad actors for prosecution.

The Identity Theft Act also authorized the Commission to share complaint data with "appropriate entities,"[15] including the three national consumer reporting agencies and others in the financial services industry. The Commission does not envision providing access to the complete database for these private sector entities because unfettered access could interfere with law enforcement efforts. FTC data analysts can, however, identify patterns that reveal a business or business practice that exposes consumers to a high risk of identity theft. Commission staff will forward appropriate information about these complaints to the entities involved so they can evaluate and revise those practices. Similarly, staff plans to share complaint data with a business if data reveal that business fails to respond to legitimate consumer complaints about identity theft or frustrates consumers' efforts to correct misinformation on their credit reports.

II. WHAT THE CLEARINGHOUSE TELLS US ABOUT IDENTITY THEFT IN CALIFORNIA

We are already seeing the fruits of collecting and analyzing identity theft complaints in a single repository. The basic complaint data show that the most common forms of identity theft reported by California consumers during the first nine months[16] of operation were:[17]

- *Credit Card Fraud*—Approximately 50% of consumers reported credit card fraud—i.e., a credit card account opened in their name or a "takeover" of their existing credit card account;
- *Communications Services*—Approximately 28% reported that the identity thief opened up telephone, cellular, or other utility service in their name;
- *Bank Fraud*—Approximately 17% reported that a checking or savings account had been opened in their name, and/or that fraudulent checks had been written;
- *Fraudulent Loans*—Approximately 10% reported that the identity thief obtained a loan, such as a car loan, in their name; and
- *Government Documents or Benefits*—Approximately 8% of consumers reported that the identity thief had obtained government documents or benefits (such as a driver's license) or filed documents (such as a tax return) in their name.[18]

Not surprisingly, the states with the largest populations account for the largest numbers of complainants and suspects. California, New York, and Florida, in descending order, represent the states with the highest number of complainants. About 60% of California victims calling the identity theft hotline report their age. Of these, approximately 41% fall between 30 and 44 years of age. Approximately 24% are between age 45 and 64, and 25% are between age 19 and 29. About 7% of those reporting their ages are 65 and over; and slightly over 2% are age 18 and under.

The data also reveal information about the perpetrators. Almost 60% of the caller-complainants provided some identifying information about the identity thief, such

---

[14] Our Consumer Sentinel database, which houses consumer fraud complaints, receives complaint data from Better Business Bureaus, consumer outreach organizations and others. The Commission is looking to replicate this approach with identity theft complaints.

[15] The Identity Theft Assumption and Deterrence Act provides, in pertinent part, "the Federal Trade Commission shall establish procedures to . . . refer [identity theft] complaints . . . to appropriate entities, which may include referral to . . . the 3 major national consumer reporting agencies." 18 U.S.C. Sec. 1028 (note).

[16] The data analysis covers the period from November 1, 1999 through July 31, 2000.

[17] Many consumers experience more than one type of identity theft. Therefore, the percentages represent the number of consumers who reported each type of identity theft.

[18] These statistics reflect complaints made by California consumers. However, nationwide statistics are similar: 54% Credit Card Fraud; 26% Communications Services; 17% Bank Fraud; 11% Fraudulent Loans; and 8% Government Documents or Benefits.

as a name, address, or phone number. Los Angeles was the most common location for suspects reported by California consumers; it was reported more than three times more often than Oakland, the next most common location.

Commission staff also are assessing the data on the monetary impact of identity theft. Some complainants provided estimates of the dollar amounts obtained by the thief, because they have received the resulting bills or been notified of the resulting bad debts. The range of dollar amounts reported by California consumers varies widely, with approximately 30% of complainants reporting theft of under $1,000; approximately 31% of complainants reporting theft totaling between $1,000 and $5,000; approximately 12% of complainants reporting theft totaling between $5,000 and $10,000; and approximately 16% of complainants reporting theft of over $10,000. California consumers reported a total monetary loss of nearly $18 million.

Consumers also report the harm to their reputation or daily life. The most common nonmonentary harm reported by consumers is damage to their credit report through derogatory, inaccurate information. Forty-nine percent of California consumers reported that they were harmed in this manner. This negative credit information leads to the other problems most commonly reported by victims, including loan denials, bounced checks, and rejection of credit cards. Identity theft victims also report repeated contacts by debt collectors for the bad debt incurred by the identity thief. Many consumers report that they have to spend significant amounts of time resolving these problems.

Consumers also report problems with the institutions that provided the credit, goods, or services to the identity thief in the consumer's name. These institutions often attempt to collect the bad debt from the victim, or report the bad debt to a consumer reporting agency, even after the victim believes that he or she has shown that the debt is fraudulent. Consumers further complain that these institutions' inadequate or lax security procedures failed to prevent the identity theft in the first place; that customer service or fraud departments were not responsive; or that the companies refused to close or correct the unauthorized accounts after notification by the consumer.

III. NEXT STEPS

A. The Identity Theft Prevention Act of 2000, S. 2328

The Commission has made great strides in assisting consumers and law enforcement to combat identity theft, but recognizes that much remains to be done. Earlier this year, the Identity Theft Prevention Act of 2000, S. 2328, was introduced in the Senate. This Act would effectively address many areas of identity theft vulnerability and would protect many consumers from becoming victims of this very serious crime. Under S. 2328, consumers will have access to information that may reveal indicia of identity theft or the source of erroneous information resulting from identity theft. These measures will enable consumers to better protect themselves against identity theft and avoid some of the frustrations that often accompany their efforts to undo the harm inflicted by the identity thief. Providing for free annual credit reports and requiring that credit card issuers advise consumers of requests for changes of address to credit accounts will help consumers help themselves. Further, requiring clear and conspicuous fraud alerts on credit reports will help to thwart the ability of identity thieves to commit ongoing fraud. The Commission is confident that these proposals will assist consumers who contact the Commission's Identity Theft Data Clearinghouse to describe the problems they encounter attempting to prevent and remedy identity theft.

B. Victim Assistance Workshop

The Commission will soon begin sharing certain limited information from its Identity Theft Clearinghouse with banks, creditors and other businesses whose practices are frequently associated with identity theft complaints. The goal is to encourage and enable industry and individual companies to develop better fraud prevention practices and consumer assistance techniques. To that end, the Commission will convene a workshop for industry, consumer groups, the public, and law enforcement on Identity Theft victim assistance, prevention, and prosecution on October 23–24, 2000. This workshop follows the National Summit on Identity Theft of March, 2000, which initiated a dialogue between the public and private sectors on identity theft. The Social Security Administration, the Department of Justice and the U.S. Secret Service will convene later workshops on identity theft prevention and prosecution.

IV. CONCLUSION

The Identity Theft Clearinghouse, the toll free hotline phone counselors, and the consumer education campaign have helped the FTC begin to address the serious

problems associated with identity theft. While more work remains to be done, the Commissions is optimistic that heightened awareness by consumers and businesses will help reduce the occurrences of this fraud. The FTC looks forword to working with the Subcommittee to find additional ways to prevent this crime and to assist its victims.

INFORMATION ON IDENTITY THEFT
FOR CONSUMERS IN CALIFORNIA
FROM NOVEMBER 1999 TO JULY 2000

FEDERAL TRADE COMMISSION

AUGUST 22, 2000

INFORMATION ON IDENTITY THEFT FOR CONSUMERS IN CALIFORNIA FROM NOVEMBER 1999 TO JULY 2000

Customer Service

Since the Identity Theft database was launched in November 1999, the Federal Trade Commission has processed 2,783 entries from consumers in California. Of these entries, 62% are complaints and 38% are inquiries. Consumers in California contacted the Federal Trade Commission in a variety of ways but the most common mode of contact was by phone: 84% of the entries were received by phone, 13% of the entries were received through the internet, and 3% of the entries were received by mail.

Consumer Information

Consumers located in the following cities in California provided the most number of complaints:

Consumer City	No. of Complaints
Los Angeles	155
San Diego	76
San Francisco	67
Sacramento	51
Oakland	35

Approximately, 60% of the consumers in California registering a complaint reported their age. The following table provides the age distribution of these consumers:

Consumer's Age	No. of Complaints	Percentage*
65 and up	76	7.4%
45-64	249	24.1%
30-44	428	41.4%
19-29	257	24.9%
18 and under	24	2.3%
Total No. of Complaints Where the Consumer Reported His/Her Age	1034	

*Percentage is based upon the total number of complaints where consumers reported his/her age.

Suspect Information

About 59% of the consumers from California registering a complaint provided some identifying information about the suspect such as a name, address, or phone number. Consumers reported the following cities in California to be the top suspect locations:

Suspect City	No. of Complaints
Los Angeles	218
Oakland	62
San Francisco	38
San Diego	31
Inglewood	29

Types of Identity Theft

The following are the most common types of identity theft complaints reported by California consumers*:

- *Credit Card Fraud*: 50% of consumers reported that a credit card was opened in their name or unauthorized charges were placed on their existing credit card.
- *Unauthorized Phone or Utility Services:* 28% of consumers reported that the identity thief had established a new telephone, cellular, or other utility service in their name.
- *Bank Fraud:* 17% of consumers reported that a new bank account had been opened in their name, fraudulent checks had been written, or unauthorized withdrawals had been made from their account.
- *Fraudulent Loans:* 10% of consumers reported that the identity thief had obtained a loan (personal, business, auto, real estate, etc.) in their name.
- *Government Documents or Benefits:* 8% of consumers reported that the identity thief had obtained government documents or benefits such as a driver's license or filed documents such as a tax return in their name.

---

* Many consumers experience more than one form of identity theft. Therefore, the percentages represent the number of consumers who are subject to the particular injury.

Harm Suffered

Monetary Injury

California consumers reported a total monetary injury of $17,979,339 resulting from identity theft.* The following table illustrates the dollar amounts obtained by the identity thief as reported by California consumers:

Amount Obtained by Identity Thief	**No. of Complaints**	**Percentage***
$10,001 or more	176	15.9%
$5,001-10,000	136	12.3%
$1,001-5,000	339	30.6%
$1,000 or less	328	29.6%
$0	129	11.6%
Total No. of Complaints Reporting Amount Stolen	1108	
Percentage of Consumers Reporting Amount Stolen	63.7%	

*Percentage is based upon the total number of complaints where consumers reported the amount obtained by the identity thief.

Non-monetary Injury

The most common non-monetary harm reported by California consumers as a result of identity theft is damage to their credit report through derogatory or inaccurate information: 49% of consumers report that they have been harmed in this manner. Other ways California consumers have suffered as a result of identity theft include: time spent resolving the problems caused by identity theft (13%), harassment by debt collectors or creditors (10%), and loan denials (7%).

---

* This sum reflects the amount obtained by the identity thief through fraudulent means. However, consumers also frequently suffer indirect monetary harm such as loss of income and legal fees.

Senator FEINSTEIN. Thanks very much, Mr. Klurfeld.

I'd like to introduce Jane Vezeris, the Deputy Inspector General of the Social Security Administration.

She has served as Deputy Inspector General since January 3 of this year.

Prior to this position, she had a distinguished career with the U.S. Secret Service.

She held a number of supervisory positions in the service, including Special Agent, in charge of the Intelligence Division, and Deputy Assistant Director in the Office of Public Affairs, and the Office of Investigations.

Her last position at the Secret Service was as Assistant Director, Office of Administration, and as such, she served as the Chief Financial Officer.

Welcome, I look forward to your comments.

STATEMENT OF JANE VEZERIS

Ms. VEZERIS. Thank you, good morning.

Senator FEINSTEIN. Good morning.

Ms. VEZERIS. Thank you for the opportunity to be here today, and discuss our office's continuing fight against identity theft.

Your interest in the issue has already been instrumental in reducing identity theft, and your continuing commitment gives us reason to be optimistic that our ongoing efforts will be even more successful, so thank you.

As you know, the enactment of the Identity Theft Act of 1998, introduced by your subcommittee was the first piece of comprehensive legislation, aimed at what is rapidly becoming the most popular and insidious crime of the new century.

In the 2 years since, we've learned that the problem is larger than anyone realized and that additional legislation must be enacted, if law enforcement is to keep pace with identity thieves.

Two bills introduced by you and the subcommittee are important steps in the right direction, and we look forward to working with you, to make both Senate Bills 2328 and 2699 important laws in this crusade.

The need for such legislation cannot be understated. The stories of the victims of identity theft, such as those that have testified here today, are heart-rending.

The stories of the perpetrators themselves can sometimes be absolutely shocking. And perhaps one of the most enterprising identity thieves we've come across recently hails from Southern California.

Our agents in San Diego were alerted, when a local law enforcement individual became suspicious, as to the validity of a Social Security number presented by a man they were questioning.

Our query of Social Security Administration records revealed that the number actually was assigned to a seventy year old woman in South Dakota.

Our agents quickly discovered that this man had been a fugitive felon for 17 years, with four prior felony convictions, including prison escape.

He had created through the use of fraudulently obtained or counterfeited identification documents, 33 separate and distinct identities.

Some of these were stolen, while others were entirely fictitious. Either way, he was able to use them, not only to avoid capture, but to, excuse me, to obtain employment as the Chief of a Fire Department, the Security Chief for a County Fair, and other significant positions of trust.

He was also able to commit bank fraud, by obtaining credit cards and loans under his assumed aliases, while receiving Social Security benefits under three of his identities.

This individual was recently the subject of a 14-count Grand Jury Indictment, and further criminal proceedings remain pending.

He illustrates the extent to which one individual can steal and create identities, capable of fooling banks, employers and even government agencies.

While most of our identity theft cases are not this extraordinary, this man's exploits certainly are not isolated occurrences.

In California alone, we've opened 42 identity theft investigations, since last October, and we've obtained 20 convictions.

These represent only the most egregious cases, those that we chose to investigate, based on our limited resources.

In fiscal year 1999, 62,000 of the 75,000 allegations that we receive involve some form of Social Security number misuse.

These numbers led us to launch Social Security number misuse pilot projects, in five cities across the country, in which our agents work jointly with Federal, State, and State local law enforcement agencies, to target perpetrators of identity crimes and Social Security number misuse.

Already, these pilots have been successful, and we've opened 197 investigations, resulting in 61 convictions, and clearly I can add that our experience supports Chief Baca's enthusiasm for having a comprehensive approach, a team approach in, in tackling this issue.

The ever-increasing number of identity theft incidents has exploded, as the Internet has offered new and easier ways for individuals to obtain false identification documents, including Social Security numbers.

To combat this, we've expanded the scope of these pilots to include undercover sale and purchase of Social Security cards, over the Internet.

Hopefully, this will enable us, for the first time, to determine the scope of the Internet trafficking of false identification documents.

As considerable as our efforts have been, much remains to be done.

Senate Bills 2328 and 2699 are important steps, in that they provide law enforcement with additional tools.

I am particularly pleased with the additional civil monetary penalty provisions, contained in S. 2328.

Civil monetary penalties have proven to be a highly effective tool, in the many cases that are not accepted for criminal or civil, criminal prosecution or civil action.

I am also pleased to see that Senate Bill 2699 recognizes the importance of formally distinguishing between valid and invalid transfers of Social Security number information.

While we have some concerns, with respect to certain enforcement mechanisms in the current draft, we stand ready to work with your staff, to make both bills more effective in the war against identity theft, and to protect consumers on the front end.

Congress should take an aggressive approach, by providing comprehensive criminal, civil and administrative sanctions, for the sale, purchase and misuse of Social Security numbers, which are quite often at the core of identity theft crimes.

I thank you for commitment to doing so, and offer the Inspector General's assistance, in reaching our common goal.

[The prepared statement Jane E. Vezeris follows:]

PREPARED STATEMENT OF JANE E. VEZERIS

Good morning, Senator. Thank you for the opportunity to appear today and discuss the Social Security Administration, Office of the Inspector General's continuing fight against Identity Theft. Your interest in the issue has already been instrumental in reducing identity theft, and your continuing commitment gives us reason to be optimistic that our ongoing efforts will be even more successful.

As you know, the enactment of the Identity Theft Assumption and Deterrence Act of 1998, introduced by your Subcommittee on Technology, Terrorism and Government Information, was the first piece of comprehensive legislation aimed at what is rapidly becoming the most popular and most insidious crime of the new century. In the 2 years since, we've learned that the problem is larger than anyone realized, and that additional legislation must be enacted if law enforcement is to keep pace with identity thieves. Two bills introduced by you and the subcommittee are important steps in the right direction. We look forward to working with you to make Senate Bills 2328 and 2699 important laws in their crusade.

The need for such legislation cannot be understated. The stories of victims of identity theft, such as those that testified here today, are heart-rending. The stories of the perpetrators themselves can be absolutely shocking. Perhaps one of the most enterprising identity thieves we've come across hails from southern California.

Our agents in San Diego were alerted when local law enforcement became suspicious as to the validity of a Social Security number presented by a man they were questioning. Our query of the Social Security Administration's records revealed that the Social Security number was actually assigned to a 70-year-old woman from South Dakota.

Our agents quickly discovered that this man had been a fugitive felon for 17 years, with four prior felony convictions including prison escape. He had created, through the use of fraudulently obtained or counterfeited identification documents, 33 separate and distinct identities. Some of these were stolen, while others were entirely fictitious. Either way, he was able to use them not only to avoid capture, but to obtain employment as the chief of a fire department, the security chief for a county fair, and other positions of trust. He was also able to commit bank fraud by obtaining credit cards and loans under his assumed identities while receiving Social Security benefits under three of his identities.

This individual was recently the subject of a 14-count grant jury indictment, and further criminal proceedings remain pending. He illustrates the extent to which one individual can both steal and create identities capable of fooling banks, employers, and even government agencies.

While most of our identity theft cases are not this extraordinary, this man's exploits certainly are not isolated occurrences. In California alone, we've opened 42 identity theft investigations since last October, and have obtained 20 convictions. These represent only the most egregious cases-those that we chose to use our limited resources to investigate.

In Fiscal Year 1999, 62,000 of the 75,000 allegations we received involved some form of Social Security number misuse. These numbers led us to launch Social Security number misuse pilot projects in five cities across the nation, in which our agents work jointly with Federal and State law enforcement agencies to target perpetrators of identity crimes and Social Security number misuse. Already, these pilots have achieved an unparalleled success, opening 197 investigations resulting in 61 convictions in the first year.

The ever-increasing number of identity theft incidents has exploded as the Internet has offered new and easier ways for individuals to obtain false identification documents, including Social Security cards. To combat this, we've expanded the scope of these pilots to include the undercover sale and purchase of Social Security cards over the Internet. This will enable us, for the first time, to determine the scope of Internet trafficking in false identification documents.

As considerable as our efforts have been, much remains to be done. Senate Bills 2328 and 2699 are important steps in that they provide law enforcement with additional tools. I am particularly pleased with the additional Civil Monetary Penalty provisions contained in Senate Bill 2328. Civil Monetary Penalties have proven to be a highly effective tool in the many cases that are not accepted for criminal prosecution or civil action. I am also pleased to see that Senate Bill 2699 recognizes the importance of formally distinguishing between valid and invalid transfers of Social Security number information. While we have some significant concerns with respect to certain enforcement mechanisms in the current draft of the Bill, we stand ready to work with your staff to make both Bills more effective in the war against identity theft.

Congress should take an aggressive approach by providing comprehensive criminal, civil, and administrative sanctions for the sale, purchase, and misuse of Social Security numbers, which are quite often the starting point for identity theft crimes. I thank you for your commitment to doing so. and offer the Inspector General's assistance in reaching our common goal. Thank you.

Senator FEINSTEIN. Thank you very much. At the appropriate time, I'll ask you about what enforcement provisions you have concerns about. So, we'll get to that.

I'd now like to introduce our last witness, Mr. Michael Ahern, U.S. Postal Inspection Service.

Mr. Ahern represents the Postal Inspection Service. He's been with the U.S. Postal Service for 27 years. He began his inspection career as a U.S. Postal Inspector in Detroit.

He progressed through a series of management positions in Washington. He was promoted to Assistant Inspector in charge, in the Los Angeles Division, then to Postal Inspector in charge, in the Boston Division.

He became Deputy Chief for Western Field Operations, this year.

Welcome, Mr. Ahern.

STATEMENT OF MICHAEL E. AHERN

Mr. AHERN. Thank you Senator, and good morning.

It's a pleasure to appear here this morning before you, and the Subcommittee on Terrorism—Technology, Terrorism and General Government.

On behalf of the Chief Postal Inspector, I want to thank you for holding these hearings on identity fraud, the fastest growing crime in America.

It's also a pleasure to appear here, to discuss the role of the Postal Inspection Service in these endeavors, and I'd also like to let you know that the Postal Inspection Service is very supportive of your Senate Bill 2328 and Senate Bill 2699 that addressed the identity theft issues.

Many of the crimes connected with, connected with identity theft, involve mail fraud or mail theft.

To give you kind of an overview nationally, postal inspectors make approximately ten thousand, three hundred arrests.

Approximately five thousand of those arrests are related to mail theft, and about twenty-four hundred, excuse me, fifteen hundred arrests relate directly to mail fraud.

Our last fiscal year, these statistics are from fiscal year 1999, we've also obtained an, approximately $606 million in court order and voluntary restitution in these cases.

One of the things that was addressed earlier by, I believe, the victims, and some of the prior testimony, is that how easy it is to obtain personal information.

Pre-approved credit card applications, pre-approved credit card forms that are discarded in the mail, are targeted by these identity thieves.

Armed with this information, of course, the criminals try to activate credit cards, and use it without the victim's knowledge.

The successful identity thieves ensure that steps are taken, that the victim is unaware that her, his or her identity is taken over.

In those types of cases, where a change of address is used, or, I believe, Mari Frank gave an example how an address was used, with her name at a different location, the victim becomes unaware of the damage that is being done to their credit, reputation and assets.

Over the past 5 years, the Inspection Service has started a data base, to try to track some identity theft investigations.

In fiscal year 1995, we had a 165 investigations. This fiscal year today, we can see that there's more than a 300-percent increase. We have open investigations, involving identity theft.

So, how do we address the fundamentals of identity theft? The Inspection Service has partnered and worked with different law enforcement agencies, the financial community, credit card companies.

We've established the Credit Card Mail Security Working Group. This group meets at least twice a year to discuss prevention initiatives, security initiatives, share intelligence and discuss best practices.

Inter-agency cooperation, I think, is very important. In June of this year, the Southern California Division assigned two postal inspectors, to work with Lee Baca, Sheriff Lee Baca's strike force on identity theft, and we welcome the opportunity to strengthen our relationship with the Sheriff's Office, and I'd like to commend and applaud Sheriff Baca for showing the initiative and leadership in this effort, and as you mentioned, it's the first identity theft strike force, in the country, and we will continue to work with the Sheriff's Department.

Since 1998, the credit card team of postal inspectors located in Los Angeles, have worked on ATM fraudulent use, which involves identity theft take-overs.

In 1998, the industry, in the Los Angeles area, would incur $106,000 in daily, that's daily fraudulent transactions.

Today, we're down to less than $25,000 in daily transactions that are fraudulent, reported to the Postal Inspection Service.

So, we're not completely, we haven't completely eliminated that problem, but we have had a lot of success. Some of it, of course, is working with this Credit Card Mail Security Group.

There are a number of statutes, historically, there are two statutes that are 125 years old. This is the mail fraud statute, and the civil false representation and lottery statutes.

The public policy behind these statutes, is simply that the postal system, created by Congress to serve the American public, should not, should not be used to conduct schemes that seek to cheat the public.

I believe you're aware of, I know you're aware of the recent legislation work you've done on that Identity Theft and Assumption Deterrence Act of 1998.

The Postal Inspection Service was one of the primary law enforcement agencies behind that initiative, simply because of the impact on the postal service and the mail.

The Postal Inspection Service supports the additional legislative efforts that you have taken, regarding these identity theft schemes.

The Identity Theft Prevention Act of 2000, which you introduced on March 30, 2000, contains several key provisions, designed to prevent identity-related fraud in credit transactions and credit reports.

And of course the Social Security Number Protection Act of 2000, which you introduced, Senator, on June 8, 2000, grants the Federal Government the authority to limit the sale and purchase of Social Security, Social Security account numbers, in circumstances that could result in fraudulent transactions.

One of the things the Postal Inspection Service thinks, we think is very important is just not going out, arresting people. That's very important, but we think prevention plays a real key role.

So, our agency has done a couple of things similar to what Sheriff Lee Baca has. We have a nationwide identity theft awareness pamphlet that tells people what identity theft is, how to prevent becoming a victim, and if you are a victim, what state you should, what steps you should take, and how to contact credit, credit card companies.

A couple of other areas in prevention, we have a website. It's *usps.gov/postalinspectors,* that issues fraud advisories about different types of identity theft schemes, and how to prevent that.

And earlier this year in March, *Showtime* released a movie, called, "Inspectors II" and it was based on the investigative files of the postal inspectors, specifically, identity theft investigations.

Last Fall, every household in America received a postcard, and it's called, "Project No Fraud," is what it is. "Project No Fraud" was to alert the public of telemarketing schemes. How to protect yourself on telemarketing schemes.

This is, this involves delivery of a 120 million pieces of mail to every address in America, to alert people.

Why do I bring this up? Because, next Spring, we're having "Project No Fraud II," and in that particular project, we will send out to every household in America, a 120 million addresses, awareness of identity theft, and what you can do to prevent identity theft, and if you are a victim, what you can do about that, also.

The Postal Inspection Service is committed to working together with Federal, State and local agencies in combating this financially crippling crime.

You can be certain that postal inspectors will continue to work with everybody to resolve this problem and prevent crime from occurring.

Senator, the U.S. Postal Inspection Service applauds your efforts in supporting law enforcement and protecting consumers throughout the United States, and our agency fully supports enactment of Senate Bill 2328 and Senate Bill 2699.

Thank you, and like the others, we'd be happy to answer any questions you may have.

[The prepared statement of Michael E. Ahern follows:]

PREPARED STATEMENT OF MICHAEL E. AHERN

Good morning Senator Feinstein and members of the Senate Judiciary Committee's Subcommittee on Technology, Terrorism and General Government. I am Michael Ahern, Deputy Chief Postal Inspector, Western Field Operations, U.S. Postal Inspection Service.

On behalf of the Chief Postal Inspector, I want to thank you for holding this hearing on the topic of identity theft, America's fastest growing crime. It is an honor to appear before you today to discuss the subject of identity theft and related fraud, and the role of the Postal Inspection Service in combating this rapidly growing category of crime. I also appreciate this opportunity to show our support for the legislation you have introduced, S. 2328 and S. 2699; both designed to prevent identity related crimes.

As you know, the mission of the United States Postal Inspection Service is to protect the U.S. Postal Service, its employees and its customers from criminal attack, and to protect the nation's mail system from criminal misuse. As one of the our country's oldest federal law enforcement agencies, founded by Benjamin Franklin, the United States Postal Inspection Service has a long, proud and successful history of fighting criminals who attack our nation's postal system and misuse it to defraud, endanger or otherwise threaten the American public. As the primary law enforcement arm of the United States Postal Service, the U.S. Postal Inspection Service is a highly specialized, professional organization performing investigative and security functions essential to a stable and sound postal system.

During fiscal year 1999, U.S. Postal Inspectors arrested 10,388 criminal suspects. Of those suspects identified, 5,051 were arrested on charges related to mail theft. Postal Inspectors investigated 3,427 mail fraud cases in 1999 and responded to 70,000 consumer fraud complaints. Mail fraud investigations resulted in 1,523 arrests, approximately $606.2 million in court-ordered and voluntary restitution, and 1,165 civil or administrative actions.

Among its varied duties, the Inspection Service works to rid the mail of drug trafficking and money laundering; mail bombs; and, perhaps one of the most despicable crimes, child exploitation. In combating fraudulent practices involving the mail, the Inspection Service employs a workforce of roughly 2000 Postal Inspectors, 1400 Postal Police Officers and 900 professional, technical and support employees.

IDENTITY THEFT AND IDENTITY FRAUD

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. All organized criminal groups appear to be involved to various degrees in identity theft schemes. The traditional reliance upon an individual's personal information by business and financial organizations, an increased availability of identifying information through the internet and other communications networks, and a willingness by criminal groups to manipulate information unlawfully obtained has led to an explosion in identity theft related crimes.

The August edition of the FBI Law Enforcement Bulletin reported that true identity theft victims are estimated to number from 350,000 to 500,000 annually. Literally hundreds of millions of dollars are lost annually to these insidious criminals, not to mention the frustration and emotional scars felt by their victims who are forced to take excruciating steps to regain their good credit. Of course, in the end we will all pay, because the losses suffered by the financial institutions are passed along to the American consumer in the form of higher interest rates and fees.

Identity theft criminals have been increasingly successful in obtaining personal data such as social security numbers, bank account or credit card numbers, victim's telephone calling care numbers, as well as other valuable identifying data. These criminals use the stolen personal information to apply for credit cards; to open new bank accounts; apply for loans; apply for apartment rentals, and to establish services with utility and phone companies, just to mention a few. In the United States

and Canada, many people have reported that unauthorized persons have taken funds out of their bank or financial accounts, or in the worst cases, taken over their identities altogether, running up vast debts and committing crimes while using the victim's names. In many cases, a victim's losses may include not only out-of-pocket financial losses, but substantial additional financial costs associated with trying to restore his/her reputation in the community and correcting erroneous information for which the criminal is responsible.

It can sometimes take identity theft victims years to repair their consumer credit file after becoming victimized. If the criminal takes steps to ensure that bills for the falsely obtained credit cards or bank statements showing the unauthorized withdrawal are sent to an address other than the victim's, the victim may not become aware of what is happening until the criminal has already inflicted substantial damage on the victim's assets, credit and reputation.

The August edition of Security Management Magazine reported that a survey of identity theft victims indicated most victims do not learn of the theft of their identify until 14 months after it has occurred. Those victims further reported an average of 175 hours actively trying to clear their names.

IDENTITY RELATED CRIMES

Many people do not realize how easily criminals can obtain our personal data without having to break into our homes. Some criminals engage in "dumpster diving"—going through potential victims' garbage cans or a communal dumpster or trash bin—to obtain copies of checks, credit card or bank statements, or other records that typically bear names, addresses, and even telephone numbers. These types of records make it easier for criminals to get control over accounts and assume identities. "Pre-approved" credit cards received in the mail and discarded without being torn-up are favored targets of the identity thief. Armed with this information, criminals may try to activate credit cards for their use without the victim's knowledge. If mail is left unsecured, criminals may try to intercept it and redirect it to another location; again to gain the personal financial information contained within. Even in public places criminals may engage in "shoulder surfing"—watching their intended victim from a nearby location as the victim punches in their telephone calling card number or credit card number.

In recent years, the Internet has become an appealing place for criminals to obtain identifying data, such as passwords or even banking information. In their haste to explore the exciting features of the Internet, many people respond to "Spam"—unsolicited E-mail—which promises them some benefit but requests identifying data. In some cases, criminals reportedly have used this scheme to obtain large amounts of personal data.

INVESTIGATIONS

Each of the Inspection Service's eighteen (18) field divisions conducts fraud investigations relating to identity theft within their respective boundaries. Identity theft investigations are reported, categorized, and tracked in an Inspection Service national database used by management to coordinate the appropriate investigative response. The following chart illustrates the recent rise in identity theft investigations conducted by postal inspectors nationwide:

Fiscal Year	*Investigations*
1995	165
1996	178
1997	198
1998	371
1999	491
FYTD–2000	626

As indicated above, identity theft activities have increased by almost 300 percent during the last 5 years, with a corresponding increase in the number of arrests and convictions. Although a national concern, the Inspection Service has observed that the largest metropolitan areas, including New York, Chicago and Los Angeles, have been responsible for the majority of the increase in identity theft activities.

To address the fundamentals of identity theft, the Inspection Service works hard to improve communication between the credit card industry, financial institutions and law enforcement. One initiative undertaken by the Inspection Service in this regard has been its sponsorship of the Credit Card Mail Security Working Group. This group, comprised of various members of the financial and law enforcement communities, meets semi-annually and offers insight and feedback relating to current programs and practices, security concerns and prevention initiatives.

INTERAGENCY COOPERATION

Postal Inspectors participate on multiple task force operations throughout the nation. In June of this year, two Postal Inspectors from the Southern California Division began working with the Los Angeles County Sheriff's task force to combat identity theft. The Inspection Service welcomes this opportunity to strengthen our working relationship with the Los Angeles County Sheriff's Department, and would like to thank Sheriff Lee Baca for his initiative and leadership in directing this campaign.

Since 1998, the Los Angeles credit card team has been working with credit card companies and local banks to reduce the losses from fraudulent credit card cash advances. As a result of this team effort, daily fraudulent cash advance activities were significantly reduced during the period by 1999 through July 2000, from $106,000 to $23,000.

In January 2000, a federal grand jury at Oakland, California, returned indictments on four individuals based on an identity theft investigation conducted by the Inspection Service's Northern California Division. This case involved mail theft in the California communities of San Ramon, Livermore, Hayward, Pleasanton, Danville, Castro Valley, Dublin, Newark, and San Leandro. The four suspects stole mail to obtain checks, credit cards and identification documents. They then created false identification documents for the purpose of cashing checks and purchasing merchandise. Postal Inspectors recovered stolen mail, false drivers licenses, altered passports and computer equipment.

In Pittsburgh, Pennsylvania, the Inspection Service leads the Financial Crimes Task Force of Southwestern Pennsylvania. This task force commenced its operation on January 17, 1995, and is housed at the Pittsburgh office of the Postal Inspection Service. Members include the United States Postal Inspection Service, the United States Secret Service, the Allegheny County, PA, Police Department and District Attorney's Office, the City of Pittsburgh, PA, Police Department, the Federal Bureau of Investigation, the Westmoreland County, PA, District Attorney's Office, the Greensburg, PA, Police Department and the Pennsylvania State Police.

Originally, this task force was formed to target major credit card fraud in the Pittsburgh area. However, with the cancer of identity theft spreading rapidly throughout America, this task force has directed most of its resources toward identity theft investigations. In fact, many of their investigations have led them to criminal groups victimizing communities and citizens around the country. The Financial Crimes Task Force of Southwestern Pennsylvania is yet another illustration of how the Inspection Service has effectively partnered with other agencies in combating identity theft.

In a recent Inspection Service investigation based in Chicago, Illinois, the destructive activities of an identity thief resulted in the loss of thousands of dollars and the death of a primary victim. In July 1999, the identity thief began dating the estranged wife of a local Chicago resident. Without his knowledge, the wife assisted the thief in stealing her former spouse's identity by providing the thief with his personal information. In August of that same year, the thief leased a sport utility vehicle (SUV) in the spouse's name using the spouse's home address as his own information.

In January 2000, an associate of the thief opened a mailbox at a commercial mail receiving agency (CMRA) using counterfeit driver's license in the spouse's name. A Change of Address (COA) order was then filed, directing the spouse's mail from his legitimate address to the CMRA mailbox. This mailbox was used to obtain credit cards and cash advances in the spouse's name. Later that month, the thief met with a former girlfriend and provided her with a credit card in the name of yet another former girlfriend. This second victim dated the thief when she was a probation officer. She had ended the relationship and had no knowledge the thief was misusing her personal information. The credit card was used to obtain two cash advances totaling over $5000.

Also during January, the spouse had a dispute with his estranged wife while she was parked in the leased SUV. He later learned the SUV had been fraudulently leased in his name. The spouse filed a complaint with the Chicago Police department after realizing that he was a victim of identity theft with losses exceeding $220,000.

In February, the spouse received a package from the thief, wrapped as a FedEx delivery. After holding the package for a few days, he received a voice mail message on his cell phone indicating the package was a gift from the thief. As he sat in his living room, he opened the package, which exploded, killing him instantly.

The investigation into the identity theft and bombing incident disclosed involvement on the part of another associate of the identity thief. In May of this year, the

individual who assisted in the construction of the bomb was arrested. In a storage shed owned by the suspect's girlfriend, Postal Inspectors found boxes containing numerous fraudulent documents, computer equipment and $100,000 in counterfeit 20-dollar bills. Later that month, the identity thief himself was arrested in Los Angeles, California, using the name and fraudulent driver's license of yet another victim. He is currently being held without bond and is scheduled to be indicted for the murder of the victim's spouse.

GOVERNING STATUTES

A number of statutes enable us to take action against fraudulent practices involving the use of the mail. Our priority weapons include two statutes originally enacted over 125 years ago: the criminal mail fraud statute and the civil false representations and lottery statute. The public policy that underlies these statues remains valid today. The postal system created by Congress to serve the American public should not be used to conduct schemes that seek to cheat the public.

While some schemes may change, con artists take advantage of economic trends and current events and plan their schemes accordingly. With today's fast-paced society and modern technology, the magnitude of mail fraud schemes is much greater and impacts more people than ever before.

THE IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT OF 1998

The Inspection Service was one of the primary law enforcement agencies involved in the legislation initiative to combat identity theft, due to the impact of these offenses on the Postal Service and the mail. The Postal Inspection Service has long understood that the majority of identity theft schemes involve the use of the mail.

Public Law 105–318, The Identity Theft and Assumption Deterrence Act of 1998, was signed into law on October 30, 1998. This law expanded the scope of the identity fraud statute (18 U.S.C. § 1028), and made it a federal crime for the unauthorized use of personal identification in the commission of any federal law (felony or misdemeanor), or a state or local felony. This Act was needed since Section 1028 ["Fraud and related activity in connection with identification documents"] previously addressed only the fraudulent creation, use, or transfer of identification documents, and not the theft or criminal use of the underlying personal information. The Act criminalizes fraud in connection with unlawful theft and misuse of personal identifying information itself, regardless of whether it appears or is used in documents.

The Postal Inspection Service supports additional legislative efforts to reduce identity related schemes. The Identity Theft Prevention Act of 2000, S. 2328, introduced by Senator Feinstein on March 30, 2000, contains several key provisions designed to prevent identity related fraud in credit transactions and credit reports. Under this Act, credit card issuers would be required to confirm cardholder change of address requests; notifications would be mailed to cardholders to confirm additional car requests; the Fair Credit Reporting Act would be amended to require consumer reporting agencies to comply with fraud alert procedures; and a standardized form would be developed for consumers to notify creditors and credit reporting agencies of identity fraud.

The Social Security Number Protection Act of 2000, S. 2699, also introduced by Senator Feinstein on June 8, 2000, grants the Federal government the authority to limit the sale and purchase of social security account numbers in circumstances that could result in fraudulent activities. The Postal Inspection Service supports restrictions on the use and dissemination of social security numbers, as they continue to be one of the prime personal identifiers used by financial institutions for credit and banking purposes. The Social Security Administration reported over 30,000 complaints relating to the misuse of social security numbers during 1999. As long as this practice exists, social security number will remain a keep element in the crime of identity theft.

OTHER INITIATIVES

In an effort to enhance the penalties associated with identity related crimes, the Inspection Service has met with and submitted recommendations to the United States Sentencing Commission. Those proposals have included a specific guideline to address the offense element of multiple victims in both the theft and fraud guidelines.

The Inspection Service further supports a change in the valuation loss for credit card offenses. In past years, we have asked the Commission to establish the alternate loss as the credit line of credit cards (the true intended loss) as opposed to the $100 minimal loss per card. We believe this is a more accurate measurement of intended loss, but support the Commission's proposed $1000 loss as a better alter-

native to the minimal value the guidelines currently set for stolen but unused credit cards.

PREVENTION INITIATIVES

While the Postal Inspection Service works hard to identify and prosecute promoters of mail fraud, we also recognize our ability to lessen the impact of fraud upon the public through various prevention campaigns. In a survey commissioned by the Postal Inspection Service it was revealed that 48 percent of the respondents who were victims of fraud did not report the crime, often citing they did not know where to go for help.

Inspection Service efforts to prevent identity theft can best be summarized as an educational campaign to alert members of the public and business communities to identity related schemes, and the problems associated with them. Those efforts have included the publication of a brochure titled, Identity Theft, An Awareness & Victim Guide, the posting of identity related fraud advisories on the Inspection Service's we page (located at www.usps.gov/postalinspectors), and the March 12, 2000, release of the Showtime movie, The Inspectors 2, based on Inspection Service files relating to identity theft investigations.

An 11-minute video titled, Identity Theft: The Game of the Name, was recently produced by the Inspection Service as an informational and reparative guide for victims of identity theft. This video profiles the exploits of an identity thief, and documents the trials and tribulations of identity fraud victims. This video will be available for distribution to law enforcement personnel and the general public.

In an effort to educate consumers, the Postal Inspection Service, in November 1999, joined forces with several federal, state and private agencies, including the AARP, Better Business Bureaus' Foundation, Department of Justice, Federal Bureau of Investigation, Federal Trade Commission, National Association of Attorneys General, and the Securities and Exchange Commission, to launch project KNOW FRAUD. This initiative was the largest consumer protection effort ever undertaken, designed to connect the public with those agencies that can help and provide consumers with new resources to stop telemarketing and mail fraud. A toll-free number and a KNOW FRAUD Website were also established to provide consumers with additional fraud prevention information and to link them with law enforcement officials who would share the information.

Although work continues on the first KNOW FRAUD initiative, plans are underway for a second one to launch in early 2001. Focusing on identity theft, the goal of this new effort is to deliver to every home in America prevention information that will raise their awareness of this growing trend and provide them with protective tactics. Information on identity theft can already be found at the KNOW FRAUD Web site (located at http:www.consumer.gov/KNOW FRAUD), and consumers may call a toll-free Identity Theft Hotline (1–877–IDTHEFT) for help with problems related to this crime. All complaints are input to the Consumer Sentinel's Identity Theft Data Clearinghouse.

Agencies participating in KNOW FRAUD: Identity Theft include the U.S. Postal Inspection Service, AARP, the Council of Better Business Bureaus' Foundation, the Department of Justice, the FBI, the Federal Trade Commission, the National Association of Attorneys General and the Securities and Exchange Commission.

PREVENTION STEPS

As part of the Postal Inspection Service's ongoing campaign to help educate and empower the American public when dealing with those criminals who attempt to steal the most personal of all things—your identity, I would offer the following prevention tips:

- Promptly remove mail from your mailbox after delivery.
- Deposit outgoing mail in post office collection mailboxes or at your local post office. Do not leave mail in unsecured mail receptacles.
- Never give personal information over the telephone, such as your social security number, date of birth, mother's maiden name, credit card number, or bank PIN code, unless you initiated the phone call. Protect this information and release it only when absolutely necessary.
- Shred pre-approved credit applications, credit card receipts, bills and other financial information you don't want before discarding them in the trash or recycling bin.
- Empty your wallet of extra credit cards and identification cards or better yet, cancel credit cards you don't use and maintain a list of the credit cards you do use.

• Order your credit report from the three credit bureaus (Equifax, Experian Information Solutions, and TransUnion) once a year to check for fraudulent activity or other discrepancies.
• Never leave receipts at bank machines, bank counters, trash receptacles, or unattended gasoline pumps. Keep track of all your paperwork. When you no longer need it, destroy it.
• Memorize your social security number and all of your passwords. Do not record them on any cards or anything in your wallet or purse.
• Sign all new credit cards upon receipt.
• Save all credit card receipts and match them against your monthly bills.
• Be conscious of normal receipt of routine financial statements. Contact the sender if they are not received in the mail.
• Notify your credit card companies and financial institutions in advance of any change of address or phone number.
• Never loan your credit cards to anyone.
• Never put your credit card or any other financial account number on a postcard or on the outside of an envelop
• If you applied for a new credit card and it hasn't arrived in a timely manner, call the bank or credit card company involved.
• Report all lost or stolen credit cards immediately.
• Closely monitor expiration dates on your credit cards. Contact the credit card issuer if replacement cards are not received prior to the expiration dates.
• Beware of mail or telephone solicitations disguised as promotions offering instant prizes or awards designed solely to obtain your personal information or credit card numbers.

INTERNET AND ON-LINE SERVICES

• Use caution when disclosing checking account numbers, credit card numbers or other personal financial data at any Web site or on-line service location unless you receive a secured authentication key from your provider.
• When you subscribe to an on-line service, you may be asked to give credit card information. When you enter any interactive service site, beware of con artists who may ask you to "confirm" your enrollment service by disclosing passwords or the credit card account number used to subscribe. Don't give it out!

ACTIONS STEPS FOR IDENTITY THEFT VICTIMS

• Contact all creditors, by phone and in writing, to inform them of the problem.
• Call your nearest U.S. Postal Inspection Service office and your local police.
• Contact the Federal Trade Commission at 1–877–ID–THEFT, to report the problem. Call each of the three credit bureaus' fraud units to report identity theft: Equifax Credit Bureau, Fraud, 1–800–525–6285; TransUnion Credit Bureau, Fraud, 1–800–680–7289; Experian Information Solutions, 1–888–397–0949.
• Ask to have a "Fraud Alert/Victim Impact" statement placed in your credit file asking that creditors call you before opening any new accounts.
• Alert your banks to flag your accounts and contact you to confirm any unusual activity; request a change of PIN and a new password.
• Keep a log of all your contacts and make copies of all documents. You may also wish to contact a privacy or consumer advocacy group regarding illegal activity.
• Contact the Social Security Administration's Fraud Hotline 1–800–269–0271.
• Contact the state office of the Department of Motor Vehicles (DMV) to see if another license has been issued in your name. If so, request a new license number and fill out the DMV's complaint form to begin the fraud investigation process.

The Postal Inspection Service will continue its public awareness and educational campaigns to prevent the spread and related consequences of identity theft. You can be certain that Postal Inspectors nationwide will continue to work together with all other federal, state and local law enforcement agencies to aggressively investigate, arrest and seek prosecution for those individuals who dare victimize hard working Americans through identity takeover schemes.

Thank you.

Senator FEINSTEIN. Thanks very much, thank you. I think that was excellent testimony.

I have found that many people don't really think this is a problem yet.

And yet every bit of testimony that we have had indicates that indentify theft, in fact, is a growing problem, and that we need to move.

I want the record just to reflect that I have sent a letter to the Secretary of the Treasury, urging that he take action, so that the Social Security number is not as available on the window envelopes that they send out checks on, and I think that's a real problem.

My first question would be, has anybody got any information that the government itself, in that sense, is helping people gain these numbers indiscriminately?

Ms. VEZERIS. I think that has been an issue, and I believe that that may have already been initiated, that the Social Security number has been removed from the visible portion of the envelope, you know, when, when government checks are being mailed.

Senator FEINSTEIN. Oh, that's excellent. I'm glad to hear that.

Ms. VEZERIS. So, I, I believe that that's, if it's not, if it's not already happened, it's in the works.

Senator FEINSTEIN. We'll check and see.

Ms. VEZERIS. And then I'll, I'll verify that——

Senator FEINSTEIN. If you would.

Ms. VEZERIS [continuing]. With your office.

Senator FEINSTEIN. Thank you.

Ms. VEZERIS. Yeah, be happy to.

Senator FEINSTEIN. Thank you, very much. I think that's, that's helpful.

Second question, you mentioned that there, there is some concern on the enforcement provisions. Do you want to give me some input in that direction?

Ms. VEZERIS. Sure. I think that these bills are, are wonderful, in its efforts to try to, at the front end help the consumers.

The concern that we have, and something that we'd like to try to work out before it's enacted, is the interplay between the FTC's regulatory responsibilities, in defining what is, and what isn't appropriate business practices, as far as the use and sale of the SSN, and how they will be treating perceived violations under their unfair trade practices, as that relates to our investigative efforts.

And I guess what we would recommend is that the FTC would concentrate on legitimate commerce, and not be entertaining, let's say, as an example, an Internet company that sells identity documents, claiming that they're novelty items, to try to circumvent the law, that the FTC would not try to treat that as an unfair business practice, but rather have law enforcement immediately get into that type of investigation, as a criminal matter, and not as an unfair business practice.

And I think it's just a matter of kind of working that out, before the legislation.

Senator FEINSTEIN. So, this is a difference in point of view, between the FTC and the Social Security Administration. Is that fair assumption?

Ms. VEZERIS. I—you don't, I——

Senator FEINSTEIN. Because we worked closely with the FTC, in drafting this.

Mr. KLURFELD. I would only remark parenthetically, Senator, that the Federal Trade Commission has not formally commented on Senate Bill 2699.

So, I can't really, because I can't speak on behalf of the full commission, what its position would be.

However, expressing my own position, certainly any legislative measure, to restrict access to Social Security numbers, which seems to be the centerpiece of this fraud in terms of capturing someone's identity, would certainly thwart identity theft.

So, to that extent, I would say that, that conceptually, this is very important legislation.

We are sensitive to the fact that there are legitimate uses for perhaps the sale of this identifying information, as my colleague indicated, in terms of, of legitimate commerce, but also to the extent that there is a great potential for misuse, then this also needs to be looked at very closely and, and the commission, of course, would do so at your request.

Senator FEINSTEIN. Yeah, we've received testimony that there are twelve websites, involved in the sale of this personal identification, and we know at least four of them sell Social Security numbers, no questions asked for as little as $25.

My view is a very clear one, that that should not be permitted. You should not be able to sell anybody's, anyone else's Social Security number, period, the end.

What I'd like to ask is that either you give Tom Oscherwitz, my judiciary Counsel the person in your department, so we can get this remedied between the two departments, before you leave.

My second point relates to your comment it is possible to buy a fraudulent Social Security card over the Internet.

Could you elaborate on that point, so that we have it in the record?

Ms. VEZERIS. What, what some of these Internet companies will do, is they will sell things that, that purport to be a Social Security card, for instance.

What they will do is attach a sticker on it that says novelty item, you know, or not for purposes of identification, but that sticker is very easily removable, and then once you do that, you in fact, have, have something that would deceive someone into thinking that it was a real form of identification.

And, and that has, I mean that's, that's out there.

Senator FEINSTEIN. And you know very well, the sticker's going to be taken off, and the card is going to be used.

So, I mean that clearly, I think we should respond to, but our point in this legislation, and this has been pretty well gone over, is that the Social Security number should not be sold, except for a specific number of limited circumstances.

Ms. VEZERIS. Right.

Senator FEINSTEIN. And I assume you've reviewed the information and you're in agreement with those circumstances.

Ms. VEZERIS. Yes, I mean we've, we've worked with your staff on those, on those items.

Senator FEINSTEIN. OK.

Ms. VEZERIS. I may add one other point of concern, and it's really just a technical point.

We really appreciate the civil monetary penalty provisions in your bills, because it really adds another dimension.

It's another tool in law enforcement's box, if you will.

Senator FEINSTEIN. Right.

Ms. VEZERIS. Especially, with the demands in, at the U.S. attorney's offices for instance.

They can't prosecute all of the cases that, that are presented.

So, at least we have then an opportunity to financially attack these people that are trying to do these things.

One of the concerns that we have with respect to the, CM, with the civil monetary penalty provision, is we would want to make sure that the way it's drafted, it does cover people who are selling these Social Security cards, with this novelty sticker on it.

It's something that we would just like to work with your office, and make sure that the language is, will cover that.

Senator FEINSTEIN. OK, thank you very much.

Let me ask Mari Frank this question. In July, when you tried to report the second instance of credit card fraud to three major credit bureaus, I'd like to know what their response was.

Was it difficult, getting through on the phone? Were you provided with adequate information?

Ms. FRANK. That's a, that's an excellent question. I was able to get through after about 30 minutes to Trans Union and to Equifax. Experian had no human on the phone. You could not get one.

I wrote letters to all three, return receipt requested. I sent a copy of my driver's license and my mortgage statement, and I did, within about a week, from Trans Union and Equifax, get my credit report.

From Experian, it took me about 20 days, and then they sent me a letter saying that I had to pay $8, which is not true. I am, as a victim, allowed to get a credit report for free.

And so, then I called and spoke to them. And, as a matter of fact, I spoke to the head of the Fraud Department, Tim Puckett, and explained to him, he said to me, to, to let you know that this doesn't always happen, and he did apologize, but it did take me this, you know, so long to get my credit report, and then when I did get, finally get a number to get a human being, that took me another half hour.

So, someone who has already been through this, who's pretty savvy, had to experience this, as badly as I did, I told him that there really needs to be some changes, because obviously, if it happened to me, and I had the problems that I did, then I can just imagine what the other consumers are experiencing.

Also, by the way, there's no help from the credit reporting agencies, and they are the one source that all victims must go to.

Not everybody knows to go to the Federal Trade Commission yet, or the Social Security Administration, but everyone has to go to the credit reporting agencies.

So, I would really like to have that kind of public private venture, where you work together, because they are not sporting, you know, referrals and assistance.

Senator FEINSTEIN. So, let me get this straight.

So, a victim would have to go to all three agencies?

Ms. FRANK. Yes.

Senator FEINSTEIN. Is there, is it not possible to evolve a kind of one-stop shop between the agencies?

It seems to me, you know, knowing how hard it is to make these calls, to get through to the right person, it seems to me some kind of one stop shop—yes please.

Mr. KLURFELD. I, I think that's a, a excellent comment, that it would certainly be far more efficient for a victim to be able to file one affidavit.

The Federal Trade Commission is working with the credit reporting agencies, to try to establish that a complaint to us could then be forwarded immediately, basically, the most efficient way is one-stop shopping to the three credit reporting agencies.

When I also think of the volume of, of, I mean this really resonates, but on our own website, in terms of identity theft, we have recorded a hundred thirty-nine thousand hits, for people who are obviously concerned about this.

And, I mean, obviously everyone isn't complaining but people do express great concern and apprehension about this.

If you were a victim, it would be excellent to be able to either file your affidavit with us, and we could then immediately transmit it to the credit reporting agencies, or if there were a mechanism for them to cooperate inter se, so they're filing it with one, would generate the fraud alerts, which are so critical to their, to competitors.

Sheriff BACA. May I comment on that?

Senator FEINSTEIN. Please. Ms. Vezeris, and then we'll go to the Sheriff.

Ms. VEZERIS. I, I would just like to add one thing.

On the enforcement side, we have established an agreement between the FTC and our office, and as allegations come in, presume most of them come to our hotline, although they can come through field offices, as well.

But when those allegations come in, with the permission of the caller, we then, we've already, it's a, it's a new agreement, and we've only done this at one time, but we will exchange that information with the FTC directly.

So, the caller can provide the information to us, and it will be fed into the FTC, so they don't have to make multiple calls.

Senator FEINSTEIN. But is there any reason that the Federal departments would feel you could not have a one-stop shop, whether it's the FTC or wherever, there should be one?

Mr. KLURFELD. Correct.

Senator FEINSTEIN. Then would you mind very much talking among yourselves, and seeing who it should be and how we get that started? That'd be helpful. Sheriff.

Sheriff BACA. I would like to say this, that if a victim were to come to the Sheriff's Department and define the scope of their problem, and one of course would be, an element of that scope, would be that they want to know what their credit report truly says.

People don't have experience with all of us in law enforcement. They tend to wander a lot on the, on the field of where do I get my help.

And so the Federal Trade Commission is, is extraordinary, as is the Social Security and the Postal Service.

All three of these agencies have incredible capabilities.

But the average citizen really needs someone like a seeing-eye dog, to kind of let them go here and go there.

Now, we ought to be able to do that in the Sheriff's Department. My investigators who are here, Sergeant Rolando Bracamontes, where are you? He's right there, stand up please, Joe Dulla.

Two of my investigators here could be very easily by policy, the person, the contact persons to the Federal Trade Commission, if that's where we trigger the process, or to Social Security, or even to the Postal Service that, that the training that local law enforcement needs to have is not one when say a victim comes in and says, what do I do? I make these phone calls, no one's on the phone. I got hits on two credit agencies, however, I need the third, can you help?

And then, I think the process should be, yeah, we can help, and we will just automatically contact these agencies for the victims and get things rolling, 'cause we're gonna wanna see that stuff, too.

Senator FEINSTEIN. That's excellent. Yeah, Mr. Klurfeld.

Mr. KLURFELD. Thank you. Again, responding to your initiatives, Senator, from the 1998 bill, the clearinghouse again is really the central repository, and this month, we are making it accessible to all law enforcement officers, throughout the country.

So, to the extent that you have a laptop computer, or you are online, and no matter how small your police department, or how large your police department, you will now have access to the very data that we have, and therefore you will be able to track trends.

So, if you wanted to find out whether a certain type of identity theft is erupting in your particular market or jurisdiction, city, town, even village, you will be able to access the Federal Trade Commission data.

Senator FEINSTEIN. Well, let's say that the FTC is the agency that handles all the complaints. Would it be possible then for the sheriff or the law enforcement officer, wherever the complaint comes in to register that affidavit with your department to save time? Because I'll tell you, people have a terrible time, when it comes to the Federal Government. I hate to say it, but they really do, even getting to the right place is a——

Sheriff BACA. Well, hey, you make the, you make it a strong, you make a strong point there, Senator.

I think, ideally, we're saying that it would be nice to have the Federal Trade Commission investigator in the task force, as Social Security and postal, recognizing it's, it's a break from the traditional way of doing things.

But these investigations have so many tentacles, that the applications of inquiry are beyond just what we're telling you here.

When you're dealing with financial institutions, this country, and Jeff you might know the answer, I don't know how many financial institutions are registered with the Federal Trade Commission, but it's gotta be what?

Mr. KLURFELD. We don't have a registration system for financial institutions, but clearly there are——

Sheriff BACA. Well, there's gotta be——

Mr. KLURFELD. When you're talking about the global economy, you're talking about millions, probably.

Sheriff BACA. Exactly, and, and so the expertise of dealing with the victim's plight, is one that has to cross over, just what we know in, in local law enforcement, and that's why I think the, the skill level is incredible, the availability of this kind of expertise is one that is emerging now.

Mr. AHERN. The, if, if I could just make one point.

Senator FEINSTEIN. Finish, then Mr. Ahern has a comment.

Mr. KLURFELD. We have a database called Consumer Sentinel, in which every law enforcement agency, and consumer protection, non-government agencies, such as a Better Business Bureau, input data to us, so we are able to find out where fraud is erupting, throughout the landscape.

This is not just confined to identity fraud theft, excuse me, but whether you're talking about telemarketing fraud or tele-funding, prize promotions, the hit list of really the rape and pillage out there, in terms of the fraud landscape.

By virtue of that database, you will also have access to all of the identity theft data, and you will be able to input, for example, if another victim were to come to you, by virtue of your taking in that information, you will be able to input it automatically, in to the Federal database, and that can be shared, as you've indicated.

You know, this thing is global at this point, and it's vital that we do, you know, cooperate, Federal, State, all levels of law enforcement.

I think we have to use all the tools that are available to us, in terms of high tech, because quite frankly, it is, it is obvious that the thief is using all those weapons and we must be as, as alert as, as they are and use the same tools.

Ms. FRANK. Senator Feinstein, can I add one quick point?

Senator FEINSTEIN. Before Mari——

Ms. FRANK. OK.

Senator FEINSTEIN. Mr. Ahern was next, and then I'll——

Ms. FRANK. OK.

Mr. AHERN. OK, thank you Senator.

One thing that kind of identified the problem to us was a couple of years ago, prior to us coming out with the identity theft awareness, bulletin and prior to "Project No Fraud," we actually ran a survey, two people, and found out that 48 percent of the victims of an identity theft didn't readily report it, because they didn't know where to go.

And I think that's what we're talking about here. So, we're talking education, and you know, prevention is very important.

This Consumer Sentinel that Jeff mentioned, I do know we have a postal inspector at our headquarters office assigned full-time with FTC. I think that's a step in the right direction.

But I'd like to support what the Sheriff said there, some kind of system, if we just have one place, that's fine for a clearinghouse, but the problem is it comes in, in a lot of different areas, and we have to make sure all the agencies, the Social Security Administration, that we forward this on, or have some way electronically.

Because I think in the past, a victim calls in to a credit agency, and they don't get a response, they can't get a human voice, they

just get frustrated. They might report to a local police officer in a small town somewhere. It might not go forward, and have to make sure we capture that.

So, I think some of the efforts, some of the discussion here, the data base with Consumer Sentinel is a step in the right direction. We'd be supportive of that.

Senator FEINSTEIN. Thank you very much.

Ms. FRANK. I get about a hundred e-mails and phone calls from victims a month, and the victims either report to the police, or to the credit reporting agencies, and I'm happy to hear that Sheriff Baca is going to refer them to the FTC.

I think that's a great place to start, and, and you move on, but if the credit reporting agencies, perhaps in your bill, you could make it incumbent upon the credit reporting agencies to have a referral to the FTC, because when you call in and you're listening to the voice mail, there's no referral to the FTC now, and in the letter that I just received last week, there was no referral to the FTC.

So, I think that would be a great place to start, is have that as part of the bill.

Senator FEINSTEIN. What, what do you think?

Mr. KLURFELD. I, I think that is excellent also.

Again, as much information as can be obtained to track trends, to find out what the extent of the problem is, is certainly welcome, to interdict the problem.

Ms. FRANK. And then you refer on, as well, correct? If they need help?

Mr. KLURFELD. Yes, we do, and also back to law enforcement. The only caveat I would have to give is again a bureaucratic one that, that would be a decision for the commission itself to make, rather than for Jeffrey Klurfeld to arena to himself.

Senator FEINSTEIN. I understand. But you will take it back.

Mr. KLURFELD. Absolutely.

Senator FEINSTEIN. Yeah, because——

Sheriff BACA. And we'll help you, if you need letters and support.

Senator FEINSTEIN. That, that, that's great. I mean, I think it is so hard, and I think if there were one clearinghouse affidavit recipient, that if it was a Social Security fraud, that it, you know, a copy went to Social Security, if it was post office, it went to post office, if it was another area, the FTC is really the agency, it seemed to me, equipped to handle that, but it is clear that, you know, we have hundreds of thousands of these now a year, so going to have to get cracking.

Lieutenant, you wanted to——

Lieutenant JORDAN. Yes, one of the things, Senator, that we did, when we started our task force, we got the strike force deputies to advise the citizens that were victims of identity theft to contact, contact the people from the Federal Trade Commission.

Also, for the police officers' standard and training class that we developed the curriculum for, earlier this year, that is one of the things we stressed for all the officers and deputy sheriffs throughout the State of California to do this.

Senator FEINSTEIN. Well, that's great.

Well, all right. Selene, do you have any comments that you might like to add at this, at this point? Or else, I think we'll——

Ms. KASSIN. Well, I think that the FTC would be wonderful as a clearinghouse, only because with my personal experience, I was shuffled from one police department to another police department, to another police department, and there were jurisdictional issues, and nobody would give me any information.

So, I had no information, and again I had the same experience as Mari Frank, calling the credit card, calling the credit bureaus and being put on hold, and, and pushing one, pushing 10, pushing five, and not, not, not having any resources to where to go next. It was a lot of investigation on my part.

Senator FEINSTEIN. Well, I, I think that's an excellent point. I think you made the point very clearly. We've got a couple of charts up there, and I don't think they're terribly visible, but I think they're important.

One chart outlines the steps that identity theft victims can take, and another shows how to prevent identity theft from happening, I think there's some very good statements in these charts, that consumers should know, like, first, regularly review your credit card statements, and bank statements for unauthorized withdrawals or charges.

Second, tear or shred charge receipts, pre-approved credit applications, bank checks and statements, so that these don't float around, but particularly, the credit card receipt.

Another one is don't carry your social security card in your purse or wallet. I do, most people do, I think.

Order copies of your credit card report each year and review them for errors, and the numbers are right there on that first chart.

And I think importantly, don't give out personal information over the phone, unless you know the contact is a valid one.

At work, be careful who has personal access to your personal information, and so on, but I think these are important things.

If there is any number one thing a person can do to protect their identity, does anyone have a suggestion what it might be, Mari?

Ms. FRANK. I, I think we need to have a monitoring of our credit reports more often, like some have, there are some websites that may be going up that will offer free reviewing of monitoring on a weekly basis, because that is the only place you're going to really know if you're a victim of fraud.

Neither Selene nor I could have done anything to protect what happened to us, nothing. If we did every one of these things, it wouldn't have done anything to help us, you know, not carrying our Social Security number, not talking on the phone, not giving out personal information on the Internet.

Senator FEINSTEIN. Wouldn't have made a difference.

Ms. FRANK. The truth of the matter is, the way to really, at least get a quick response, is to find out if there's any inquiries that are fraudulent, that are coming on your credit report. That's the one thing you can do.

And if you can take your profile off-line, then no one could access it, to get your credit.

In other words, if I could, and I've been asking the credit reporting agencies to do that, which is they won't allow us to take our profile off-line, so that no credit cards could be issued.

So, that would be another thing, to allow, have that, that a consumer could take his credit off-line.

Senator FEINSTEIN. I think that's a good point. Yes, and, and I think our bill mandates that every consumer would be entitled to one free credit——

Ms. FRANK. Right.

Senator FEINSTEIN [continuing]. Report a year.

Ms. FRANK. We do.

Senator FEINSTEIN. I mean, just getting a credit report is difficult.

So, I think your point, allowing the consumer to remove their credit from on-line would also be something we should add. So, I think that's a good point.

Any other suggestions, and we'll close it off?

Well, let me just say, I think this has been a great hearing. I thank you very much.

Sheriff, you're going to ask each of these departments for cooperation and assignment, and I'm happy to back you up on that.

Sheriff BACA. We have an excellent relationship now, Senator. I think that undoubtedly, their resources are like any law enforcement agency's resources, limited.

If it's possible that they can assign full-time investigators to this task force, we have the space available, the office equipment is there.

I think it would be useful. I think we're just at the tip of the iceberg, Senator, to be really honest with you.

Obviously, you've focused on the right part of the problem. Undoubtedly, there are people in this audience here, who have had fraudulent credit card charges on their accounts, and then when they've called their credit card agency sources, they've literally had those charges wiped off. Police reports were never made.

The issue has a clear need for a tremendous amount of additional research.

Senator FEINSTEIN. All right.

Sheriff BACA. You've done a magnificent job, but there's much more that we need to find out about it.

Senator FEINSTEIN. That's absolutely right.

Sheriff BACA. And when we find out more, Senator, as you know, we're gonna come back to you with this information, and I think we should probably give you a, an update, probably in another 6 months to a year, as to where we've gone from here.

You, you've done wonderful, you're the leader on this matter.

Senator FEINSTEIN. Well, it's, as you said, it's the tip of the iceberg, and we can only address what we know is happening now, but my sense is that this is going to be growing in sophistication, as the data becomes available, and I think the key thing that I'm trying to do is make a beachhead with the Social Security number.

Social Security numbers shouldn't be something that's traded or sold. It's not intended to be that, it's not meant to be that, that's not its purpose.

And so, if we can get that established and really, just kind of crack down in one area, it might, then we can see what else develops, but it's an ever-moving target, no question.

Let me just thank everybody very, very much, and the hearing stands adjourned. Thank you.

[Whereupon, at 10:44 a.m., the subcommittee adjourned.]

○