AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 107–900

IDENTITY THEFT

HEARINGS

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

MARCH 20 AND JULY 9, 2002

Serial No. J–107–68

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
85–794 WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts	ORRIN G. HATCH, Utah
JOSEPH R. BIDEN, JR., Delaware	STROM THURMOND, South Carolina
HERBERT KOHL, Wisconsin	CHARLES E. GRASSLEY, Iowa
DIANNE FEINSTEIN, California	ARLEN SPECTER, Pennsylvania
RUSSELL D. FEINGOLD, Wisconsin	JON KYL, Arizona
CHARLES E. SCHUMER, New York	MIKE DEWINE, Ohio
RICHARD J. DURBIN, Illinois	JEFF SESSIONS, Alabama
MARIA CANTWELL, Washington	SAM BROWNBACK, Kansas
JOHN EDWARDS, North Carolina	MITCH MCCONNELL, Kentucky

BRUCE A. COHEN, *Majority Chief Counsel and Staff Director*
SHARON PROST, *Minority Chief Counsel*
MAKAN DELRAHIM, *Minority Staff Director*

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

DIANNE FEINSTEIN, California, *Chairwoman*

JOSEPH R. BIDEN, JR., Delaware	JON KYL, Arizona
HERBERT KOHL, Wisconsin	MIKE DEWINE, Ohio
MARIA CANTWELL, Washington	JEFF SESSIONS, Alabama
JOHN EDWARDS, North Carolina	MITCH MCCONNELL, Kentucky

DAVID HANTMAN, *Majority Chief Counsel*
STEPHEN HIGGINS, *Minority Chief Counsel*

CONTENTS

MARCH 20, 2002

STATEMENTS OF COMMITTEE MEMBERS

	Page
Cantwell, Hon. Maria, a U.S. Senator from the State of Washington	3
Feinstein, Hon. Dianne, a U.S. Senator from the State of California	1
Grassley, Hon. Charles E., a U.S. Senator from the State of Iowa	56
Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah	57
Kyl, Hon. Jon, a U.S. Senator from the State of Arizona	19
Sessions, Hon. Jeff, a U.S. Senator from the State of Alabama	13
Thurmond, Hon. Strom, a U.S. Senator from the State of South Carolina	62

WITNESSES

Beales, Howard, Director, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C.	6
Cannon, Louis P., President, District of Columbia Lodge, Grand Lodge, Fraternal Order of Police, Washington, D.C.	28
Foley, Linda, Executive Director, Identity Theft Resource Center, San Diego, California	34
Gregoire, Christine O., Attorney General, State of Washington, Olympia, Washington	20
Twentyman, Sallie, Falls Church, Virginia	24

SUBMISSIONS FOR THE RECORD

California Department of Consumer Affairs, Sacramento, California, statement	58
LexisNexis, Norman Willcox, Chief Officer for Privacy, Industry and Regulatory Affairs, Washington, D.C., letter and attachment	67

JULY 9, 2002

STATEMENTS OF COMMITTEE MEMBERS

Feinstein, Hon. Dianne, a U.S. Senator from the State of California	81
Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah	103
Kyl, Hon. Jon, a U.S. Senator form the State of Arizona	95
Thurmond, Hon. Strom, a U.S. Senator from the State of South Carolina	104

WITNESSES

Beales, Howard, Director, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C.	90
Collins, Daniel P., Associate Deputy Attorney General and Chief Privacy Officer, Department of Justice, Washington, D.C.	83
Lormel, Dennis M., Chief, Terrorist Financial Review Group, Federal Bureau of Investigation, Washington, D.C.	87

IDENTITY THEFT: RESTORING YOUR GOOD NAME

WEDNESDAY, MARCH 20, 2002

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY, TERRORISM,
AND GOVERNMENT INFORMATION,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:05 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Dianne Feinstein (chairman of the subcommittee) presiding.

Also present: Senators Feinstein, Cantwell, Kyl, and Sessions.

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

Chairperson FEINSTEIN. I would like to call this hearing to order and welcome our witnesses and also the people in the audience. The ranking member, Senator Kyl, is delayed. He will be here shortly, but I thought because we all have a busy day that we might just begin the hearing.

This hearing is on "Identity Theft: Restoring Your Good Name." What is identity theft? Identity theft occurs when a criminal assumes the identity of another person for illicit gain. Often, a thief will steal another person's Social Security number, birth date, driver's license, or other identifying information to obtain credit cards, car loans, phone plans, or other services in the victim's name.

In 1998, Congress took an important first step in curbing identity theft by passing the Identity Theft Assumption and Deterrence Act, which made identity theft a Federal crime. But the deterrence provided in the 1998 law is really only one piece of the puzzle.I21For the last two years, I have urged Congress to enact measures to prevent identity theft. Our laws need not only to punish identity thieves who are caught, but also make it more difficult to commit this crime. We haven't done that so far. It is far too easy for identity thieves to capture another person's identity and ruin their good name.

Just two weeks ago, the General Accounting Office reported that identity theft cases continue to surge. One of the three national credit card agencies reported a 53-percent increase in identity theft alerts. Allegations of Social Security number fraud have increased by 500 percent in the past several years, from 11,000 in 1998 to 65,000 in fiscal year 2001. In prior hearings, we have had the Social Security Administration testify and indicate that they have been amazed, truly amazed, at the number of these thefts. Fraud

losses at financial institutions are running now well over $1 billion a year.

In order to cut down on identity theft, we must plug the loopholes in our financial services system that allow identity thieves to thrive. To this end, I have introduced the Identity Theft Prevention Act with my ranking member, Senator Kyl, and Senator Grassley of this committee.

The bill directs banks, credit bureaus, and other financial institutions to take some practical steps to protect sensitive personal information. This would require credit bureaus to inform credit issuers if a credit card applicant has a different address than the address on file with the credit bureau. Variations in address are tell-tale indicators of identity theft.

Secondly, we would impose fines against credit card vendors who issue new credit cards to identity thieves even after a fraud alert is placed on the identity theft victim's credit report.

Finally, we would require machines that print out credit card receipts to print out only the last five numbers of the credit card on the receipt. California has enacted this law and it makes very good sense. There is no reason to display a full credit card number on a receipt. The owner of the card already knows his or her number. Moreover, thieves can steal the credit card number when the consumer tosses the receipt out or by stealing the store receipt, and this happens extraordinarily often.

We can make it more difficult for thieves to take over credit card accounts. One common practice is for a thief to steal your credit card number and then ask that a new credit card be sent to his address. To stop this scheme, the bill requires a credit card company to notify consumers at both their old and new address when an additional credit card is requested on an existing credit account within 30 days of an address change request.

These measures are pretty simple, but they are really very necessary. It is really time, I think, for the financial services industry to take some affirmative measures to protect the sensitive information consumers entrust to them.

I have another bill, a big bill, which we heard about at the last hearing a few weeks ago, which is an opt-in/opt-out bill which says it would be illegal for Social Security numbers to be displayed or sold to the public. That is not what the Social Security number was designed to do in the first place. Secondly, for other personal financial data, the company would have to get your permission to use that material.

Frankly, I don't want anybody to sell my personal identification, my personal financial data, or my personal health data without my permission and I think most Americans feel exactly the same way.

Someone who has been a big leader in this area and has a bill that we are going to be discussing today is Senator Cantwell, and I am delighted she is here. She has a bill that is the subject of this hearing and I am going defer to her at this time and ask her if she would like to make some opening comments and talk about her bill, and then we will begin the testimony.

STATEMENT OF HON. MARIA CANTWELL, A U.S. SENATOR FROM THE STATE OF WASHINGTON

Senator CANTWELL. Thank you, Madam Chairman.

I want to thank Senator Feinstein for calling this hearing today and commend her for her hard work on this particular issue of identity theft and the larger issue of protecting personal privacy. I know that she and Senator Kyl have held many hearings on this issue and I want to thank them for drawing attention to the problem of identity theft.

I also want to welcome Attorney General Christine Gregoire, from my home State of Washington, who is going to be on the second panel. Her leadership in the State of Washington has been instrumental in fighting identity theft and we look forward to hearing her remarks today.

With over 500,000 victims last year alone, identity theft is one of the fastest growing crimes in America. One in five American families have been victimized by identity theft. This simple fact alone underscores why Senators Feinstein, Kyl and I have all introduced legislation to help prevent identity theft, and we are looking forward to hearing today's testimony.

My bill, based on Washington State law, puts identity theft victims' rights first by empowering them to reclaim their identity. It also makes common-sense revisions to the statute of limitations on victims' ability to sue in an identity theft case so that the clock starts ticking when the victim learns of misrepresentation, not when it occurs. Finally, it increases information flow among local law enforcement and State and Federal agencies fighting identity theft, especially when issues of theft related to terrorism might be involved.

Today, in this country, victims of identity theft often must become their own private investigators to clear their names, and typically they do so without the help of the information that they need most. That is why this legislation would require businesses to give victims of identity theft the records they need to back up their good name. This is already required in Washington State and California. Now, we need to take this good idea and move it to a national level and make it work on behalf of others.

Think about it. When your TV is stolen or your car is stolen, it is right out of your home or in front of your home. But when your identity is stolen, it could be stolen from anywhere. A consumer shopping online in Seattle may purchase golf shoes from a manufacturer in San Diego and have her identity stolen by someone hacking into the system in Washington, D.C. The implication is crystal clear: We need a stronger Federal role in protecting consumers from identity theft.

This legislation also restores a sensible rule on the limits of consumers' rights to sue under the Fair Credit Reporting Act. Last year, the Supreme Court ruled that a California woman, a victim of identity theft, couldn't sue a credit reporting agency because she filed her case more than two years after the agency has reported to others fraudulent information about her. This legislation makes common sense prevail, ensuring that the clock on the statute of limitations doesn't begin ticking until the victim knows that they have been harmed.

Finally, with the war on terrorism and the concern about the ability of terrorists to possibly steal passport or visa or other identification information, we have become painfully aware that identity theft can threaten more than our pocketbooks. This bill requires the Federal coordinating committee that monitors Federal identity theft enforcement to find ways that the Federal Government can help State and local enforcement address identity theft, especially when the identity theft may be related to terrorism. By giving consumers and law enforcement additional tools to fight identity theft, this bill will make it harder for terrorists to steal identities and to hide their true identity.

Before we begin the testimony, Madam Chairman, I want to thank Linda Foley, who has been a tireless advocate for identity theft victims and a driving force behind the Identity Theft Resource Center. I also appreciate the support of Mr. Cannon's Fraternal Order of Police and their testimony today, and the Consumers Union, the Police Executive Research Forum, the Privacy Rights Clearinghouse, and others who are providing important information at today's hearing. I look forward to hearing the testimony.

Thank you, Madam Chairman.

[The prepared statement of Senator Cantwell follows:]

March 13, 2002.

Help Victims of Identity Theft Restore Their Good Name

Dear Colleagues:

Identity theft is the fastest growing crime in America and its victims need our help.

The Reclaim Your Identity Act of 2001 establishes a process for victims of identity theft to reclaim their identity and gather evidence to assist law enforcement to apprehend the identity thieves.

Although Congress has provided for penalties for identity theft, we have done little to help victims reclaim their identity. Identity theft can wreak havoc on a victim's life that can take an extreme financial and emotional toll. Victims usually have to become their own sleuth to clear their names. It takes a victim an average of 175 hours and over $800 of out-of-pocket expenses to clear their names. We need to provide consumers and businesses alike with a clear process to help victims of identity theft recover their good name and good credit, and reduce identity theft fraud.

- The Reclaim Your Identity Act of 2001 creates a simple process that allows a victim and law enforcement access to business records that relate to the identity theft fraud.
- The bill also requires consumer credit reporting agencies to block bad credit reports that result from identity theft.
- The bill clarifies that the two-year statute of limitations on Fair Credit Reporting Act actions would not begin until the victim discovers the fraud.
- Most identity theft law enforcement is undertaken at the state and local level. The bill requires the federal government to examine how it can better help state and local law enforcement through appropriate federal resources and better information sharing between federal and state or local agencies.

The Consumers Union, Fraternal Order of Police, Police Executive Research Forum, Identity Theft Resource Center, Privacy Rights Clearinghouse, U.S. Public Interest Research Group all support this bill. The National Association of Attorneys General supports federal identity theft legislation. If you are interested in cosponsoring the Reclaim Your Identity Act of 2001 or have any questions about this legislation, please have your staff contact Stacy Baird at 224–3441.

Sincerely,

MARIA CANTWELL,
U.S. Senator.

RECLAIM YOUR IDENTITY ACT OF 2001

SENATOR MARIA CANTWELL

The Reclaim Your Identity Act establishes a nation-wide process for victims of identity theft to obtain the evidence to reclaim their identity and assist law enforcement to find the identity thieves, requires consumer credit reporting agencies to block reporting of bad credit that arises from identity theft and extends the statute of limitations for the Fair Credit Reporting Act to two years after the consumer discovers the misrepresentation. The Act:

(1) **Empowers consumers to reclaim their identity:** The Reclaim Your Identity Act provides that where (a) a victim of identity theft requests of a business (including telecommunications and utilities companies) that has records related to a fraud based on an identity theft (such as applications or bills), and (b) submits to the business, any of the following as the business requires, a copy of the police report, the Federal Trade Commission standardized Identity Theft Affidavit or any other affidavit of fact of the business' choosing, the business must provide, at no charge, copies of those business records to the victim or a law enforcement agency or officer designated by the victim within 10 days of the victim's request. The business may decline to disclose records where it believes, in the exercise of good faith and reasonable judgment, the request is based on a misrepresentation of facts. Further, a business is exempt from liability for any disclosure undertaken in good faith to further a prosecution of identity theft or assist the victim.

(2) **Protects consumers' good name from bad credit generated by fraud:** The Reclaim Your Identity Act amends the Fair Credit Reporting Act to require consumer credit reporting agencies to block information that appears on a victim's credit report as a result of identity theft provided the victim did not knowingly obtain goods, services or money as a result of the blocked transaction.

(3) **Enhances multi-jurisdiction enforcement:** The Reclaim Your Identity Act amends the Internet False Identification Prevention Act to expand the jurisdiction and membership of the coordinating committee currently studying enforcement of *federal* identity theft law to examine *state and local enforcement* problems and identify ways the federal government can assist state and local law enforcement in addressing identity theft and related crimes.

(4) **Increases information flow to aid anti-terrorist activities:** The Reclaim Your Identity Act also amends the Internet False Identification Prevention Act to expand the jurisdiction of the coordinating committee to address how the federal government can best provide timely and current information regarding terrorists or terrorist activity as such information relates to identity theft.

(5) **Gives businesses new tools to pursue identity thieves:** The Reclaim Your Identity Act gives businesses a new avenue to pursue perpetrators of identity theft fraud by amending Title 18 to make identity theft *under state* law a predicate for federal RICO violation.

(6) **Preserves consumer rights to claim damages:** In response to the Supreme Court decision in *TRW v. Andrews*, the Reclaim Your Identity Act amends the Fair Credit Reporting Act to provide that the two-year statute of limitations for a claim starts *when the consumer discovers* a misrepresentation has been committed.

(7) **Gives State Attorneys General additional legal tools:** The Reclaim Your Identity Act provides that State Attorneys General may bring a suit in federal court on behalf of state citizens for violation of the Act.

Chairperson FEINSTEIN. Thanks very much, Senator, and thank you for your leadership.

I will introduce you now, Mr. Beales, and then when Senator Kyl comes we will hear his statement. I hope that is all right.

Howard Beales is the Director of the Bureau of Consumer Protection at the Federal Trade Commission. Mr. Beales began his career at the FTC in 1977 as an economist specializing in consumer protection problems. Now, as Director, he oversees the work of some 152 lawyers and a $77 million budget. His major areas of expertise

and interest include law and economics, and aspects of government regulation of the economy.

Mr. Beales, may I ask you this, if you could summarize your testimony and take about five minutes and then we will put the bulk of your testimony in the record, and then we will have an opportunity to ask you questions prior to the next panel.

STATEMENT OF HOWARD BEALES, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, WASHINGTON, DC

Mr. BEALES. Sure, that would be fine.

Chairperson FEINSTEIN. Thanks very much.

Mr. BEALES. Madam Chairman and members of the committee, thank you very much for the opportunity to appear here today.

The Commission has had the privilege of testifying before this subcommittee several times in the past, each time updating you on our activities under the 1998 Identity Theft Act and highlighting what we are learning from the data we collect.

We all know that identity theft is a major problem. Each week, we receive almost 3,000 phone calls from consumers. It is a crime that seriously harms its victims and injures our financial system. And until the passage of the 1998 act, it all too often flew under the radar of law enforcement.

Today, I will describe the Commission's recent efforts to assist consumers, support law enforcement, and coordinate with industry in this troubling area. First, let me start with our consumer efforts.

In 2000, this committee heard from Maureen Mitchell, a victim of identity theft. In her testimony, she provided a list of suggestions on how the system could be improved. One of her ideas was to create a single form to dispute charges and fraudulent accounts. This would eliminate the burden of filling out a separate lengthy form for each creditor or business where the identity thief struck.

We therefore began the process of developing a standard fraud affidavit, working closely with financial institutions, the consumer reporting agencies, consumer advocates, and others. We completed this project several months ago and now identity theft victims have a single form to use in disputing fraudulent accounts. That is the front page over here, and this is sort of the whole form and the instructions.

Already, the three major consumer reporting agencies—Chase Manhattan, the Bank of America, AT&T—and about 40 other businesses and groups have formally endorsed the affidavit and have agreed to accept it in lieu of their own forms. We believe that many more creditors and businesses accept the form as a matter of course. In fact, we haven't heard about anybody yet that has refused it.

Our next major initiative will be to try to streamline the fraud alert process. Because there are three major credit reporting agencies, consumers must make three separate phone calls to lock down their credit if they are victims. We are now discussing a project to transmit from our hotline the consumer's request for a fraud alert directly to the credit reporting agencies. This would eliminate three phone calls from the victim's "to do" list. There are many technical challenges to this project, but we are hopeful that at the end of the

day we will be able to further lighten the burden on identity theft victims.

Another recent FTC initiative recognizes that identity thieves strike all segments of the population, including non–English speakers. We therefore released "Robo de Identidad," a Spanish version of our booklet "When Bad Things Happen to Your Good Name." We also released the uniform affidavit in Spanish as well.

One of the ways we work with our colleagues in the criminal enforcement field is through our I.D. Theft Data Clearinghouse. The clearinghouse receives complaints from consumers who reach us through our toll-free number, our online complaint form, and through the mail.

Our interaction with consumers is a two-way street. Our phone counselors give them information that they need to repair their finances. The consumers as crime victims provide us with information about the theft of their identity. This information is accessible by more than 270 law enforcement agencies around the country through the clearinghouse.

What makes the system work is the fact that the clearinghouse provides a single nationwide repository of identity theft complaints. The 1998 Act, spearheaded by this subcommittee, recognized that consolidation of complaint data offered the most efficient and effective means to support law enforcement across local, State and Federal levels.

The increase in our call volume shows that consumers are increasingly aware that the FTC is the place for victims to turn. We are going to continue build on our outreach efforts to grow the clearinghouse and increase its value to law enforcement.

In order to increase law enforcement's use of the data, we have a new project to develop preliminary investigative reports and send them to the Secret Service's financial crime task forces around the country. The investigative reports identify particularly egregious episodes of identity theft. Our staff then builds out the cases with intelligence from a number of other sources.

We have been greatly assisted in this effort by a special agent from the Secret Service who has been detailed full-time to work with our identity theft team. The project is in its infancy, but we are hopeful that it will encourage and support prosecution of identity theft.

We also want to be sure that criminal law enforcement agencies are aware of our database and how it can be used to help investigate and prosecute these cases. We have therefore just kicked off an I.D. theft training program to enable detectives, cops on the beat, and investigators to identify and pursue cases of identity theft. Our first session in Washington last week attracted more than 100 law enforcement officers. We are following with training in Chicago, Dallas and San Francisco in the next few months.

Another critical area is coordination with industry. I have mentioned one area, the affidavit, and the one-call fraud alert. Our next effort is focused on prevention. We are hosting a conference to look at industry best practices for preventing I.D. theft to encourage the spread of those best practices among other businesses. How do businesses successfully protect themselves and their customers? We think we can learn a lot from that.

There is much to be done in educating consumers and increasing the law enforcement response and in focusing industry, but we are pleased that we have found a willingness to help and cooperate.

I would be pleased to answer your questions.

[The prepared statement of Mr. Beales follows:]

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON IDENTITY THEFT: THE FTC'S RESPONSE

I. INTRODUCTION

Madam Chairman, and members of the Committee, I am Howard Beales, Director of the Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on one of the most serious consequences that can result from the misuse of consumers' personal information: identity theft.

The passage of the Identity Theft and Assumption Deterrence Act of 1998 ("Identity Theft Act")[2] brought identity theft to the forefront of the public's attention. Media attention and high profile cases[3] have heightened concerns about the serious injury caused by identity theft.

In particular, the specter of identity theft has focused consumers' concern about the misuse of their personally identifying information. There is good reason for this concern. Identity theft can result in temporary and sometimes permanent financial loss when wages are garnished, tax refunds are withheld, or liens are placed on victims' property as a result of someone else's criminal use of their identity. Beyond direct financial loss, consumers report being denied employment, credit, loans (including mortgages and student loans), government benefits, utility and telecommunications services, and apartment leases when credit reports and background checks are littered with the fraudulently incurred debts or wrongful criminal records of an identity thief.

The 1998 legislation positioned the FTC to play a key role in the national dialogue on identity theft. The FTC enforces a number of laws that address consumers' privacy,[4] and intends to increase substantially the resources devoted to privacy protection. The FTD's identity theft program is an important part of that initiative. Consumer and victim assistance, data sharing with law enforcement and financial institutions, and cooperative efforts with the private sector are among the most visible examples of the FTC's efforts.[5] Recent FTC initiatives, including a Spanish language version of our consumer brochure, law enforcement training, and a standard Identity Theft Affidavit, complement the measures we have already undertaken to fulfill our mandate under the 1998 Act.

II. THE FTC'S RESPONSE TO THE IDENTITY THEFT ACT

The Identity Theft Act directed the Commission to establish procedures to: log the receipt of complaints by victims of identity theft; provide identity theft victims with

[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. The statistical information summarized in this statement covers the period of time from January 1 through December 31, 2001.

[2] Pub. L. No. 105–318, 112 Stat. 3010 (1998).

[3] Celebrities including Ted Turner, Martha Stewart and Oprah Winfrey have been reported in the press as being victims of identity theft. Jenny Lynn Bader, Paranoid Lately? You May Have Good Reason, N.Y. Times, March 25, 2001, at 4, Section 4.

[4] *See, e.g.*, Federal Trade Commission Act, 15 U.S.C. § 41 *et seq.* (prohibiting deceptive or unfair acts or practices, including violations of stated privacy policies); Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* (addressing the accuracy, dissemination, and integrity of consumer reports); Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6101 *et seq.* (including the Telemarketing Sales Rule, 16 C.F.R. Part 310) (prohibiting telemarketers from calling at odd hours;, engaging in harassing patters of calls, and failing to disclose the identity of the seller and purpose of the call); Children's Online Privacy Protection Act, 15 U.S.C. § 6501 *et seq*. (prohibiting the collection of personally identifiable information from young children without their parents' consent); Identify Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 (directing the FTC to collect identity theft complaints, refer them to the appropriate credit bureaus and law enforcement agencies, and provide victim assistance); Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.* (requiring financial institutions to provide notices to consumers and allowing consumers (with some exceptions) to choose whether their financial institutions may share their information with third parties).

[5] Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority.

informational materials; and refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.[6] To fulfill the purposes of the Act, the Commission implemented a plan with three principal components: a toll-free telephone hotline, a datebase of identity theft complaints, and consumer and business education.

(1) Toll Free Hotline. The Commission established its toll-free telephone number (the "hotline"), 1–877–ID–THEFT (438–4338) in November 1999. The hotline now responds to an average of over 3000 calls per week. When consumers call to report identity theft, the hotline counselors enter information from their complaints into the Identity Theft Data Clearinghouse (the "Clearinghouse")—a centralized database used to aid law enforcement and track trends involving identity theft.

The counselors advise the callers to contact the credit reporting agencies and the entities where the fraudulent accounts were opened in order to place a fraud alert on their credit files and shut down the fraudulent accounts, respectively. They also encourage consumers to contact their local police departments to file a police report, both because local law enforcement may be in the best position to catch and prosecute identity thieves and because a police report helps consumers demonstrate to creditors and debt collectors that they are in fact genuine victims of identity theft. Forty-seven states have enacted their own identity theft laws and the FTC hotline phone counselors, in appropriate circumstances, will refer consumers to otherstate and local authorities. Lastly, when another federal agency has a program in place to assist consumers, callers are referred to that agency.[7]

Of the callers to our hotline, thirty-four percent are seeking information about how to guard against identity theft.[8] The phone counselors provide suggestions on steps they should take to minimize their risk.

(2) Identity theft complaint database. The information that the consumers share with the phone counselors can provide the foundation for investigation. The telephone counselors enter the complaints received by the FTC through the hotline, by mail, and through the FTC's secure on-line theft complaint form into the FTC's Clearinghouse database. In addition, the Social Security Administration's Office of Inspector General transfers into the Clearinghouse complaints of identity theft received by its consumer hotline.

The Clearinghouse is the federal government's centralized repository of consumer identity theft complaint information. It contains detailed information regarding the identity theft victim, the suspect, and the ways the identity thief misused the victim's personal information. More than 270 law enforcement agencies nationwide have signed confidentiality agreements that grant them membership and access to the Identity Theft Data Clearinghouse. The Clearinghouse information is available directly on members' desktop PCs via the FTC's secure law enforcement Web site, Consumer Sentinel. Access to the Clearinghouse information supports law enforcement agencies' efforts to combat identity theft by providing a range of complaints from which to augment their ongoing investigations and spot new patterns of illegal activity.

(3) Consumer and business education. The FTC has taken the lead in coordinating with other government agencies and organizations to develop and disseminate comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime. For example, in collaboration with other federal agencies, the FTC published a comprehensive informational booklet, Identity Theft: When Bad Things Happen to Your Good Name, in February 2000. Since its publication through February 2002, the FTC has distributed more than 600,000 hard copies of the booklet and recorded over 609,500 visits to our Web version. Other federal agencies have also printed and distributed this publication.

Consumers can also find comprehensive information about preventing and recovering from identify theft at the FTC's identity theft Web site, *www.consumer.gov/idtheft*. The site also links to a secure Web-based complaint form, allowing consumers to send complaints directly to the Clearinghouse. The FTC now receives an average of 400 complaints per week via the Internet; overall, more than 18,000 victims filed their identity theft complaints online as of the end of December 2001. The

---

[6] Pub. L. No. 105–318, 112 Stat. 3010 (1998)(Codified at 18 U.S.C. § 1028(a) note).

[7] For example, we may refer consumers to the Social Security Administration or their state department of motor vehicles.

[8] This statistic reflects the experience only of the consumers who contacted the FTC directly, and does not reflect data contributed by the Social Security Administration, Office of Inspector General ("SSA–OIG"). See infra at 4. While the SSA–OIG collects many of the same fields of data, they do not collect identical data. Unless otherwise noted, as in Section IV, the statistics used in this testimony include data from FTC and SSA–OIG.

FTC's identity theft Web site had more than 699,000 hits since it was launched in February 2000.

To expand the reach of our consumer education message, the FTC has begun an outreach effort to Spanish-speaking victims of identity theft. Just last month, we released a Spanish version of the Identity Theft booklet (Robo de Identidad: Algo malo puede pasarle a su buen nombre) and the ID Theft Affidavit (discussed below in Section III). In addition, we have added Spanish-speaking phone counselors to our hotline staff. We will soon launch a Spanish version of our online complaint form.

III. THE FTC'S RECENT COLLABORATIVE AND OUTREACH EFFORTS

Over the past year, the Commission has worked closely with other government agencies and private entities to encourage the investigation and prosecution of identity theft cases, and help consumers resolve identity theft problems.

(1) Law Enforcement. One of our goals is to provide support for identity theft prosecutions nationwide. In the past year, the Commission launched an identity theft case referral program in coordination with the United States Secret Service, which assigned a special agent on a full-time basis to the Commission to assist with identity theft issues.[9] The identity theft team, assisted by the special agent, develops case leads by examining significant patterns of identity theft activity in the database and by refining the data through the use of additional investigative resources. Then, the team refers the case leads to one of the Financial Crimes Task Forces located throughout the country for further investigation and potential prosecution.

We provide support for law enforcement in other ways as well. Just last week, the FTC, in cooperation with the Department of Justice and the United States Secret Service, initiated a full day identity theft training seminar for state and local law enforcement officers. This first session was held in Washington, D.C.; subsequent sessions are planned in Chicago, Dallas, and San Francisco. The training seminar provides officers with technical skills and resources to enhance their efforts to combat identity theft, including strategies for both traditional and high-tech investigations. The training also identifies key components for successful actions by local, state, and federal prosecutors, and identifies resources, such as the Clearinghouse database, that are available to law enforcement when conducting identity theft investigations. Our goal is to encourage the prosecution of these cases at all levels of government.

(2) Private Industry. Identity theft victims spend significant time and effort restoring their good name and financial histories. Such burdens result, in part, from the need to complete a different fraud affidavit for each different creditor where the identity thief opened or used an account in their name.[10] To reduce that burden, the FTC worked to develop the ID Theft Affidavit ("Affidavit"). The Affidavit was the culmination of an effort we coordinated with private industry and consumer advocates to create a standard form for victims to use in absolving identity theft debts with each of the creditors where identity thieves opened accounts. The Affidavit is accepted by the three major credit reporting agencies and many creditors. From its release in August 2001 through February 2002, we have distributed more than 112,000 print copies of the Affidavit. There have also been nearly 185,000 hits to the Web version.

The FTC will continue working with private sector financial institutions to find additional ways to assist consumers. For example, we plan to work with businesses to highlight the importance of securing business records containing personally identifying information from would-be identity thieves, and providing consumers with notification in the event that their business records are compromised.

The FTC is examining other ways to lessen the difficulties and burdens faced by identity theft victims. One approach under consideration is to develop a joint "fraud alert initiative" with the three major credit reporting agencies ("CRAs"). This initiative would allow the FTC to transmit regularly to the three major CRAs requests from identity theft victims that fraud alerts be placed on their consumer report and copies of their reports be sent to them. This would eliminate the victim's need to contact each of the three major CRAs separately.

The CRAs have also asked the FTC to help promote their recent "police report initiative," which follows an earlier program supported by the FTC. After learning from our first twelve months of data that over 35% of victims contacting the FTC

[9] The referral program complements the regular use of the database by all law enforcers from their desk top computers.

[10] See ID Theft: When Bad Things Happen to Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Judiciary Comm. 106th Cong. (2000) (statement of Mrs. Maureen Mitchell, Identity Theft Victim).

were not able to file police reports on identity theft, the FTC began working with the International Association of Chiefs of Police ("IACP") to encourage local police officers to write police reports for victims of identity theft. In November 2000, the IACP passed a Resolution in support of providing police reports to victims of identity theft and referring victims to the FTC's hotline.[11] In 2001, the consumers reporting to the FTC that the police would not issue a report dropped to 18%.[12] Under their new initiative, the CRAs have agreed to block inaccurate information resulting from the identity thief's activities from a victim's credit report if the victim provides the CRA with a police report on the incident. This program further speeds the process of rehabilitating the victim's good name.

IV. IDENTITY THEFT: HOW IT HAPPENS

Access to someone's personal information, through legal or illegal means, is the key to identity theft. Unlike most crimes where the victim is immediately aware of the assault, identity theft is often silent and invisible. Identity thieves do not need direct contact with their victims. All they need is access to some key components of a victim's personal information, which, for most Americans, may be maintained and used by numerous different public and private entities. Thus, it is hardly surprising that nearly 80% of the victims who report identity theft to the FTC do not know how or where the identity thief obtained their personal information.[13]

Some victims can recall an event or incident that they believe led to the identity theft. Eight percent of the victims who contacted the FTC had their wallet or purse lost or stolen. Three percent of the victims discovered that their mail had been stolen or that a fraudulent address change had been filed with a creditor. One percent of victims contacting the FTC recalled giving out personal information in response to a solicitation over the telephone or Internet, and another 1% reported that their identification had been stolen from their residence or car.[14]

Notably, 13% of the victims who contact the FTC report that they personally know the suspect. These relationships include family members (6%), other personal relationships, such as friends (3%), neighbors (2%), "significant others" or roommates (1%), or someone from the victim's workplace (1%).

The FTC also receives reports of identity theft from victims who learn of it only upon notification by their employer on an entity with whom they do business that their employee or customer records were stolen. This is called "business record identity theft." Between March 2000 through late December 2001, the Clearinghouse received reports regarding thirty-five different companies or institutions in which identity thieves stole records containing employees' or clients' personal information. The institutions included hospitals, tax preparers, municipalities and schools.[15] In many of these instances the records were stolen by insiders. Some of these thieves sold the records, while others exploited the information themselves. Some of the targeted companies sought our assistance in dealing with the aftermath of the theft, and in other cases, we reached out to them to offer assistance. When we provide assistance, we encourage the entities to contact the persons whose records were compromised, notify them that they were potential victims of identity theft, and advise them to contact the FTC's hotline.

While most victims do not know how or where the identity thief obtained their personal information, 68% of the complaints in the Clearinghouse do contain some identifying information about the suspect, such as a name, address, or phone number. This includes any identifying information victims can provide about the suspect, which might be gleaned from the bills, letters or phones calls of would-be creditors

---

[11] While this resolution is not binding, it sends an important message to the police around the country. The FTC has conveyed the same message in numerous law enforcement conferences across the country.

[12] Ninety-eight percent of victims reported whether they had been able to file a police report. The statistics regarding filing police reports reflect the experience only of the consumers who contacted the FTC directly, and do not reflect data contributed by the SSA–OIG, which does not collect such information. See supra at note 6.

[13] Nearly all of the statistics in Section IV reflect the experience only of the consumers who contacted the FTC directly, and do not reflect data contributed by the SSA–OIG. As indicated at note 6 supra, this is because the SSA–OIG data do not contain the same fields as the FTC data. Again, these statistics cover calendar year 2001.

[14] Recent Internet scams reportedly have emerged that try to trick consumers into revealing their information. For example, consumers report receiving emails from an entity purporting to be their Internet service provider, health insurer, or bank. The scammers request personal information, to confirm the consumer's identity or eligibility for a program. In reality, these are traps for unwary consumers. We are looking for such scams and will take appropriate action.

[15] Jacob H. Fries, Worker Accused of Selling Colleagues' ID's Online, N.Y. Times, March 2, 2002, at B2.

and debt collectors, or from a victim's report. Such information about suspects allows law enforcement investigators to link seemingly unrelated complaints of identity theft to a common suspect.[16]

V. SUMMARY OF DATABASE INFORMATION

The Clearinghouse database has been in operation for more than two years.[17] For calendar year 2001, the Clearinghouse database contains over 86,000 complaints from ID theft victims. It also contains over 31,000 inquiries from consumers concerned about becoming victims of identity theft. These figures include contacts made directly to the FTC and data contributed by SSA–OIG.

While not comprehensive, information from the database can reveal information about the nature of identity theft activity. For example, the data show that California has the greatest overall number of victims in the FTC's database, followed by New York, Texas, Florida, and Illinois. On a per capita basis, per 100,000 citizens, the District of Columbia ranks first, followed by California, Nevada, Maryland and New York. The cities with the highest numbers of victims reporting to the database are New York, Chicago, Los Angeles, Houston and Miami.

Eighty-eight percent of victims reporting to the FTC provide their age.[18] The largest number of these victims (28%) were in their thirties. The next largest group includes consumers from age eighteen to twenty-nine (26%), followed by consumers in their forties (22%). Consumers in their fifties comprised 13%, and those age 60 and over comprised 9%, of the victims. Minors under 18 years of age comprised 2% of the victims.

As noted above, consumers often do not become aware of the crime for some time. Forty-four percent of victims who contact the FTC provide information on when the identity theft occurred and when they discovered it. The majority of these victims (69%) reported discovering the identity theft within 6 months of its first occurrence.[19] In fact, 44% noticed the identity theft within one month of its occurrence. However, 5% were unaware of the theft for longer than five years. On average, 12 months elapsed between the date the identity theft occurred and when the victim discovered it.

Thirty-five percent of the victims had not yet notified any credit bureau at the time they contacted the FTC,[20] 46% had not yet notified any of the financial institutions involved.[21] Fifty-four percent of the victims had not yet notified their local police department of the identity theft. By advising the callers to take these critical steps, we enable many victims to get through the recovery process more efficiently and effectively.

The Clearinghouse data, which represents complaints received by both the FTC and the SSA–OIG, also reveal how the thieves use the stolen identifying information. This data, summarized below, help provide a broad picture of the forms identity theft can take.[22]

• Credit Card Fraud: Forty-two percent of the victims in the Clearinghouse report credit card fraud. Sixty-two percent of these victims indicate that one or more new credit cards were opened in the victims' name. Twenty-four percent of these victims indicate that unauthorized charges were made on an existing credit card. Thirteen percent of the credit card fraud victims were not specific as to new or existing credit.

• Unauthorized Telecommunications or Utility Services: Twenty percent of the victims in the Clearinghouse report that the identity thief obtained unauthorized telecommunications or utility equipment or services in their name. New wireless telecommunications equipment and service comprised 48% of these complaints, new land line telephone service or equipment comprised 26%, new utilities such as elec-

[16] Suspect identifying information is collected both by FTC and SSA–OIG. This statistic includes data contributed by the SSA–OIG to the Clearinghouse.

[17] The Clearinghouse was established in November 1999. Because it is relatively new, the information in the database may be influenced by geographical differences in consumer awareness of the FTC's identity theft hotline and database.

[18] The statistics regarding consumers' age reflect the experience only of the consumers who contacted the FTC directly, and do not reflect data contributed by the SSA–OIG, which does not collect information about the victim's age. See supra at note 6.

[19] The statistics regarding when victims discover the crime and what entities they have notified reflect the experience only of the consumers who contacted the FTC directly, and do not reflect data contributed by the SSA–OIG, which does not collect such information. See supra at note 6.

[20] Ninety-five percent of victims reported whether they had contacted any credit bureaus.

[21] Sixty-three percent of victims reported whether they had notified any financial institutions.

[22] Many consumers experience more than one form of identity theft. Therefore, the percentages represent the number of consumers whose information was used for each various illegal purpose.

tric or cable service comprised 12%, 11% of these complaints were not specific, and 2% comprised unauthorized charges to the victims' existing telecommunications or utility accounts.

• Bank Fraud: Thirteen percent of the victims report fraud on their demand deposit (checking or savings) accounts. Forty-seven percent of these victims report fraudulent checks written on their existing account, 20% report a new bank account opened in their name, 15% report unauthorized electronic withdrawals from their account, and 18% of these complaints were not specific.

• Employment: Nine percent of the victims in the database report that the identity thief used their personal information for employment purposes.

• Fraudulent Loans: Seven percent of the victims report that the identity thief obtained a loan in their name. Fifty-three percent of these complaints relate to a personal, student, or business loan, 28% concern auto loans or leases, 10% concern real estate loans, and 9% are unspecified.

• Government Documents or Benefits: Six percent of the victims report that the identity thief obtained government benefits or forged government documents in their name. Forty-four percent of these victims report a false driver's license, 11% report a false social security card, and 4% report the falsification of other government documents. Thirty-one percent report fraudulent claims for tax returns, 6% report fraudulent claims for government benefits, and 3% of these victims were not specific.

• Other Identity Theft: Nineteen percent of the victims in the database reported various other types of identity theft. Nine percent of these victims report that the thief assumed their identity to evade legal sanctions and criminal records (thus leaving the victim with a wrongful criminal or other legal record), 9% report that the thief obtained medical services, 6% report that the thief opened or accessed Internet accounts, 5% report that the thief leased a residence, 2% report that the thief declared bankruptcy in their name, 1% report that the thief purchased or traded in securities and investments, and 69% of these complaints were miscellaneous or unspecified.

• Multiple Types: Twenty percent of the victims in the database reported experiencing more than one of the above types of identity theft.

VI. CONCLUSION

Identity theft, once an unknown term, is now the subject of day time talk shows. The economic and non-economic injury caused by the misuse of consumers' personal information is significant. But there are real and positive steps we can take to alleviate the harm to consumers, and reduce the incidence of this crime. We are committed to working with our partners in the public and private sectors and will continue to forge a comprehensive approach to this challenge. I would be pleased to answer any questions you may have.

Chairperson FEINSTEIN. Thanks very much, Mr. Beales. I know we do have questions, but I would really like to thank you for the work of your agency. You are right. Your agency has testified before us before, and I just want you to know how much we appreciate your cooperation.

We are joined by Senator Sessions and I am delighted that he is here and has an interest in this subject.

Senator, would you like to make a statement?

STATEMENT OF HON. JEFF SESSIONS, A U.S. SENATOR FROM THE STATE OF ALABAMA

Senator SESSIONS. Just briefly, as a Federal prosecutor for a number of years, we were involved in matters involving fraudulent use of identification, particularly to defraud banks, as usually one thing goes to another, or individuals.

When you look at what really happens and what really needs to occur to have a surge in prosecutions and identification of people who do these things, it has got to be a partnership between the lowest level of the Federal, State and local officials and those who are most involved in seeing the fraudulent activity.

When they work together—and we created such a task force in my district—the prosecutions surge, and many of them were small cases that Federal officials say, well, you don't want to fool with. But they go from State to State; they rip off 50 people at $1,000, $2,000 each, and it is disrupting their lives in a substantial way.

So I think it is a bigger problem than people realize and it is easier to deal with if we come up with the right solution, because there are not that many people doing it and if the word gets out that you are going to get caught and get whacked if you do it, you can stop it. If the word gets out that you can do these kinds of nonviolent crimes and you don't run up too much money and nobody cares, you will see more of that crime.

That is all I would want to add, and thank you for your leadership in trying to focus our attention on it. It is an important matter. It disrupts the lives of people substantially.

Chairperson FEINSTEIN. Well, thank you very much.

I held a hearing actually in Los Angeles in the last session of the Congress on the subject, and the sheriff of Los Angeles County, which, of course, is the biggest county in America—it is such a problem that he has set up a special unit. Interestingly enough, the average identity theft loss in the Nation is $18,000. That is a lot of money.

Senator SESSIONS. That is more than I thought.

Chairperson FEINSTEIN. Yes, because they pick their people. The other thing is the average time it takes for an individual to regain their identity is, I think, 18 months, which is a long time when you have lost your identity and you are struggling to get it back.

Mr. Beales, let me begin. I want to ask you a question about truncation—I hate the word—of credit card numbers. Printed store receipts are real assets for identity thefts because they often contain a card-holder's entire credit card number.

I have introduced legislation prohibiting companies from printing more than the last five digits of any credit card on any receipt provided by the card-holder. The State of California, with the support of the Better Business Bureau, has just established a similar truncation law.

Do you know how it is working, and what the FTC's view of such a truncation requirement is?

Mr. BEALES. Well, I have to say that the views that I am giving today are my own views and not the Commission's. The prepared statement is obviously the Commission's views, but my comments are my own.

We, too, find that credit card receipts are an important source of information for identity thieves, and we urge in our consumer education materials for consumers to be careful with those receipts and not to leave them behind and not to leave them where other people can get a hold of them.

Truncation is a way to protect consumers from their own mistakes, if you will, that we are seeing increasingly happen in the private sector on a voluntary basis. I know a lot of the receipts I get these days seem to display just the truncated credit card number, and that is a great idea.

We don't really know how much of an impact it would have on the prevalence of identity theft, in part because most of the time

our main source of information, which is the victim, doesn't know how the thief got their information. That is just hard for consumers to tell. As long as it is phased in in a way that accommodates the life of the equipment and as long as it is done in a way that makes it easy for small businesses that are still using manual systems, it seems like an excellent idea.

Chairperson FEINSTEIN. When you are at a restaurant and you give your credit card and you get back the little ticket that you sign, and it sometimes has a duplicate, I mean I was told several times "we don't furnish duplicates." Well, it is not really the consumer's fault if you are told that. Let's say you do and the waiter may have taken the second receipt. He has got the number, he has got your signature. Or if you don't tear it up in small enough pieces, somebody picks up the pieces and they have got it, or it falls out of your purse or your pocket, for example.

It is really a very important document, and I think you are right in warning people and trying to get people adjusted to it. On the other hand, the truncation of a credit card number really stops a thief cold. So I am going to try to find out how California is doing with that.

Let me ask you about the fraud alert. One of the witnesses on our second panel, Sallie Twentyman, is a victim of identity theft. Using her name and Social Security number, a thief took her credit card account and obtained $13,000 in cash advances. Even after she placed a fraud alert on her account, two credit cards were subsequently issued to the identity thief.

Now, in your view, how effective is the current voluntary fraud alert system? Should fraud alerts be codified and subject to FTC supervision?

Mr. BEALES. Well, I think we are frankly puzzled by fraud alerts that get ignored, and don't completely understand how or why that happens. One possibility is simply people making mistakes. That certainly will happen in some cases in the best of circumstances.

A potential fear—and we don't know to what extent this is an issue now, but there are some people who encourage fraud alerts where there is no fraud, and that unfortunately has the other effect of encouraging people to ignore fraud alerts when there is fraud. A fraud alert needs to identify fraud and the financial institutions looking at whether to issue credit or not need to take that seriously.

Chairperson FEINSTEIN. Well, would the FTC consider fining a merchant who ignored a fraud alert and issued another credit card to the thief?

Mr. BEALES. Well, we would have to find either a deceptive practice or an unfair practice in what the creditor was doing.

Chairperson FEINSTEIN. Absolutely.

Mr. BEALES. And the difficulty is this is an area where there is in many cases, or can be in many cases a benefit to the consumer of being able to get credit immediately, where the fraud alert might get in the way.

For example, as a hypothetical that somebody on my staff told me about happening to them, somebody puts on a fraud alert. It is two years later. They have forgotten about the fraud alert. They haven't had problems in the meantime and they go to establish in-

stant credit somewhere again. With identification, maybe they can talk the merchant into issuing credit immediately. There is a real benefit to the consumer in that sort of circumstance.

Chairperson FEINSTEIN. Well, that is right. Thank you.

Senator Sessions, do you have questions?

Senator SESSIONS. Under the Uniform Commercial Code, if a retailer ignores a fraud alert, are they, rather than the person whose identity is stolen, ultimately liable for the purchases? Is the customer not required to pay? It doesn't always get decided promptly, leaving the victim in a lot of uncertainty, but isn't that the way it is supposed to work? Isn't that a penalty against them?

Mr. BEALES. That is ordinarily the case. It is the credit issuer that is ultimately liable for fraudulent credit and the consumer isn't going to have to pay. But it does take some time and effort and it is a substantial inconvenience, at the very least, to the consumer.

Senator SESSIONS. You mentioned a task force or team you are putting together involving the Secret Service. Would you tell me a little bit more about what that is about?

Mr. BEALES. Well, there are a series of task forces around the country that involve us and the Secret Service, the Justice Department, and State and local prosecutors.

Senator SESSIONS. At what level is that? Is this county, city level, or is it regional or what?

Mr. BEALES. It is regional, but it includes State and local officials. I mean, it is not simply the Federal agencies on a regional basis. It tries to bring in the State and local prosecutors, as well, because they are an important part of this puzzle. I think you are right.

Senator SESSIONS. Well, just for example, we had an innovative Secret Service agent in Mobile, the head of the Secret Service, and he had monthly luncheons that I frequently attended. We had a committed Assistant United States Attorney, and maybe 7 or 8 Federal investigators and probably 10, 15 local, and many more really because the local police are the ones who are hearing about this first usually. It worked exceedingly well. Prosecutions went up, and once we learned how to prosecute the cases and how to identify cases that needed to be prosecuted, things went, I thought, very well.

I believe that more times than you would think, Madam Chairman, the people that were caught had done it in New Orleans or Atlanta or Memphis, and things got hot there and they just left and came to the next town. They would live there and run up $100,000 or more.

At first, it would take some time to identify this person, and then a lot of Federal prosecutors seem to believe that if it is not $100,000 in fraud, they shouldn't investigate it. Sometimes, we haven't gotten it down to the level that we need to have it operate at.

I just believe, as a practical matter, we could do a lot better job. I think United States Attorneys need to know that they need to prosecute some of these cases. The actual amount in that district that is fraudulent may not meet the highest standards that they normally would look at, but you have to realize they may go to the

next town, the next town and the next town, and they need to be stopped. So I just believe you are on the right track with that.

Madam Chairman, I thank you for your leadership. I look forward to studying your legislation in more detail, but you are clearly stepping out in the right direction and I thank you.

Chairperson FEINSTEIN. Thanks, Senator, very much.

Senator Cantwell?

Senator CANTWELL. Thank you, Madam Chairman.

Again, Mr. Beales, thank you for being here this morning. I appreciate the hard work that the agency has done in trying to fight identity theft and provide information on a national basis. I would like to follow on some of the questions that Senator Feinstein asked in the sense of where do we go from here, given that this crime is continuing to be one of the fastest growing in the country.

I guess first I would like to start with this issue on the statute of limitations. I know that your agency can't by your own actions change that, but what is your thought on that particular challenge that we face? Do you believe that we should change the statute of limitations?

Mr. BEALES. Well, I think there are pros and cons, and I don't have a clear view of what would be the best solution here. I can appreciate the difficulties that a discovery rule creates for people who have to maintain records to address possible problems that may have occurred well in the past. And that is particularly true in the credit reporting agency, where the data sort of expires after seven years under the Fair Credit Reporting Act, but the statute of limitations may not if it is strictly discovery-based.

Most consumers in our data, about 70 percent, discover the identity theft within the first 6 months, but there is a tale of about 5 percent of cases where it is more than 5 years before the crime was discovered. What we are doing is try to look more closely at those cases that take a long time to discover to see if there is anything about those cases that might let you shape a statute of limitations change that would target them without affecting the vast majority of cases where consumers find out quickly. At this point, we don't know anything about that, but we are going to try to look at those cases to see what they look like.

Senator CANTWELL. The other issue that obviously has a lot of concern is the 30-day compliance time frame by which information should be corrected. Do you get a lot of complaints at the FTC about that?

Mr. BEALES. We do get complaints about the time and how long it takes in a number of instances.

Senator CANTWELL. And most instances aren't resolved in 30 days?

Mr. BEALES. Well, I think most instances are resolved within 30 days. We do get complaints of cases where it hasn't happened, but we don't have any firm data on what the averages are like. We are working with credit reporting agencies to try to figure out what goes wrong in those cases where it takes longer and try to get those particular problems fixed as quickly as possible because that is clearly what is in the best interest of consumers.

Senator CANTWELL. In general, you have indicated 42 percent of the victims reporting to the clearinghouse and 20 percent report

unauthorized telecommunications or utility services. What else could be done to address some of these most targeted industries, the credit card issuers in utilities, to encourage cooperation with the victims?

Mr. BEALES. Well, that is one of the things we want to explore in the best practices workshop. I mean, I think the financial institutions have faced this problem longer and more clearly and probably with larger losses than utilities and telecommunications folks, and have a better sense of ways to prevent those losses, and at the same time prevent the injury to victims. What we would like to do is to identify some of those best practices and see if they can't be transferred to businesses in other sectors to reduce losses there as well.

Senator CANTWELL. Thank you. Thank you, Madam Chairman.

Chairperson FEINSTEIN. Thank you very much.

Thanks very much, Mr. Beales. We are delighted to have you and I think we will move on with the second panel now.

I would like to enter into the record a statement by Senator Grassley, Senator Hatch; also, a statement and paper by Normal Wilcox. The record will remain open for additional statements.

Mr. BEALES. Thank you for the opportunity to be here.

Chairperson FEINSTEIN. Thank you very much, Mr. Beales.

If the next panel will come forward, please?

I would like to defer to my colleague, Senator Cantwell, for her introduction of the Attorney General of the State of Washington.

Senator CANTWELL. Well, thank you, Madam Chair. We are very excited to have Attorney General Christine Gregoire joining us today. She has, as I mentioned in my opening comments, played an important leadership role in this important issue in my State and has lent her expertise to the Senate on numerous occasions, testifying just recently on the impact of the Enron collapse on State pension funds. So we very much appreciate that she is here with us today.

Obviously, some people may remember her from her work on the tobacco settlement and her leadership role on behalf of the AGs on that issue. But she has been a leader in this fight against identity theft in our State, which is one of the top ten States hardest hit by identity theft, and she helped draft and pass the legislation that we are going to be hearing about today that is the basis for the Reclaim Your Identity Act that is before us today.

So I want to introduce and thank our Attorney General for being here.

Chairperson FEINSTEIN. Thanks very much, Senator.

Madam Attorney General, we have just been joined by Senator Kyl, the ranking member of the subcommittee, also the main cosponsor of my bill on identity theft.

Senator Kyl, would you like to make a statement now and then I will introduce the other witnesses?

Senator SESSIONS. Madam Chairman, could I just express a word of greeting to my former colleague, Christine Gregoire?

Chairperson FEINSTEIN. Of course.

Senator SESSIONS. I appreciate her leadership in the Attorney Generals Association for many years. She is one of the more out-

standing spokesmen for issues important to the attorneys general in the country and has been a leader in the association.

We are glad to have you, Christine.

Ms. GREGOIRE. Thank you, Senator.

Chairperson FEINSTEIN. Thanks, Senator.

Senator Kyl.

STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator KYL. Madam Chairman, I will simply put my statement in the record, but note my appreciation both for this panel and the other panel. We have been working on this at least since 1998, and I think this latest GAO study that we requested demonstrates that the problem is as big as ever, if not getting worse. Therefore, everything we can do to try to deal with it will be progress.

So I appreciate the fact that you have scheduled this hearing and I appreciate the testimony of the witnesses, and everything else I have to say will be in writing.

[The prepared statement of Senator Kyl follows:]

OPENING STATEMENT OF SENATOR JON KYL

I would like to begin by thanking Senator Feinstein for chairing this important hearing on identity theft and how its victims can regain control of their good names, and their lives. We have been concerned with the issue of identity theft for many years. I sponsored the Identity Theft Assumption Act of 1998, which focused the public's attention on this form of crime. That law made it illegal to transfer or use another person's name or any identifier that is used to identify a specific individual without that person's consent.

Senator Feinstein and I have worked together to devise congressional legislation that will protect the public from the growing problem of identity theft. A recently released General Accounting Office report that Senators Grassley, Feinstein, and I requested indicates that incidents of identity theft have continued to rise and that it is the number one concern of consumers. Although it is difficult to get concrete numbers on the prevalence of identity theft because no one specific database exists to accurately quantify it, the overall statistics are troubling.

The Federal Trade Commission's Identity Theft Data Clearinghouse received approximately 94,000 complaints from victims from November 1999 through September 2001. The Social Security Administration's Office of the Inspector General has reported that, since its Fraud Hotline was established in 1998, until the fiscal year 2001, allegations of misuse of Social Security numbers have increased fivefold. The Inspector General indicates that 81 percent of all allegations of Social Security Number misuse relate directly to identity theft.

Those are staggering statistics; however, we must remember that each statistic represents an individual who is a real victim of identity theft. That individual faces not only monetary harm but emotional and other nonmonetary injury. Many victims may only suffer small monetary losses; however, many hours are expended attempting to reestablish their credit records and good names. In addition, a victims often have a lingering fear that information about them can still be used to create debt and otherwise besmirch their reputation. These crimes are also financially burdensome to private industry and law enforcement. The Management and Organizational Division of the United States Secret Service has estimated that a financial crime investigation costs, on the average, $15,000.

I am aware that these statistical increases are partially the result of the public being better informed about identity theft, and reporting it more, and also the government agencies being more aggressive in assisting the victims of this crime. Even with that recognition, I know we can and should do more legislatively to combat identity theft. It is important that access to personal information be restricted, that members of the public be educated on how best to protect themselves, that law enforcement at the local, state, and federal levels work together, and finally, that private industry take a proactive part in preventing the theft of citizens' identities.

Senator Feinstein has brought together a group of witnesses that I believe can help us better understand the problem of identity theft and, more importantly, can

assist this subcommittee and the Congress in crafting laws to lessen the incidence of identity theft.

I am interested in hearing how we can limit the unnecessary use of Social Security numbers and how we can make the system of reestablishing a victim's identity more efficient and less time-consuming. At the same time, I do recognize that, in today's society, private industry, the government, and law enforcement must rely on Social Security numbers to provide valuable services to the public. This is a delicate balance that requires all interested parties to work together.

I anticipate that today's law enforcement and State Attorney General witnesses can shed some light on the problems they face on a daily basis. Since this is a crime that is not limited to a geographic region, I would like to hear their opinions on what can be done to assist the victims and the law enforcement community.

Finally, Senator Feinstein and I have introduced the Identity Theft Prevention Act of 2001. The legislation will, among other things, seek to cut back on needless access to public information about citizens, will require additional notifications to consumers, and will require changes to the fraud-alert system. I look forward to your comments on this legislation.

In closing, again I would like to express my thanks for Senator Feinstein's dedication and assistance in helping to wage this difficult battle against the crime of identity theft. It is a complex issue and, as always, I look forward to working more with her on it.

Chairperson FEINSTEIN. Thank you very much.

I will quickly introduce the other witnesses. The second person testifying will be Sallie Twentyman. She is a high school teacher and also the victim of identity theft. The crime occurred in late 1999 and Ms. Twentyman is still feeling the repercussions from it.

Linda Foley is the founder and executive director of the Identity Theft Resource Center. That is a non-profit victim advocacy and consumer education program located in San Diego, California. She is terrific. This victims center was established in 1999 in response to the growing need for victim assistance and public empowerment caused by the rise of identity theft. She is a former victim herself and so she is really uniquely suited to understand some of the problems.

Finally, Inspector Lou Cannon is the president of the District of Columbia Chapter of the Fraternal Order of Police, the largest law enforcement organization in the country. Few could fit that position better, as Inspector Cannon was a member of the Metropolitan Police Department for 22 years. He has also served with the Library of Congress Police Department at the United States Mint.

Ladies and gentlemen, we welcome you, and we will begin with the Attorney General.

STATEMENT OF CHRISTINE O. GREGOIRE, ATTORNEY GENERAL, STATE OF WASHINGTON, OLYMPIA, WASHINGTON

Ms. GREGOIRE. Well, good morning, and thank you, Madam Chair and members of the committee. It is a delight for me to be here and testify on this very important issue with you today.

I really do appreciate your interest in helping to protect citizens from what has become one of the fastest growing and most expensive consumer frauds in America. Identity thieves don't just steal victims' money; they rob them of their time, they rob them of their credit, and they rob them of their reputation.

In January 2000, identity theft reports were arriving at the FTC at the rate of 300 per week. Just one year later, the rate had grown ten-fold to 3,000 per week. As the GAO report on identity theft issued this month indicates, the true incidence of this crime is very difficult to measure, but in the five minutes that I speak to you,

an estimated five more Americans will have their identities stolen. Those five people will spend nearly $6,000 in notary fees, copying charges, and legal fees to clear their names. That doesn't count their lost wages or their lost credit.

It takes time, too. Those five victims will spend somewhere in the neighborhood of 875 hours, or nearly 22 work weeks, dealing with the impact of the theft over the next 2 years. One or two of them might even become the subject of a criminal investigation, or even become the victim of an arrest because someone has fraudulently stolen their identity. Businesses will pay, too. Those five identity thefts that occur as I speak will cost business somewhere in the neighborhood of $33,000. Over the course of a year, it adds up to an estimated $3.5 billion.

Those are just the numbers, averages that help describe the problem on a national scale. But to really understand it, I think you need to look at what identity theft does to an innocent individual like Jenni D'Avis, from my State, who brought this to my attention.

Jenni thought there had been some type of simple error when she got two bills for maxed-out credit cards she didn't have. Then she got a phone call from the General Motors Acceptance Corporation asking why she was late on her payment on her Chevy Suburban. She wasn't making payments because she had never purchased the vehicle. Someone else had done so using her I.D.

Piecing it together, she discovered that a thief had obtained her Social Security number from a student roster at her community college. The thief used the Social Security number to get a State identification card, then launched a spending spree. By the time she realized what was going on, the thief had run up $72,000 worth of charges on 13 credit accounts, 9 cellular phone accounts, and 6 checking accounts.

Jenni didn't get stuck with those bills, but she learned that she would quickly get stuck with some very nasty marks on her credit. GMAC told her that they would list the stolen Chevy Suburban as a "repossession" on her credit report and that she would have to clear it up sometime later. In three weeks, Jenni's sterling credit was horribly tarnished. She was forced to sue her creditors and her credit reporting agencies to finally clear her name. It took her more than two years.

Unfortunately, her story is not unique. My State has the dubious distinction of being among the top ten in the Nation per capita as victims of this crime. That is why we passed our identity theft law last year.

First, we wanted to ensure that the criminal justice system recognized this for what it was, a crime against individuals of a very costly nature, not just in money. But even more importantly, we wanted to give the victims the tools to get their good name and reputation back timely and without having to spend a lot of their own money.

But our law simply isn't enough. Identity theft is a crime that does not respect State or regional boundaries. A Social Security number stolen in Washington can be used to obtain a credit card in Delaware that is being used to get a cash advance in Ohio. That is why we do need work on the Federal level.

In December, our National Association of Attorneys General passed a resolution calling for Federal legislation to address this growing crime. This resolution supports legislation to both prevent identity theft and to make it easier for victims of identity theft to recover their reputations.

So I am very pleased that you are tackling this most difficult problem in two ways. Senator Kyl and Senator Feinstein, your bill will help prevent identity theft by decreasing thieves' access to our personally identifiable information, and that is very important.

Let me tell you about another woman in my State, Berniece Phelps. Ms. Phelps discovered her identity had been stolen in August, shortly after our State law had come into effect. She made the discovery because credit card companies called to ask her if she had moved to Florida. By calling to verify the change in the address, which would be a requirement under your bill, the companies helped Ms. Phelps stop the damage to her credit. Your bill will address prevention in a very needed way.

We also need to recognize, however, that these thieves are very persistent, as Senator Sessions has indicated. We are not going to be able to stop all of them, and that is why I am also here to support very strongly Senator Cantwell's bill, the Reclaim Your Identity Act.

As I mentioned, Berniece Phelps' identity was stolen just two months after our State law went into effect, and the difference between her experience and that of Jenni D'Avis' experience is stark. Ms. Phelps used our new law to get help from businesses and credit agencies. She did not have to sue them. She was able to get her credit report corrected quickly and easily. These are key components of our new law. Senator Cantwell's proposed bill will make sure victims across the country have the same resources and that kind of experience and not the nightmare of Jenni D'Avis and what she went through.

It adds some significant features beyond those found in Washington State's law. Under existing law, as a result of our Supreme Court ruling, as you just mentioned, the two-year statute of limitations for filing suit can expire before an identity theft victim even becomes aware that a crime has been committed. But under this new bill, the statute of limitations clock does not start running until the consumer knows, or reasonably should have known, that their identity had been stolen. The bill provides another means to go after identity thieves by making a conviction under State law a crime that can be pursued by a Federal racketeering violation.

Since our law went into effect last July, people in my State have had help in restoring their good names and their good reputations. I see no reason why residents in other States should not have the same protection from identity theft that our State citizens now enjoy. The Reclaim Your Identity Act will help ensure that an identity victim in Phoenix, Raleigh or Frankfort will have the same protections as an identity victim in Seattle, and it will give victims, regardless of where they call home, a fighting chance at getting their credit repaired and their lives back on track.

Again, thank you, Madam Chair and members of the committee, for your interest in this issue and your willingness to take this most pressing problem up with the American people.

[The prepared statement of Ms. Gregoire follows:]

STATEMENT OF CHRISTINE O. GREGOIRE, ATTORNEY GENERAL OF WASHINGTON STATE

Good morning.

Thank you Senator Feinstein and members of the committee for the opportunity to testify here today.

I appreciate your interest in helping to protect citizens from what has become one of the fastest growing and most expensive consumer frauds in America.

Identity thieves don't just steal victims' money. They rob them of their time, credit and reputation.

In January 2000, identity theft reports were arriving at the FTC at a rate of 300 per week.

Just one year later, the rate had grown tenfold, to 3,000 reports a week.

As the GAO report on identity theft issued this month indicates, the true incidence of this crime is difficult to measure.

But in the five minutes I speak to you, an estimated five more Americans will have their identities stolen.

Those five people will spend nearly $6,000 in notary fees, copying charges and legal fees to clear their names.

That doesn't count any lost wages or lost credit.

It takes time, too. Those five victims will spend 875 hours—or nearly 22 work-weeks—dealing with the impacts of the theft over the next two years.

One or two of them might even become the subject of a criminal investigation or even arrest because of someone's fraudulent use of their identity.

Businesses will pay, too.

Those five identity thefts that occur as I speak will cost businesses $33,500. Over the course of a year, it adds up to an estimated $3.5 billion.

Those are just numbers, averages that help describe the problem on a national scale.

But to really understand it, I think you need to look at what identity theft does to innocent individuals like Jenni D'Avis from my state.

Jenni thought there had been some type of simple error when she got two bills for maxed out credit cards she didn't even have.

Then she got a call from the General Motors Acceptance Corporation asking why she was late on payments for her Chevy Suburban.

She wasn't making payments because she had never purchased the SUV. Someone else did, using Jenni's I.D.

Piecing it together, Jenni discovered that a thief had obtained her Social Security number from a student roster at the community college she attended.

The thief used the Social Security number to get a state I.D. card, then launched a fraudulent spending spree.

By the time Jenni realized what was going on, the thief had run up $72,000 worth of charges on 13 credit accounts, nine cellular phone accounts and six checking accounts.

Jenni didn't get stuck with those bills, but she learned that she would get stuck with some very nasty marks on her credit record.

GMAC told her they would list the stolen Chevy Suburban as a "repossession" on her credit report and that she would have to clear it up later.

In three weeks, Jenni's sterling credit was horribly tarnished. She was forced to sue her creditors and credit reporting agencies to finally clear her name. It took her more than two years.

Unfortunately, Jenni's story isn't unique.

My state has the dubious distinction of being in the top ten states for identity thefts per capita.

That's why Washington passed a new identity theft law last year.

We wanted to ensure the criminal recognized the gravity of the crime. But even more importantly, we wanted to give victims the tools to get their good names and reputations back quickly and without having to spend a lot of their own money.

But one law isn't enough.

Identity theft is a crime that does not respect state or regional boundaries.

A Social Security number stolen in Washington can be used to obtain a credit card in Delaware that is then used to get a cash advance in Ohio.

That's why citizens need help at the federal level.

In December, the National Association of Attorneys General passed a resolution calling for federal legislation to address this growing crime.

The resolution supports legislation to both prevent identity theft and to make it easier for victims of identity theft to recover their reputations.

So I am pleased to see you tackling this difficult problem in two ways.

Senator Feinstein, your bill to help prevent identity theft by decreasing thieves' access to our personal identifying information is very important.

Let me tell you about another woman in my state, Berniece Phelps. Mrs. Phelps discovered her identity had been stolen in August, shortly after our state law had taken effect.

She made the discovery because credit card companies called her to ask if she had moved to Florida.

By calling to verify the change in address, which would be a requirement under Senator Feinstein's bill, the companies helped Mrs. Phelps stop the damage to her credit.

Senator Feinstein's bill addresses prevention very well.

But we also need to recognize that these thieves are persistent and we won't be able to stop all of them.

And that's why I also support, very strongly, Senator Cantwell's "Reclaim Your Identity Act."

As I mentioned, Berniece Phelps' identity was stolen just two months after our state law went into effect.

And the difference between her experience and Jenni D'Avis' experience is stark.

Mrs. Phelps used the new law to get help she got from businesses and credit agencies.

She was able to get her credit report corrected quickly and easily. These are key components of our new state law.

Senator Cantwell's proposed bill will make sure victims across the country have the same resources so they can have that kind of experience and not the nightmare that Jenni D'Avis went through.

And it adds some significant features beyond those found in Washington's law.

Under existing law, as a result of the Supreme Court ruling in TRW v. Andrews, the two-year statute of limitations for filing suit can expire before an identity theft victim even becomes aware of the crime.

But under Senator Cantwell's bill, the statute of limitations clock doesn't start running until the consumer knows, or reasonably should know their identity has been stolen.

And the bill provides another means to go after identity thieves by making a conviction under state law a crime that can then be pursued as a federal racketeering violation.

Since our law went into effect last July people in my state have had help in restoring their good names.

I see no reason why residents in other states should not have the same protections from identity theft that our state's citizens now enjoy.

The "Reclaim Your Identity Act" will help ensure that an identity theft victim in Phoenix, Raleigh or Frankfort will have the same protections as a victim in Seattle.

And it will give victims—regardless of where they call home—a fighting chance at getting their credit repaired and their lives back on track.

Thank you.

Chairperson FEINSTEIN. Thank you very much, Attorney General. That was excellent testimony and very helpful.

Sallie Twentyman, we welcome you and would love to hear your story.

STATEMENT OF SALLIE TWENTYMAN, FALLS CHURCH, VIRGINIA

Ms. TWENTYMAN. Thank you. I do appreciate this opportunity to appear today to tell you about some of my experiences as a victim of identity theft.

On September 14, 1999, I received a credit card bill that changed my life, a bill that included charges of one convenience check for $9,500, three other cash advances totalling about $2,500, and a payment of $8,300. I was in shock, wanting to believe that there was an easy explanation for the bill, that the credit card company had sent me somebody else's bill by mistake or that someone had keyed in numbers incorrectly.

But when I called the bank to report the error, I found out that the charges were very real. Someone had stolen my renewal credit card from the mail before it reached me and had immediately called the credit card company with a change of address. During the conversation, this person also obtained information about other credit card accounts I held at that same bank and, using my Social Security number, convinced the customer service representative to open more accounts in my name.

The only error with the bill was that it had been mailed to me at my old address instead of to the thief at the new address. Today, I am thankful for that error, as I found out earlier that I had become yet another victim of identity theft, a crime I heard of at the time but had never thought of as happening to anybody I knew, and certainly myself.

I spent the next few months of my life immersed in restoring my good credit and trying to educate those around me about how to lower the risk of it happening to them. Over a period of six months, my credit report showed that I moved almost every month to four different new addresses, from Falls Church, Virginia, to Brooklyn, New York, to Seapointe, Georgia, to Chicago, Illinois, and Pleasanton, California. These reports also showed me attempting and succeeding at opening several new credit card and bank accounts, and this was all after I had placed a fraud alert on my name file.

During the six months, I experienced many frustrations. There was no one there to help, and the people who were there I didn't know about. Since the crimes all occurred in different States and jurisdictions from my residence, law enforcement agencies didn't help. Banks conducted investigations, but they usually didn't begin the investigations until four months to a year after the crimes occurred.

Banks kept making mistakes and no one seemed accountable for their mistakes. Once, a bank FedEx'ed a card to the fraudulent address after I had notified them of the fraud. On another occasion, the thief convinced the bank that I was a thief—this was the original bank where it started—even though I had lived at my address for 12 years and the thief had only been at her address for 2 weeks.

I felt that no matter how hard I tried, I was always a step behind. The only information I could receive about my crime I gleaned from credit reports. And my thief was smart. By the time that new information addresses were posted to the reports, the thief or thieves had already moved on to another location.

Banks refused to give me information about activity in my name. The bill that I actually received was the only specific information that I ever received about amounts, the kinds of purchases, et cetera, in my name. Banks refused to give me information, since the cases were under investigation, and I found this one of the most frustrating things.

I am grateful to hear your discussion today about the Feinstein-Kyl bill and the Cantwell bill. There are provisions of these bills that I feel would have helped me if they had been in place at the time and will certainly help future identity theft victims.

Granting the FTC authority to fine the merchants for ignoring fraud alerts might make merchants more careful about checking

credit bureau files before issuing instant credit. It would certainly make them more accountable for the mistakes they make.

Three of the provisions would let victims know of their identity theft early and let them correct information with merchants before negative information is sent to the credit bureaus. They are: the requirement that credit card companies notify consumers when additional cards are requested on an existing account within 30 days of a change of address request, a requirement for notification to be sent to both the new address and the former address, and the requirement that the FTC issue rules requiring credit bureaus to investigate discrepancies between a credit card applicant's address and the records in its files. My address kept changing every month after the fraud alert and I never heard about it until I got copies of the credit report.

The requirement that businesses give identity theft victims a copy of any documents, such as credit card applications related to an identity theft, will make it easier for the victim to protect themselves, or at least to feel like they are doing something that would help.

I will never forget the confusion and frustration I felt that day and have felt to some extent everyday since the day I received the bill, the day I learned I was the victim of a crime that feels in many ways like financial cancer. Today, as far as I know, I am in remission from the cancer, but I cannot be sure that I will ever be completely cured.

The thief is probably still out there, unapprehended, with enough of my personal information in hand to destroy my credit all over again at any time. And other potential thieves can easily access this information from Internet sites that sell personal information, including Social Security numbers. In my case, I never learned who the thief was. What was more disturbing to me was that I don't believe anyone ever really tried to find the thief.

I applaud your efforts and urge your continued efforts to protect victims of identity theft. I am also grateful to the Government agencies, such as the FTC and the U.S. Postal Inspection Service, and to the media for workingtogether to educate citizens about how to reduce their risk of becoming victims and how to restore their credit if it should happen to them.

Thank you.

[The prepared statement of Ms. Twentyman follows:]

STATEMENT OF SALLIE TWENTYMAN

I appreciate the opportunity to appear here today to tell you about some of my experiences as a victim of identity theft.

On September 14, 1999, I received a credit card bill that changed my life—a bill that included charges for one convenience check for $9600, three other cash advances totaling about $2500, and a payment of $8300. I was in shock, wanting to believe that there was an easy explanation for this bill—that the credit card company had sent me someone else's bill by mistake, or that someone had keyed in some numbers incorrectly.

But when I called the bank to report "the error", I found out that the charges were very real. Someone had stolen my renewal credit card from the mail before it reached me and had immediately called the credit card company with a change of address. During the conversation, this person also obtained information about other credit card accounts that I held at that same bank, and, using my social security number, convinced the customer service representative to open more accounts

in my name. The only error with this bill was that it had been mailed to me at the "old" address instead of to the thief at the "new" address.

Today, I'm thankful for this error, as I found out early that I had become yet another victim of identity theft, a crime I had heard of but never thought of as happening to anyone I knew. I spent the next few months of my life, immersed in restoring my good credit and tying to educate those around me about how to lower the risk of this happening to them.

Over a period of six months, my credit reports showed that I moved almost every month, to four different "new" addresses—from Falls Church, VA to Brooklyn, NY to Seapointe, GA to Chicago, IL and Pleasanton, CA. The reports also showed me attempting and succeeding at opening several new credit card and bank accounts. And this was all ***AFTER*** I had placed a fraud alert on my file.

During those six months, I experienced many frustrations.

- There was no one there to help. Since the crimes all occurred in different states and jurisdictions from my residence, law enforcement agencies didn't help. Banks conducted investigations, but they didn't usually begin their investigations until four months to a year after the crimes occurred.
- Banks kept making mistakes, and no one seemed accountable for their actions. Once, a bank FedEx'ed a card to the fraudulent address ***after*** I had notified them of the fraud. On another occasion, the thief convinced a bank that ***I*** was the thief, even though I had lived at my address for 12 years and the thief had only been at her address for two weeks.
- I felt that, no matter how hard I tried, I was always a step behind. The only information I could receive about my crime I gleaned from my credit reports. And my thief was smart. By the time that new information and addresses were posted to my reports, the thief (or thieves) had already moved on to another location.
- Banks refused to give me information about activity in my name. The bill that I actually received was the only specific information that I ever received about amounts, the kinds of purchases, etc. in my name. Banks refused to give me information since the cases were "under investigation".

I am grateful to hear of your discussions today about Senator Feinstein's bill (S. 1399) and Senator Cantwell's bill (S. 1742). There are provisions in these bills that I feel will help future identity theft victims:

- ***Granting the*** FTC authority to fine merchants for ignoring the fraud alert might make merchants be more careful about checking credit bureau files before issuing instant credit. It would certainly make them more accountable for the mistakes they make.
- Three of the provisions would let victims know of their identity theft early, and let them correct information with merchants before negative information is sent to the credit bureaus. There are (1) the requirement that credit card companies notify consumers when additional cards are requested on an existing account within 30 days of a change of address request, (2) the requirement for notification to be sent to both the new address and the former address, and (3) the requirement that the FTC issue rules requiring credit bureaus to investigate discrepancies between the credit card applicant's address and the records in its files.
- The requirement that businesses give identity theft victims copies of any documents (such as credit card applications) related to an identity theft would make it easier for a victim to protect himself.

I'll never forget the confusion and frustration I felt that day and have felt, to some extent, every day since the day I received that bill, the day I learned that I was a victim of a crime that feels, in many ways, like "financial cancer". Today, as far as I know, I'm "in remission" from this "cancer", but I cannot be sure that I'll ever be completely cured. The thief is probably still out there, unapprehended, with enough of my personal information in hand to destroy my credit all over again, at any time. And other potential thieves can easily access this information from Internet sites that sell personal information, including social security numbers.

In my case, I never learned who the thief was. What was more disturbing to me was that I don't believe anyone ever really ***tried*** to find the thief.

I applaud your efforts and urge your continued efforts to protect victims of identity theft. I am also grateful to the government agencies such as the FTC and the US Postal Inspection Service and to the media for working together to help educate citizens about how to reduce their risk of becoming victims and how to restore their credit if it should happen to them.

Chairperson FEINSTEIN. Thank you very much.

Inspector Cannon.

STATEMENT OF LOUIS P. CANNON, PRESIDENT, DISTRICT OF COLUMBIA LODGE, GRAND LODGE, FRATERNAL ORDER OF POLICE, WASHINGTON, DC

Mr. CANNON. Good morning, Madam Chairman, distinguished members of the Senate Subcommittee on Technology, Terrorism, and Government Information. My name is Lou Cannon. I am a 30-year veteran of law enforcement, currently with the Department of Treasury, U.S. Mint.

The FOP is the Nation's largest law enforcement labor organization, representing more than 300,000 rank-and-file law enforcement officers in every region of the country. I am here this morning at the request of Steve Young, National President of the FOP, to discuss our support of two pieces of legislation: S. 1399, the Feinstein-Kyl bill, the Identity Theft Protection Act, introduced by you, Madam Chairman, and Mr. Kyl, and S. 1742, the Restore Your Identity Act, introduced by Senator Maria Cantwell.

The technology of information age has allowed criminals to commit traditional crimes in new ways. Identity theft is one such example. A criminal who obtains key pieces of personal information—and at this time, Madam Chairman, I would like to thank you for providing me with the information that I needed to obtain a credit card.

Chairperson FEINSTEIN. I provided that?

Mr. CANNON. Yes, ma'am. I will give it to you after the hearing.

Chairperson FEINSTEIN. Oh, that is our Web site.

Senator CANTWELL. I think what he means, Madam Chairman, is that it is so simple——

Mr. CANNON. The technology is there and you can provide it if you know what you are doing.

Chairperson FEINSTEIN. Oh, I see what you are saying.

Mr. CANNON. You didn't give it to me, but I got it.

Chairperson FEINSTEIN. Thank you. I got worried for a minute.

Mr. CANNON. No, you didn't give it to me. I got it from you.

Chairperson FEINSTEIN. Oh, all right.

Mr. CANNON. Let me finish and you will see.

Chairperson FEINSTEIN. Uh-oh, trouble. [Laughter.]

Mr. CANNON. They can then commit fraud and other crimes by purchasing credit, merchandise, and services in the name of the victim. In 2001, an estimated 700,000 consumers became victims of identity theft. Reports of these crimes have doubled in many jurisdictions and there is no reason to believe that this trend will not continue.

The cost of these crimes is high. The U.S. Secret Service estimates that in 1997 consumers lost more than $740 million as a result of identity theft. Victims find their entire credit histories ruined, affecting their ability to obtain future credit, good interest rates, loans to buy homes or businesses or pay college tuition, or obtain security clearances.

According to a report issued by the California Public Interest Research Group and the Privacy Rights Clearinghouse, it takes a vic-

tim an average of 175 hours and more than $800 to destroy the damage done to their credit rating by these criminals.

These crimes are often ones of opportunity. For the criminal, the risk is relatively low. It was for me; I just sat at my computer. The potential profit is relatively high. Furthermore, the nature of the crimes makes it difficult for local and State law enforcement to investigate these crimes effectively or even take a report.

For example, a victim in South Carolina has his identity stolen while on vacation in Florida and the information is used to buy merchandise in New Jersey. Where was the crime committed? South Carolina, where the victim resides, in Florida where the information was stolen, or the point of purchase in New Jersey? What if the fraudulent purchase was made online?

The investigation of these crimes presents a very real challenge for law enforcement. At present, we lack the tools to effectively investigate these crimes. I do not have any official statistics at this time, but anecdotally I estimate that the clearance rate for such cases—that is, those cases in which an arrest is made—is less than 10 percent.

The legislation that this subcommittee is considering today, Madam Chairman, aims to make it more difficult for criminals to obtain the sensitive personal data used to perpetrate identity crimes, restoring and preventing the damage done by such crimes, and to enhance the ability of law enforcement to investigate and prosecute these types of offenses.

For example, 1399, the Feinstein-Kyl bill, would require a credit card company to notify the card-holder whenever they receive a request for a new card or a change of address. An alert consumer will be able to tell immediately that someone is attempting to steal their identity. Credit card companies would also be required to disclose discrepancies to consumer credit reporting agencies, better enabling the victims of identity theft to retain their good credit rating.

The legislation would also require new credit card machines that print receipts to truncate all but the last five digits of the card, frustrating attempts to steal this information. Remember, identity theft is a crime of opportunity. The more difficult it is for criminals to obtain this information, the fewer instances of these crimes will occur.

This bill also codifies the current industry practice of issuing fraud alerts and provides for rulemaking by the FTC to require credit card reporting agencies to investigate discrepancies between credit applications and credit reports, as well as to develop procedures for referral of consumer complaints about identity theft and fraud alerts between consumer reporting agencies. In addition to helping victims of identity theft, these changes will better enable law enforcement to gather information about these crimes and improve our ability to investigate open cases.

The second piece of legislation being considered by the subcommittee is S. 1742, Senator Cantwell's bill. The FOP believes this bill will enhance the ability of law enforcement to gather evidence while investigating these crimes.

For instance, many creditors are unwilling to divulge information about open accounts because of liability concerns and a good-faith

desire to protect the privacy rights of the account-holder. Many will not release any information without a court order or unless the victim agrees to claim responsibility for the account, meaning the outstanding balances.

The sad fact of the matter is that law enforcement is unable in the vast majority of cases to expend the resources necessary to obtain a court order in this type of case without additional evidence of criminal activity, making it a catch-22 of sorts.

In addition, the lack of timely information about the fraudulent transaction delays the progress of the investigation and the chances of closing the case. It also means that the victim's name may be used again and again to perpetrate fraud. Criminals who engage in identity theft count on the inability of law enforcement to gather in a timely fashion the evidence needed to find and convict them. It is one of the things that makes this crime both low-risk and profitable.

Your bill would change this by mandating that a victim of identity theft may request and receive relevant documentation about questionable transactions from the business or service possessing such information within ten days. The legislation correctly insulates these businesses from liability with respect to these disclosures, which could help both victims and law enforcement get the information in a timely manner.

Now, how might his help in investigations? Let us say, for example, that a criminal has obtained a credit card in someone else's name and is using it to purchase merchandise. If law enforcement receives the information from the credit card company about the transactions within a few days, it might be possible to contact the business and obtain a description of the suspect, or even catch the suspect on a videotape. This is very strong evidence that can help bring these criminals to justice. Timely access to the information will greatly increase the risk factor for those criminals who engage in this type of crime.

S. 1742 would also amend the Internet False Identification Prevention Act, and include State and local law enforcement in the FTC study examining enforcement of identity theft laws, improving communication and coordination in multiple jurisdictions. This is very important because even though identity theft is a Federal offense, State and local authorities are most likely to take the initial report and investigate the crime, as Senator Sessions has brought out. The gathering and dissemination of information about these crimes is critical to developing successful strategies to deal with the growth of identity theft crimes.

The bill also allows for aggressive prosecution of criminals engaged in fraud or identity theft crimes by making the offense under State law a RICO case. The aspects of this bill will greatly increase the penalties for those who engage in identity theft and will reduce the profits available to those persons trafficking in stolen identities in order to aid others in perpetrating fraudulent transactions.

The reason that identity theft is on the rise is that it is easy, profitable crime with a low risk of being caught. The FOP believes that these two bills together will reduce the opportunities of criminals or potential criminals from obtaining the personal information that makes identity theft possible.

Additionally, the bills aim to increase the risk of discovery and arrest by making it easier to obtain evidence against the perpetrators and enhancing the penalties for committing these types of crimes. With the tools provided in both of these pieces of legislation, you are providing victims and law enforcement with the tools they need to protect themselves and bring this new kind of criminal to justice.

I thank you for asking me here and giving me the opportunity to testify. I would like to close with borrowing just one little slogan: it is everywhere you want to be. Make sure it is you who is there.

Chairperson FEINSTEIN. Thanks very much, Inspector Cannon, and tear up that piece of paper.

Mr. CANNON. I will be giving it to your staff afterwards.

[The prepared statement of Mr. Cannon follows:]

STATEMENT OF LOUIS P. CANNON, PRESIDENT, DISTRICT OF COLUMBIA LODGE, GRAND LODGE, FRATERNAL ORDER OF POLICE

Good Morning, Madam Chairman, Ranking Member Kyl, and distinguished Members of the Subcommittee on Technology, Terrorism, and Government Information. Thank you for giving me the opportunity to appear before you today. My name is Lou Cannon, and I am the President of the District of Columbia Lodge, and Chairman of the Federal Officers Committee.

I am here this morning at the request of Steve Young, National President of the Grand Lodge, Fraternal Order of Police, to speak in support of S. 1399, the "Identity Theft Prevention Act of 2001" introduced by Chairman Feinstein and Senator Kyl, and S. 1742, the "Restore Your Identity Act of 2001" introduced by Senator Cantwell. The F.O.P. is the largest law enforcement labor organization in the United States, representing more than 300,000 members.

Identity theft occurs when a criminal obtains personal identifying information, such as a social security number, date of birth, credit card account number, or bank account information, and then fraudulently uses this information for criminal purposes. Simply possessing personal information is not considered a criminal act, but the use of it is. Tracking and investigating identity theft crimes have proven dffficult for law enforcement. In today's world, vast amounts of personal information, once difficult to obtain, is now easily accessible to anyone with access to the Internet. In addition, personal information is being sold on the black market. For a price, criminals can access a ready-made database of information without risk or effort of retrieval.

The sharp rise in identity theft crimes is of grave concern to the law enforcement community. The Federal Trade Commission (FTC) announced this January that identity theft was the top consumer fraud complaint of 2001, garnering forty-two percent (42%) of the complaints entered into the Consumer Sentinel database, with Internet auctions a distant second at ten percent (10%). As you know, the Consumer Sentinel database, which incorporates information submitted by law enforcement agencies, is a clearinghouse of information collected by the FTC. It is estimated that there were more than 700,000 victims of identity theft in 2001, with a reported 2,000 calls a week to the FTC identity theft hotline. A 1999 study commissioned by an identity theft prevention service found that one out of five people or family members have been victimized by identity theft. The cost to the victims, financial institutions, and law enforcement is tremendous. In 1997, the Secret Service estimated that victims lost an aggregate $745 million as a result of identity theft, and this number is expected to rise.

Besides the financial losses associated with identity theft, victims may also encounter additional hardships that are not quantifiable. For example, victims might have difficulty securing educational loans or qualifying for home mortgages. When a criminal has compromised a victim's credit rating, their ability to rent an apartment, open a bank account, or apply for store credit can be irreparably damaged. Circumstances might even lead to permanent consequences, such as a criminal record for the victim. Victims of identity theft may even be denied employment for their lack of credit worthiness. For example, as reported in a 1998 Washington Post article, a victim had his wallet stolen, followed by his identity. After committing several unrelated offenses, the identity thief was arrested. Upon his apprehension, the criminal falsely identified himself as the victim and produced corroborating identi-

fication. As a result, the victim was burdened with a criminal record and was subsequently rejected by several potential employers for this reason.

The crime of identity theft is repetitive in nature, for as long as the criminal is in possession of the victim's personal information, they can be re-victimized. Even if fraud insurance covers any financial loss, the victim will continue to suffer a flawed credit history, and will be forced to prove their innocence repeatedly to creditors, credit bureaus, and debt collectors for an indefinite period of time. According to the Identity Theft Resource Center, victims spend an average of 175 hours and $808 in out-of-pocket expenses to restore their credit and clear their names.

There are numerous means by which personal identifying information can be obtained, but there are several "tried and true" methods employed by identity thieves. These criminals often rummage through the trash of a private residence or business, steal wallets containing identification, or hijack bank and credit card statements or applications from the mail. They may complete a change of address form to direct mail to another address, use information provided on the Internet, or buy personal identifiers through the black market. Once the identity thief locates the personal identification, they have unlimited power to wreak havoc on the unsuspecting victim. The criminals may operate on a very basic level, or possess a certain degree of sophistication when using the fraudulently obtained data. Identity theft plots may be as simple as establishing new lines of credit or utility service and failing to pay, writing bad checks or counterfeit checks on a bank account in the victim's name, using the victim's identification as an alias upon arrest by law enforcement; or as complex as purchasing a home or car in the victim's name, or filing for bankruptcy to avoid unpaid debts accrued by the thief.

There are measures an individual can take to safeguard their personal information, like shredding bank statements, ripping up credit card receipts with the account number printed on them, and destroying expired credit cards in order to prevent criminals from collecting information by rummaging through the trash. Yet, despite a conscientious effort to protect personal information, potential victims have no control over how their privacy is safeguarded by those who do have access to their personal information.

For these reasons, the F.O.P. strongly supports S. 1399, the "Identity Theft Prevention Act of 2001". First, the bill mandates notification to consumers when a credit card company receives a change of address request for an existing account followed within thirty (30) days by a request for a duplicate credit card. The intent of this notification is to prevent a criminal from stealing the credit card number and related personal identifying information. By arming victims with this knowledge, they will be better able to defend against any unauthorized activity and prevent any further damage from occurring. In addition to this preventative measure, S. 1399 requires consumer reporting agencies to disclose any anomalies in the victim's file as they pertain to the address listed on the credit report to the company making the request. Creditors are thereby warned of possible fraudulent credit applications, frustrating criminal attempts to use this information. The information needed to steal an identity is easy to acquire—pilfering through garbage to obtain credit card account information, diverting mail through a change of address, or "skimming" credit cards to record the personal data contained on the magnetic strip. Identity thieves know that their risk of apprehension is low, and even if they are convicted, the penalty for such illegal activity is minimal. The proposed legislation appropriately addresses the means by which to hold businesses and creditors accountable for the mismanagement of private information.

Second, the legislation you have introduced also permits potential victims to demand that consumer reporting agencies place a fraud alert in their file, the purpose of which is to prevent the issuance of credit without expressed permission. By definition, a fraud alert means "a clear and conspicuous statement in the file of a consumer that notifies all prospective users of a consumer report made with respect to that consumer that the consumer does not authorize the issuance or extension of credit in the name of the consumer" unless by some prearranged method mutually agreed upon between the consumer and consumer reporting agency. Enforcement of this provision will make the crime of identity theft more difficult to accomplish, and therefore less attractive to the criminal element.

Third, this legislation promotes cooperation among the three major credit bureaus through an FTC rulemaking to be conducted within 270 days after the enactment of S. 1399. Victims of identity theft will benefit from the sharing of information between these agencies. For example, as required by the rulemaking, the procedure for reporting consumer complaints about identity theft and fraud alerts will be streamlined so that victims will not have to report the same information to each credit reporting agency, saving the victim valuable time and effort. The rulemaking

also requires investigation of discrepancies between a victim's credit application and credit report, should any such irregularities exist.

Finally, the bill requires all new credit card machines that print receipts electronically to leave off the expiration date of the credit card and all but the last five numbers of the account. Receipts thrown away by potential victims often end up in the hands of an imposter who uses the personal information on the receipt to make unauthorized purchases and run up debt that the victim is unaware of. Truncation of the credit card account number will effectively halt the practice of stealing information from receipts, even if the receipt is disposed of improperly. These preventative measures, combined with aggressive enforcement of identity theft legislation, will enhance the campaign to slow, and ultimately reverse, the growth of identity theft crimes.

The crime of identity theft presents a very real challenge to law enforcement to investigate and prosecute the offenders, partly because evidence of the crime is unavailable in a timely fashion. That is why the F.O.P. is pleased to support S. 1742, introduced by Senator Cantwell, which seeks to improve the cooperation among the credit reporting agencies, businesses, victims, and law enforcement. This is a critical first step to the successful investigation and prosecution of identity theft crimes. First, this bill requires a business possessing records related to an identity theft to furnish the relevant documentation within 10 days of the request, provided that the identity of the victim can be verified by the business. Many creditors have been unwilling to divulge information about open accounts or recent transactions because of liability concerns and a good faith desire to protect the privacy rights of the consumer. S. 1742 addresses this concern by exempting these businesses from liability with respect to any disclosure made to further the investigation of identity theft or assist the victim. The disclosure of evidence to the victim aids law enforcement in pursuit of the thief. With an estimated 700,000 consumers falling prey to identity theft in 2001, and law enforcement resources and manpower stretched to their limits, the cooperation of the business community is essential to stopping these types of crimes.

Second, through an amendment to the Internet False Identification Prevention Act, local and State law enforcement will be included in the Federal Trade Commission Study examining the enforcement of identity theft laws. This is important because these agencies, not Federal authorities, are most likely to investigate these types of crimes, despite the fact that identity theft is a Federal offense. Moreover, because the stolen identities are frequently used to commit offenses in multiple jurisdictions, State and local law enforcement from around the United States may be called upon to investigate the same crime. Therefore, it is imperative that information is quickly gathered and shared, keeping the lines of communication open to effect a swift and successful arrest and prosecution.

Third, the bill also allows for aggressive prosecution of criminals engaged in fraud or identity theft crimes by making the offense under State law a Federal Racketeer Influencing and Corrupt Organization (RICO) predicate. Businesses will be better equipped to defend themselves against such criminal activity, resulting in increased penalties for those who engage in identity theft. Civil actions brought by the State Attorneys General on behalf of victims in that State are also permissible under Senator Cantwell's legislation. Whereas prosecutors may be unable to prove criminal identity theft, the victims could still see justice done through civil litigation.

Fourth, alternatives to criminal punishment, such as the filing of civil suits in Federal court as set forth in S. 1742, increase the opportunity to enforce identity theft laws and hold the imposters accountable for their deception. This is a win-win situation for both victims and law enforcement, since tough enforcement of the law increases the risk of detection and thus deters crime.

Fifth, Senator Cantwell's legislation also amends the Fair Credit Reporting Act, giving victims a greater chance of recovering their good name, by providing that the two-year statute of limitations on an identity theft-related claim begins after the victim discovers the theft, not at the time the crime was actually perpetrated. Similarly, the bill requires that harmful information resulting from identity theft must be blocked from the victim's credit report, assuming the victim did not participate in the crime itself or profit directly or indirectly from it.

The reason that identity theft is on the rise is that it is an easy, profitable crime, with a low risk of being caught. Anecdotal evidence collected by Ventura County, California indicates that less than ten percent (10%) of identity theft crimes result in an arrest and conviction. The F.O.P. believes that these two bills together will reduce the opportunities of criminals or potential criminals from obtaining the personal information that makes identity theft possible. Additionally, the bills aim to increase the risk of discovery and arrest by making it easier to obtain evidence against the perpetrators and enhance the penalty for committing these types of

crimes. Collectively, both pieces of legislation will frustrate purveyors of identity theft and ultimately curb the rapid progression of this costly offense.

I want to thank the Subcommittee for the opportunity to appear before you here today. I would be pleased to answer any questions you may have at this time.

Chairperson FEINSTEIN. Linda Foley.

STATEMENT OF LINDA FOLEY, EXECUTIVE DIRECTOR, IDENTITY THEFT RESOURCE CENTER, SAN DIEGO, CALIFORNIA

Ms. FOLEY. Thank you very much, Senator Feinstein and members of the subcommittee. I thank you for having me here today. It is an honor especially because I have had a chance to work with both Senator Cantwell and Senator Feinstein in helping to put some of these bills together.

By the way, our program has expanded. Besides victim assistance, we are also serving as a resource and advisory center for everyone involved in this crime, from legislators, governmental agencies, law enforcement, businesses, consumers, and victims.

In the interest of time, I did submit a detailed written statement and I am just going to highlight a few points this morning.

I believe both of these bills are desperately needed and long overdue. The three points I would like to highlight today are the mandatory observation of fraud alerts, the providing of transaction and application information to victims and law enforcement, and why we believe that these bills are smart business, and it is a subject I don't think has yet been addressed this morning.

The Identity Theft Resource Center communicates with between 50 and 70 victims and consumers per week by e-mail or by telephone. We get about 10,000 visits per month to our Web site. These are people who are concerned that their information may be in the hands of another or being used by another or could be. They want to know how to prevent this person from abusing that information, and are dismayed when they find out that fraud alerts are advisory in nature only right now.

We have worked with victims who have also had their identities stolen, as in Sallie's case, after fraud alerts have been placed. I do understand why that is happening. I was part of a panel a few weeks ago that talked about that and I will be happy to address it a little later if you would like.

The Feinstein-Kyl bill helps to empower consumers who want to regulate those who have the ability to open accounts in their name. It stops criminals, who we know are repeat offenders and are very good at their job, from taking advantage of poor business practices, and ensures that all credit issuers will be duly warned of possible dangerous situations which could cause them severe economic loss.

One thing I would like to add that we have not yet addressed is when someone places a fraud alert on their credit report, right now it tends to be 90 days only. What happens is consumers think they have placed a fraud alert and it disappears. They don't understand that it also needs to be applied for in writing so that it has a longer period of time that it will last. They say, well, I placed a fraud alert, and two months later or three months later it is gone. So that is one of the things we keep talking about.

Chairperson FEINSTEIN. Do you know why it is just 90 days, what the rationale was?

Ms. FOLEY. Until they provide information in writing that they would like this as a permanent alert, which means anywhere from 3 to 7 years, they are putting it down as a 90-day alert only, in the belief that maybe this is not a true case of identity theft.

I am the victim of identity theft. My imposter was my employer. She is still out there, she is on probation. As far as I am concerned, I will have a fraud alert on my report the rest of my life because she still has access to that information. That means I have to take the time to re-put that on there every 3 years to make sure it continues on.

The second area I would like to highlight is in Senator Cantwell's bill, which I was very honored to be asked to participate in, and that is to allow law enforcement and victims access to the application and transaction information. I will say from personal experience that is how I found out who my imposter was.

Solving a case of identity theft is much like solving a jigsaw puzzle. If you only see one small piece of the crime, which is typically what corporate fraud investigators see, they don't see the whole picture. When victims and law enforcement can start putting together pieces from 10, 20, 30 accounts that have been opened in their name, then we start to see the entire picture.

This information can help a victim to identify an imposter. It can provide evidence that helps to prove a victim's innocence. It indicates trends, shipping information, possible witnesses to a crime. It can establish if that identity is being used by one or multiple impostors. It might even help to establish how that information was originally obtained. It is a good tool in crime prevention, and also in apprehension and arrest.

It would seem logical to me that if an account is being held in my name that I should have access to that information. What I hear from businesses is they say you can't because once you have said it is not your account, you become a third party and there is a legal issue and a privacy issue that they are concerned about. What your bill actually does is sort of takes them off the hook. We have that law in California, as well, and businesses are delighted to see it because it has sort of given them that opportunity to say this is something we wanted to do; we just weren't sure we could.

The burden of proving one's innocence rests solely on the shoulders of the victim. Yet, the victim doesn't have access to that information. It is interesting that in a court trial the defendant has the ability to access information that is going to be used against him. That is not true in identity theft. The cards are held with the credit issuers and they don't want to share anything with you. How do I prove that I am not that person when I don't see what you have against me?

Finally, while at first glance both of these bills seem to be consumer-oriented, I would like to also point out that I believe they are smart business. I will take some numbers that I know I have gotten from different sources.

We know there are between 500,000 and 1.1 million victims annually. That is information I get from law enforcement, by the way. A Florida grand jury was empaneled to study the problem of identity theft. They just released their first interim report and they

came up with a number similar to what we have heard and what you stated, $17,000 per average crime.

If you take a moderate number of 700,000 victims, times $17,000, you are looking at $11.9 billion of economic loss to the business community. By the way, the same report came out that the average bank heist is $3,500. There is a considerable difference here in risk, as well as in benefit.

That does not, by the way, include secondary losses, which would be legal time, investigative time, and the fact that consumers can go out and buy this merchandise that has been gained by impostors from another source, which is a second loss to those businesses because they are losing business.

We know that companies that practice good business practices, that observe fraud alerts, that confirm address changes, and that practice truncation are not as inviting to impostors and they turn to more happy grounds to steal from. In the end, I believe that the business community will realize an economic gain, will be less vulnerable to identity theft, and will demonstrate that they are looking out for the safety of consumers.

I will be happy to talk about the truncation issue and why fraud alerts are ignored. By the way, the Los Angeles Times just came out with an article that said that the arrest rate was about 5 percent.

I thank you very much, and I thank Senator Feinstein, Senator Kyl and Senator Cantwell for introducing these bills.

[The prepared statement of Ms. Foley follows:]

TESTIMONY PROVIDED BY: LINDA FOLEY, EXECUTIVE DIRECTOR, IDENTITY THEFT RESOURCE CENTER

Senator Feinstein and the members of the committee: Thank you for the opportunity to provide both written and oral testimony for your committee today and for your interest in the topic of identity theft. I feel strongly that these two valuable pieces of legislation will help to combat identity theft, empower consumers and assist law enforcement and business to reduce loss due to this crime.

The Identity Theft Resource Center's (ITRC's) mission is to research, analyze and distribute information about the growing crime of identity theft. It serves as a resource and advisory center for consumers, victims, law enforcement, legislators, businesses, media and governmental agencies.

In late 1999, I founded this San Diego-based nonprofit program after becoming a victim of identity theft myself. In my case, the perpetrator was my employer and my story is just one illustration of why we need the legislation you are considering today. ITRC's work with thousands of victims, law enforcement officers, governmental agencies and business has taught us much. I hope to share some of what I have learned with you today.

My written testimony will be divided into three parts:

- The crime: What is identity theft, its prevalence, why it is so popular among criminals
- Senate Bill 1742: Why ITRC supports this bill and believes it will assist victims, law enforcement and businesses
- Senate Bill 1399: Why ITRC supports this proactive identity theft protection act and believes it will prevent additional crime.

The Crime of Identity Theft:

The Federal Trade Commission has declared that identity theft is the fastest growing crime in our nation today, gathering speed and popularity among the criminal element of our society. Experts estimate that between 500,000 and 1.1 million people became victims in 2001. Why? Because it is a high profit, low risk and low penalty crime.

There are three main forms of identity theft:

• In financial identity theft the imposter uses personal identifying information, primarily the Social Security number, to establish new credit lines in the name of the victim. This person may apply for telephone service, credit cards or loans, buy merchandise, or lease cars and apartments. Subcategories of this crime include credit and checking account fraud.

• Criminal identity theft occurs when a criminal gives another person's personal identifying information in place of his or her own to law enforcement. For example, Susan is stopped by the police for running a red light. She says she does not have her license with her and gives her sister's information in place of her own. This information is placed on the citation. When Susan fails to appear in court, a warrant is issued for her sister (the name on the ticket).

• Identity cloning is the third category. This imposter uses the victim's information to establish a new life. He or she actually live and work as you. This crime may also involve financial and criminal identity theft as well. Types of people who may try this fraud include undocumented aliens, wanted felons, people who do not want to be tracked (i.e., getting out of paying child support or escaping from an abusive situation), and those who wish to leave behind a poor work and financial history and "start over."

As an aside, in view of the discussion about national ID cards or national driver's licenses, we do not see these cards as a way to address identity theft. More typically, those who would commit identity theft will either use fraudulent ID cards or carry none at all. In my opinion, a national ID program will create a larger black market for the acquisition of documentation and cards than we currently have today.

Identity theft is a dual crime and no one is immune, from birth to beyond death. There are at least two sets of victims in each case: the person whose information was used (consumer victim, to be referred to as victim from this point forward) and the merchant who has lost services or merchandise (commercial victim). Unfortunately, many commercial victims do not report the crime to law enforcement, finding it more fiscally advantageous to write off the loss.

Postage, telephone, travel, photocopying, time lost from work, costs involved in getting police reports and fingerprints, and resource materials. Some victims never truly regain their financial health and find credit issuers and even employers reluctant to deal with someone with "baggage."

The emotional impact of identity theft can be extremely traumatic and prolonged due to the extensive amount of time it can take to clear one's name. Some victims can be dealing with the crime for 3 to 7 years after the moment of discovery. Last week I was contacted by someone who also had been a victim of my imposter (my employer was a magazine publisher). This woman had been an advertiser in the magazine and our imposter used her credit card for other purchases. We believe that she may have applied for secondary card use. We started to put together a timeline. It appears that my employer started to use my information just weeks after this woman closed down the violated credit account. This woman and her uncle are still trying to clear records now 4 years old. It took several days for me to recover from talking with her. Our conversation brought back all the original feelings of violation and betrayal.

The addendum at the end is a brief outline of potential victim emotional reactions.

Identity Theft Is a High Profit Crime:

The report stated: "The average loss to the financial industry is approximately $17,000 per compromised identity. For criminals, identity theft is an attractive crime. An identity thief can net $17,000 per victim, and they can easily exploit numerous victims at one time, with relatively little risk of harm. By comparison, the average bank robbery nets $3,500 and the criminal faces greater risk of personal harm and exposure to a more serious prison sanction if convicted." (reprinted at "http://www.idtheftcenter.org" MACROBUTTON htmlResAnchor www.idtheftcenter.org under Speeches)

Their number is for financial institutions only. VISA and Mastercard also report the number to be lower. Part of the problem may be that not all commercial victims report the crime, lowering the number. In fact, many in law enforcement have expressed frustration that businesses prefer just to write the loss off rather than to get involved in an investigation. I also believe they have a vested interest in underreporting the loss so as to retain consumer confidence in their industry and to not encourage a greater number of fraudsters.

I have based my numbers on those given by law enforcement, the Florida and PRC reports and victims—sources I believe are unbiased and more complete.

Using the number of $17,000 per victim and the estimate of 700,000 victims, the economic loss could total $11.9 billion to merchants, credit issuers and the financial industry in 1 year alone.

I would like to further add that that $11.9 billion loss is just the beginning. You also have to add the cost of law enforcement and criminal justice time, costs to victims (including expensive attorney time) and secondary economic losses to merchants when merchandise "bought" by imposters is resold, resulting in a lessening of customer trade. Finally, there is the cost of investigating and prosecuting secondary illegal activities (drug trafficking, etc.) funded with the money made by imposters or information brokers who sell the documents used by some imposters and those wishing to identity clone.

Identity Theft Is a Low Risk and Low Penalty Crime:

Identity theft is a relatively easy crime to commit, often involving little risk to the imposter. It is almost as if they wear a "cloak of invisibility" and are given permission, even encouragement, to try.

First, the Internet and telecommunications have made it easy to not only apply for credit but also to make purchases from a variety of private and public locations. Even those who appear in person do so with the relative assurance that by the time the crime is discovered, they will not be remembered and any video surveillance will be long gone. FTC statistics prove that while some crimes are discovered within weeks of the first attempt, the average time between the beginning of criminal activity and discovery is about 15 months. Identity criminals are quite clever at finding ways to receive deliveries at locations other than at home. Many use drop spots or private postal boxes, switching from store to store frequently.

Second, we have a problem in that identity thieves take advantage of a system that is basically flawed, often due to poor business practices by credit issuers and merchants. Because the credit reporting agencies are subscriber services, credit issuers and merchants buy various levels of service. I have been told that not all see fraud alerts or even statements that the consumer is a fraud victim. Others simply choose to ignore the alert, balancing the potential risk vs the financial gain of a sale and unwillingness to irritate a new customer.

Third, law enforcement often finds this a frustrating crime to investigate. One financial crimes task force representative told me that an easy case of identity theft may take about 100 hours of investigative time, a difficult case can take in excess of 500 hours.

Why? There are many obstructions to investigating these crimes for both victims and law enforcement. After reporting the crime to credit issuers, victims frequently hear the comment: If you are not the person who opened the account, we can't provide information to you. Yet, these same victims are held financially responsible for the bill until they prove their innocence.

These two pieces of legislation in front of you today will help victims and law enforcement to more readily access information for investigation, give consumers more control of when and how credit is issued, make it more difficult to commit identity theft and help us to better understand the nature of this crime.

While they both appear to be consumer-driven, I will also address the benefits to taxpayers, businesses and the financial industries, which I believe will be substantial.

Testimony in Support of S 1742 (Cantwell):

There are three sections of this bill I would like to address.

Section 5: Information Available to Victims

Section 5 of S 1742 provides investigating law enforcement and verified identity theft victims with copies of application and transaction information on accounts opened in their name and identifying information.

It would seem logical that when an account is opened in your name that both investigating law enforcement and the victim should be able to access the information that is associated with that account. However, many companies refuse to provide copies of application and other documentation, claiming that it would be a violation of the imposter's, or true card holder's, privacy. They claim that once a victim says it is not their account, they lose all rights to information about it and have claimed legal problems in releasing information to law enforcement and victims. Yet, unless that person proves his or her innocence, that victim is still held financially responsible. How does one prove innocence when you don't know what is being held against you? In a court trial, the defendant has the right to view all evidence that will be used, but not in a case of identity theft.

When I became a victim of identity theft (Sept. 1997), I was fortunate in that the first credit card company I called shared the application information with me. I was

able to immediately identify my imposter. It was my employer and she used her business address, which I recognized, as the mailing address for the account. The second credit card company provided me with a copy of the application which I turned over to the police. Armed with evidence, the detective could then get a search warrant that led to her conviction.

Unfortunately, even the companies that helped me have now adopted policies that make it next to impossible for victims to gain access to information on accounts opened in their names. I was told that there was a legal issue involved. Credit card fraud investigators told me that once I said it was not my account, they feared that they would be in violation of the Fair Credit Reporting Act by disclosing information to a "third party," someone who is not the account holder. They wanted to provide the information but their legal departments were unsure of what to do. The reality is that once this account has been established as fraudulent and that a crime has occurred, all rights to privacy for the person who opened the account should be suspended. Access to the information regarding the account should be freely given to the victim and law enforcement investigating the crime. Based on the reaction in California and Washington, both states with a law similar to this one, I believe you will see a positive reaction from business because this law will clarify their legal status in giving out information.

Application and transaction information on fraudulent accounts provides the following information that the victim and law enforcement could use to establish the true holder of the account and/or prove innocence. This documentation:

- Can help the victim to identify the imposter, especially if the suspect is someone personally known to the victim, as in my case. In some cases, this information revealed a family secret that led to counseling and expert help.
- Can provide proof that the signature on the form is not that of the victim.
- Shows trends, valuable to police and to victims.
- Shows names and addresses where merchandise is shipped.
- Indicates phone records or transactions that could point to potential witnesses to the crime.
- Can establish location of transactions—was the crime local only or is the information being used by a number of imposters at the same time?
- Can establish method of theft?
- Might point to information that establishes how original information was obtained. For instance, a middle initial that was used only on a cell phone application, a legal name only used for payroll purposes, etc.
- Might provide evidence of multiple fraudulent accounts that could help to convince a bank or credit card company that this is a genuine act of identity theft and not just a customer finding a way to not pay a bill.

Solving a case of identity theft is much like putting together a puzzle. Each credit issuer fraud detective only sees one or two pieces of the puzzle. It isn't until the victim, or law enforcement, see many pieces that the picture begins to form. If you can't get the pieces, the case remains unsolved and even more frustrating for the victim, is considered unsubstantiated by law enforcement.

We recently passed a bill similar to this in California, now Penal Code 530.8 (SB 125, California Senator Dede Alpert, San Diego), enacted January 2002. The ITRC was the sponsor of the bill and had the opportunity to talk with many groups about the purpose of the legislation and to listen to those who did not originally support it.

Some of those who opposed the bill feared we would create a vigilante environment. Far from it. Victims of identity theft only want to clear their name. They are more than willing to let law enforcement take over in terms of criminal prosecution. Victims are well aware that some imposters are on drugs or part of gangs and that even driving past a known location could be dangerous.

This bill will also enable law enforcement to gather evidence in a timely manner, saving critical staff time and taxpayer money. This bill ultimately should result in getting larger numbers of these imposters off the street and lead to minimizing the economic loss to business.

Sec. 6. Amendments to the Fair Credit Reporting Act

This section deals with two issues: the ability to block fraudulent accounts on an individual's credit report and extension of the statute of limitations from moment of occurrence to the moment of discovery.

Blocking: Fraudulent accounts can and are being used in assessing credit scores and affect a consumer's purchasing power. If I am able to show with some reliability that I was not the person who opened this account it should not be held against me. Unfortunately, it may take several months for a credit issuer or collection agency fraud investigator to look into a case and make a determination—is this a case

of a deadbeat card holder who charged more than they realized or is this a legitimate case of identity theft.

This section will enable victims to more quickly expedite their recovery. This is vital especially since many victims hear about the crime when applying for credit. They may be purchasing a house or a car. Even a delay in a few weeks could affect the cost and availability of the purchase item. One of ITRC's regional coordinators (from San Francisco, CA) found out about her situation when trying to purchase a house. It took 1½ years to finally clear her credit report to the point that she could qualify for a mortgage again. Of course, housing costs had significantly increased and the mortgage broker asked for a higher interest rate.

I do have one problem with this section that will probably need to be addressed in future legislation—the requirement of a police report. According to the 2001 FTC report, 20% of all victims were unable to get the police to take a report. ("http://www.consumer.gov/sentinel" MACROBUTTON html ResAnchor www.consumer.gov/sentinel) My work with victims indicates that number may be much higher, perhaps ranging upwards to 50% or greater depending on the state and jurisdiction. At this time, California is the only state that I am aware of that mandates a police report must be taken, in this case in the jurisdiction where the victim lives (California PC 530.6). We do need to find a way to require local law enforcement to take police reports.

I have been informed that the credit reporting agencies may have a new policy of blocking on the basis of a "police report" and they believe section 6 is not necessary. As a consumer and victim advocate, I would like the reassurance that this voluntary policy has been made into a law, one that is not subject to change by the economic interests of a company whose primary customers are not consumers but businesses. I applaud their intent and do not understand their reluctance to back it up with legislation.

Statute of Limitations: Identity theft is an unusual crime. Most victims of other types of crime are involved from the moment the crime began. If your car is stolen, your house is robbed or you are mugged and your purse taken, you know about the crime almost immediately. This is not true in identity theft. In three studies (FTC, Florida Grand Jury, Privacy Rights Clearinghouse—all cited in footnotes below), the average victim didn't find out until 13–16 months after the crime first began. By law the clock started when the crime began, giving identity theft victims only a few months to investigate, assess the damage and find out how the crime may have begun. Many victims take a year or more to get to this point.

It is illogical to hold an identity theft victim to moment of occurrence. As in many cases of adultery, we are often the last to know of the crime. The group that knows best when an identity theft crime first occurs is the credit industry. They are the ones who know whether each application item exactly matches the items on the existing credit report. To date, consumers who place a fraud alert, requesting that no credit be issued without their express permission, do so with the understanding that credit issuers are not required to honor that request. (to be addressed in S1399).

Sec. 7. Commission Study of Coordination between Federal, State, and Local Authorities in Enforcing Identity Theft Laws

One of the biggest problems facing both law enforcement and victims is that identity theft is a multi-jurisdictional crime. I live in San Diego but the imposter may be opening accounts in Los Angeles, New York and Dallas. The perpetrator may make purchases in various areas in one county. The Los Angeles area has 46 different law enforcement agencies in that one county alone. That does not include federal law enforcement, DMV, military, post office, immigration, IRS or Inspector General's Office of the Social Security Administration.

There are many questions that still need to be addressed.

- Who should investigate the crime? Most often it falls to local law enforcement to solve the crime. But which one? Is it the agency where the consumer lives? Is it in the jurisdiction where the biggest commercial victim is, assuming that they filed a crime report which many do not? If the crime is occurring in multiple areas, can one local agency afford to investigate a crime that may cross the nation? Rarely.
- Does this conflict contribute to the low arrest rate? Probably. It definitely contributes to victim frustration as they get passed from one agency to the next. In terms of prosecution, we find the same confusion and eagerness to pass the case to another location.
- Why are businesses reluctant to report this crime to law enforcement? Is there a way to encourage more active reporting?
- Is there a way to ease communications between jurisdictions?

- Where are these crimes going to be prosecuted? Is it in the jurisdiction where the consumer lives or where the largest economic loss to a commercial victim is located? Will the crime be combined or is this person going to be tried repeatedly, once in each location?

Clearly we need studies to make recommendation about this issue. I hope one other recommendation will be to require the reporting of identity theft crime by law enforcement, perhaps even including it on the FBI Master Crime Index. Until we statistically know the extent of the crime we can't combat it. I know that you have been also frustrated by the varying statistics you have encountered. Of course, it raises the issue of how to count identity theft crime. If one imposter uses the information of 10 consumers to steal merchandise from 20 stores, is this one crime, 10 crimes or 30 crimes?

Testimony in Support of S. 1399:

For years consumers have sought to have more effective control over who can access credit lines in their names. We know that criminals have taken full advantage of the reluctance of the credit industry to take positive, proactive steps against identity theft. This bill takes vital steps in empowering consumers and businesses to avoid identity theft situations. Again, I will address the major three sections of this bill.

Confirmation of Changes of Address—Account Takeover and Consumer Reports

Account takeover has been a problem for many years. It is fairly easy to find out the credit card number of an individual, through mail interception, shoulder surfing, on register receipts and through scams both by telephone and over the Internet.

The United States Postal Service introduced a successful program that mirrors the one recommended in this legislation. It mandates that when an address change is requested that a card be sent to the current address on record and to the new address, informing the consumer of the requested change. The card directs the consumer to notify a toll-free hotline should they dispute the change of address request.

This bill would create a similar program providing a consumer a proactive way to control changes on accounts already opened under his or her name. It would prevent criminals from changing the billing address on an account and then applying as a secondary card user. By changing the address, it could take several months for the consumer to realize another person had accessed the account, especially if this was a card that was not used frequently.

The second part of this section addresses the problem in which a person has requested a credit report relating to a consumer, and the request includes an address for the consumer that is a different location from the most recent address in the file of the consumer.

One problem area of identity theft is that many thieves use addresses that are different from that of the original consumer. Each time a perpetrator applies for credit the address on the application is entered onto your credit report. These addresses may be drop spots at postal box stores, apartments used for criminal purposes, the middle of a lake, an empty lot or even the address of an innocent third party who works between 8 am and 5 pm, the times that FedEx and UPS usually deliver. The criminal picks up the package with the homeowner never knowing that their address has been used to commit a crime.

Because of this, many consumers find any number of erroneous addresses on their credit reports. In my work with victims I've seen credit reports with up to 20 wrong addresses, all apparently currently in use. The three major CRAs are all using automated systems now. When a consumer requests a copy of a report, he or she must give the number part of his/her residence, supposedly the last one on the report.

Again, it stands to reason that the credit reporting agencies need to exercise due diligence in verifying that the credit report goes to the right person.

If you will excuse my candor, both of these bill concepts are no-brainers and should have been implemented voluntarily by industry years ago.

Fraud Alerts

The ITRC receives at least 50 inquiries each week from consumers who either are concerned about identity theft vulnerability or who fear they may have already become a victim of identity theft. They contact our offices asking about what actions they could take to prevent identity theft and to make sure that no one can open credit lines without permission. They want to be good consumers and wish to protect their family and credit history.

A 1999 Lou Harris-IBM Consumer Privacy Survey reports that 94% of Americans think personal information is vulnerable to misuse. I believe that number has re-

mained the same or even increased. We have all heard media reports that explain that our information is handled by far too many people on a daily basis. In an advertisement recommending traveler's checks, American Express stated that a wallet is lost or stolen every 10 minutes.

Current identity theft victims want to stop the perpetrator from opening yet another account. Many fear with good reason that unless they immediately lock the door to credit the perpetrator will continue to attack them for years to come. Even if the imposter is arrested, there is no guarantee that he or she will not sell the information to another individual who in turn will try to open credit using the consumer's information.

The only measure of control over the establishment of new credit lines is through a fraud alert placed with the three major credit reporting agencies. Unfortunately, at this time the notice of a fraud alert—"Do not issue credit without my express permission. I may be reached at 555–555–5555"—is advisory in nature only.

This bill addresses two vital issues. It will make sure that every credit issuer sees and observes the words "fraud alert" or "fraud victim" regardless of whether a full credit report, credit score, or summary report is requested. This has been the bill that consumers have wanted for years, the ability to lock the door before a theft occurs. To not allow consumers to have this option is the same as saying—"Yes, you may put a deadbolt lock on the door but you don't have control over when it gets used." The measure of security that this bill will provide is tremendous.

In your explorations of identity theft, you have probably learned far more about your vulnerability than you used to know. Perhaps more than you ever wanted to know. As someone who hears about the results of this crime multiple times a day, I am all too aware of my exposure. I am more than willing to forgo instant credit in exchange for the knowledge that with a fraud alert, no one shall be able to get credit in my name without my permission. The savings of 175 hours and $1,100 (victim costs to restore financial health) are small compared to the emotional impact of this crime. I pray that none of you will experience the problem of identity theft. This bill might help make that wish possible.

Second, it establishes penalties for failure to observe these preauthorization requests and alerts. This is essential. Without the penalty part of this bill, I fear that the decision between "should I observe a fraud alert" and "the customer will take his or her business elsewhere and I'll lose my $400 commission" is too subject to the whims of avarice.

It is impossible to state loudly or clearly enough how important this section of S. 1399 is to consumers and in turn to the nation's economy. If this bill is passed, the potential savings to credit issuers, financial institutions and merchants could be in the billions of dollars.

Truncation of Credit Card Account Numbers

This section requires that no person, firm, partnership, association, corporation, or limited liability company that accepts credit cards for the transaction of business shall print more than the last 5 digits of the credit card account number or the expiration date upon any receipt provided to the cardholder.

My comments on this shall be brief. Mary goes shopping. It's a busy time, perhaps a white sale or during the holidays. As she wanders from store to store, she doesn't notice the gray-haired woman walking behind her. In fact, unless you are trained, you may not even notice that the older woman has slipped her hand into Mary's purchase bag and pulled out the receipt for the sweater she bought a few minutes ago. On this receipt is Mary's credit card number. By the time Mary gets home a few hours later, this woman (minus the wig) has hit two nearby shopping centers and charged about $3,000 in merchandise to Mary's account.

California has already established a truncation law. At first, stores were reluctant to embrace this law stating that it would cost too much. Using an extended implementation date, similar to the one on this bill, California merchants have been allowed the opportunity to make computer changes in registers as they were replaced and didn't require a quick overhaul of their entire system. Truncation is smart business, both in showing that merchants are concerned about consumers' economic safety and in terms of loss prevention. Even the California Better Business Bureau is supporting this action in California (as reported by the San Diego branch) and reminds businesses about truncating whenever they find a receipt where the system has not yet been changed.

Concluding Statements

Identity theft is a national crisis and the system allows, in fact encourages, criminals to take advantage of sloppy and thoughtless business practices. Media and community groups I speak with often asked why the increase in this crime. The answer

is simple—this crime is almost irresistible. It has become ridiculously easy to commit this crime. Criminals know victims will get bounced from one jurisdiction to the other, often failing to find someone to investigate the crime.

They also know that most businesses will not file charges against them. They count on the fact that in today's tight competitive market a company's greed may overcome caution and that fraud alerts will be ignored.

How does one combat a crime like identity theft given all these issues? How do you finally start to control the crime rather the crime controlling society?

We educate consumers and businesses. We give law enforcement the budget, staff and training they need to investigate financial crime. And finally, we do what I hope you will do as a result of today's hearing. We pass laws that make it more difficult to commit the crime. We pass laws that empower consumers and law enforcement to find these criminals so they can't hide because of the system. We pass laws that force reluctant businesses to do the right thing, despite the fact that it may cost a few dollars up front. In the end, they will realize an economic gain—in reducing investigative time of fraud investigators, in loss of services and merchandise, in legal fees, restocking time and costs, and in improved customer relations which draws people to their front doors.

This bill is smart business and companies, credit issuers and financial institutions should actively lobby for this bill. Companies who carefully monitor the bottom line and observe fraud alerts, confirm address changes and practice truncation are not as inviting to imposters. I believe law enforcement when they tell me that imposters trade information on easy targets and ways to commit identity theft. The explosive growth of identity theft confirms this as well as the number of repeat offenders. Like any other job, you improve with experience. The imposters of today have turned their livelihoods into a multi-billion dollar industry.

Your constituents deserve nothing less than the passage of these two bills. To not pass them would be to enable criminals to continue to attack and victimize consumers and businesses.

Thank you for your tine in considering my statements. If you have any questions, I would be most willing to answer them. I may be reached at ="mailto:voices123@att.net"MACROBUTTONHtmlResAnchorvoices123@att.net or during work hours at 858–693–7935. Please be persistent in calling. Our lines get very busy with victim calls.

Linda Foley
Executive Director
Identity Theft Resource Center

Addendum from ITRC 5

Many victims compare identity theft to rape, others to a cancer invading their lives. Many of the symptoms and reactions to identity theft victimization parallel those of violent crime. The following information is for understanding and, perhaps, to reassure victims that what they are experiencing is not abnormal. The reaction to identity theft can run the full spectrum from mild to severe. Clearly, the complexity of the crime itself will also define the severity of the import, as will any other traumatic events that may occur around that same time frame.

Impact: The moment of discovery.

- Can last from 2 hours to several days.
- Reactions include shock, disbelief, denial, inappropriate laughter, feeling defiled or dirty, shame or embarrassment.

Recoil:

- Can last for several weeks or months, especially as other instances of theft are uncovered.
- Physical and psychological symptoms may include: heart palpitations, chest discomfort, breathing difficulties, shortness of breath, hyperventilation, dizziness, clumsiness, sweating, hot and cold flashes, elevated blood pressure, feeling jumpy or jittery, shaking, diarrhea, easily fatigued, muscle aches, dry mouth, lump in throat, pallor, heightened sensory awareness, headaches, skin rashes, nausea, sexual dysfunction, sleep disturbance.
- It is not uncommon for victims to frequently search through events trying to pinpoint what they did to contribute to this crime.
- Anger, rage, tearfulness, overwhelming sadness, loss of sense of humor, an inability to concentrate, hyper-protectiveness, and a deep need to withdraw are all part of the psychological reactions to identity theft.
- You may misplace anger on others, especially loved ones causing family discord. Those who tend to lean on unhealthy habits such as under or overeating, smoking, alcohol or drugs may be drawn to those additions for comfort.

- During Recoil, victims may experience a sensation of grief. They may grieve the loss of: financial security, sense of fairness, trust in the media, trust in people/humankind and society, trust in law enforcement and criminal justice systems, trust in employer (especially in workplace ID theft), trust in caregivers and loved ones, faith, family equilibrium, sense of invulnerability and sense of safety, hopes/dream and aspirations for the future.
- At one point or another, almost all victims will also grieve a loss of innocence, sense of control, sense of empowerment, sense of self and identity, and sense of self worth.

Equilibrium/Balance/Recovery:

- In identity theft, this phase may come as early as several weeks after the crime and for others may take months or years. It usually depends on how quickly the actions of the imposter are resolved and cleared up.
- For all victims, achieving balance and entering recovery will take awareness and purposeful thought.

IDENTITY THEFT RESOURCE CENTER 2001 MILESTONES AND ACHIEVEMENTS

The level of activity in ITRC's office increased dramatically in 2001 as we assumed a larger role in the battle against identity theft. In July, we increased our staffing level to two by adding a Director of Consumer/Victim Services in response to the severity and volume of victim cases we receive, up from 2–5 per week in 2000 to 60 requests for help each week by email or phone by the end of 2001.

ITRC's web site,
="http://
www.idtheftcenter.org"MACROBUTTONHtmlResAnchorwww.idtheftcenter.org,
which first appeared in March 2001 is one of the most comprehensive sites on this topic today. It contains current information on prevention, self help guides (self-advocacy encouraged), a comprehensive reference library, fraud complaint forms, legislative information resource links and access to help groups nationwide. It averages 10,000 visits each month.

On the legislative front, ITRC is proud to announce that our first recommendation for legislation in California, SB 125 (Alpert), was signed and now is California Penal Code 530.8. This law gives victims and law enforcement greater and easier access to information on fraudulent accounts opened in a victim's name. By the end of 2001, ITRC had been sought out by legislators throughout the country, requesting support and guidance about state and federal legislation under consideration, including 2 federal bills now under discussion.

Our volunteer staff, who give so graciously of their time, has also increased. Our regional network has expanded and now includes coordinators in San Francisco, Wine Country/No. Calif., Dallas, TX, New Hampshire, Maryland, Olympia, WA, Atlanta, GA, Seattle, WA, Bridgeport, CT, Southcentral/East Michigan, Chicago, Akron, OH, Milwaukee, WI, Los Angeles and San Diego CA.

Besides being available to all media, ITRC is particularly proud of the inclusion of an identity theft consumer education page in the California 2001–2002 Pacific Bell white pages, recommended to the company by Exec. Director Linda Foley and written by her. A letter by Foley that appeared in the Aug. 12, 2001 Ann Landers column resulted in more than 1,000 emails from victims and concerned consumers in a 4-week period of time and an increase of more than 6,000 additional visits to ITRC's web that month alone.

Presentations made to financial institutions and law enforcement agencies have inspired identity theft awareness programs and enhanced relationships with victims. Foley and ITRC is currently working with the California Association of Collectors to put together an information sheet and standardize practices by collection agencies dealing with identity theft cases.

ITRC is now called regularly by law enforcement around the country—to ask advice on how to handle a situation, for permission to reprint self help guides for distribution and to refer difficult cases for assistance. Exec. Director Foley spoke at the March 2001 CA Union of Safety Employees, took an active role in the creation of the new FTC Standard Fraud Form, served on the CA Dept. of Motor Vehicles' Anti-Fraud Task Force, the CA Attorney General's Identity Theft Task Force and acts as an advisor for the CA Department of Consumer Affairs, Office of Privacy Protection, which included a training program for their hotline counselors.

Finally, ITRC is proud to announce that our director, Linda Foley, has received several citations for her exemplary work and is the recipient of the Channel 10

Leadership of San Diego "Individual Leader of the Year" Award for 2001, awarded by KGTV, the San Diego ABC affiliate.

Chairperson FEINSTEIN. Thanks very much, all of you, for your testimony. It was very interesting.

Attorney General, let me begin with you. It is my understanding that Washington State law, along the lines of what Ms. Foley was saying, gives identity theft victims copies of any documents the businesses have, such as credit card applications related to identity theft. I am concerned about the opportunity for a thief to exploit that. That is the only downside that I can see to this.

Could you comment on what your experience has been with this and what happens if a thief pretends to be a victim and convinces a company to give him another person's credit application?

Ms. GREGOIRE. Well, that was an issue that we dealt with when we introduced the legislation. In the end, what business and the credit card companies and we agreed to, though a bit onerous on victims, but nonetheless addresses the concern you just expressed, is that a victim of identity theft in the State of Washington can request the information.

If the business is concerned at all about whether this person is, in fact, a victim and the actual person, then they go into the State Patrol of Washington State and are fingerprinted and can prove they are who they say they are, the result of which is the business must then produce the information and is then held not liable for in good faith responding to the request of the consumer.

Chairperson FEINSTEIN. Does your law require that fingerprinting identification?

Ms. GREGOIRE. Yes. If the business is unwilling to turn it over, then in order to hold that business liable for refusing to turn it over—if they do not turn it over at the request of the consumer, the business is liable and can be held liable in court. The business has the right to ask for that fingerprinting through the State Patrol. Once that is done, once that compliance is done by the victim, then the business absolutely has to turn it over or be held accountable in court.

Chairperson FEINSTEIN. Would you advise that in a Federal law?

Ms. GREGOIRE. Well, you know, our concern about that is it is onerous on victims. Our law has only been in place since July. We have had about 20-plus, 22, who have actually had to go down and get their fingerprints taken. I wish there was a less onerous kind of thing that could be done by victims in order to prove that, whether that is this document that can be done maybe in a way that would be acceptable to businesses and consumers equally. That may be the more appropriate vehicle. I am very concerned about satisfying the needs of the business, while at the same time not, in essence, revictimizing the victim.

Chairperson FEINSTEIN. Right, right.

Do you want to comment on that, Ms. Foley?

Ms. FOLEY. Yes, I would, because California also has a law. It is Penal Code 530.8, and actually the Identity Resource Center was the source of that bill. We helped to inspire that when it was carried by California Senator Dede Alpert, whom I know you know.

Chairperson FEINSTEIN. Right.

Ms. FOLEY. The Department of Consumer Affairs' Office of Privacy Protection is now working on a forum to help victims work with this situation. What we have required is a police report along with the affidavit of fraud, and that is submitted to the businesses.

The problem with that is that while California has a law, it says a police report must be taken in the jurisdiction where the victim lives. That is not true in many States and we still see a high number of victims who are not able to get police reports to start with. Without a police report, the credit issuers don't take you seriously. So we almost have to do something simultaneously that says a police report must be taken by local law enforcement to help that victim. The idea behind that was if someone is willing to go to the police and make a police report, they are less likely to be an imposter.

Chairperson FEINSTEIN. Inspector Cannon, do you want to comment on that?

Mr. CANNON. I would agree. By coming in and making a false report, first of all, they are going to subject themselves to a separate liability for the false report. Additionally, it would be a problem in some areas, depending on what the current statutes are, because if you go to the police and you say you want to report an identity theft, if there is no crime there, some agencies may have a problem taking the report because they are not reporting a crime. So what do I take the report for?

The best thing that I could probably do in most jurisdictions is take a miscellaneous report, which is going to get filed in just a general field. If someone actually needs to come back and research that, they are going to have trouble locating that. So that would be a problem for the victim. Even though they are making a report of identity theft, it is going under miscellaneous. It is not a crime, it is an incidental.

Chairperson FEINSTEIN. Do you happen to know, in every State can a victim get a copy of a police report? I don't think so, under present law.

Mr. CANNON. No. It would be difficult. Then again, it would depend on the agency taking the report, too. For instance, we had a case of identity theft at the U.S. Mint, where one of our employees had her identity stolen. The report was made to us, the U.S. Mint Police, not to the Metropolitan Police Department. So this report was processed through the Department of the Treasury and not through a local agency.

Chairperson FEINSTEIN. So in other words, if we were going to provide for that, we would have to provide that in these cases a police report should be provided to the victim, which might be difficult.

Ms. FOLEY. We also have another problem. There are still five States within the United States that do not consider identity theft a crime. I believe Alabama just finally added to the group that does state that identity theft is a crime, but we still have five States, including New York, which is one of the top five States in the country in terms of number of suspects and victims of identity theft.

Chairperson FEINSTEIN. Of course, that is going to change. One of the problems is going to be that every State is going to have a different set of laws and it is going to make it very difficult for

businesses. There will be no common threshold for businesses. I think as Inspector Cannon and others have pointed out, one thief can touch a dozen or two dozen States easily, so it becomes a difficult problem

Ms. FOLEY. You almost have to say the jurisdiction is where the consumer lives. There are always two sets of victims in this crime, the consumer victim and the commercial victim.

Chairperson FEINSTEIN. Thank you.

Senator Kyl.

Senator KYL. I will just ask one question and then I am going to have to leave and I will figure out later here from the staff exactly what else we need to do to hone in on this, because we need to be aware of the very practical problems in constructing this, and I know that is the intention of all of us here.

When you say that there is no crime, Mr. Cannon, there is a report that my identity might have been stolen and I want the police to know about that. Is that what you mean, but you don't necessarily have any tangible evidence that, in fact, that happened?

Mr. CANNON. Let's say we do have tangible evidence. Law enforcement operates on probable cause, the key foundation of every case. Let's say that I do have probable cause that your identity was stolen, but I don't have a law to back it up with. That is the first problem, such as in the States that do not have identity theft laws.

So then even though I may as a law enforcement officer have probable cause to believe that your identity was stolen, if I don't have a law that it violated, I have probable cause on nothing.

Senator KYL. I understand that, but if I call you up and say my house was just broken into and they stole camera, well, you don't know whether they stole my camera or not, but you will still take a report on it, won't you?

Mr. CANNON. Absolutely, based on the law. There is a law there.

Senator KYL. I understand you have to have a law, but if I come down and I say I believe that my identity has been stolen and here is the information that leads me to that conclusion, and there is a law in the State of Arizona that prohibits that, then the officer needs to take that down in a police report, right?

Mr. CANNON. Absolutely. The officer then has a foundation to start on because you are providing him with some type of avenue to start and to investigate based on the fact that you may have the credit card receipts, you have different things that you can produce. So he should take a report and the investigation should start.

Senator KYL. And then finally is there anything on the police report that should render it unavailable to the reporting victim?

Mr. CANNON. There is nothing that should. In many cases, even if there is no provision, under a Freedom of Information Act request you can normally get it.

Senator KYL. So there is no particular reason why it shouldn't be made available to the victim, in your opinion?

Mr. CANNON. That is correct.

Senator KYL. Attorney General, do you agree with that?

Ms. GREGOIRE. Absolutely.

Senator KYL. Okay, good, thanks, and I apologize for having to leave.

Chairperson FEINSTEIN. Thanks very much, Senator.

Senator Cantwell.

Senator CANTWELL. Thank you, Madam Chairman. I want to go back to a couple of points that are about the basic information and access to information and how critical that is, and coordination.

Mr. Cannon, you emphasized in your testimony how important it was for law enforcement, not just the victims, but for law enforcement to have access to this information. Oftentimes, it is nearly impossible for you to follow up and do your job because you don't have access to the information.

Mr. CANNON. That is correct. We have several active cases that are being investigated right now. We have had problems garnering information from the companies that we need to get it from in regard to where property was shipped to or whatever because they have liability concerns about who they are violating.

We know that they are not violating the victim, but we either have to go sometimes to a grand jury, grand jury subpoenas for them to produce it, or we will have to take an inordinate amount of time to get to the case source of what we need. By the time we get to the base source, by the time we get to that address, as you have heard, they have moved on to another address. Therefore, we are back to starting all over again. So quick access is a definite need for law enforcement.

Senator CANTWELL. And if the process was expedited either by an I.D. theft affidavit or some other process, then you could become a participant in that investigation almost immediately.

Mr. CANNON. Absolutely, we would be able to become a participant. The other key thing there would be the fact that we would be able to link hopefully with other law enforcement agencies.

Let's say the identity has been stolen here in Washington, but they purchased the property in Mobile. We want to be able to contact a local law enforcement agency in Mobile. They also may be violating additional local laws there as far as forgery or other things that we could get them on. That would also enable the local prosecutors to get involved.

As you have heard many times, there is a threshold that people are looking for. Sometimes, Federal prosecutors are reluctant to take it because it doesn't make that high threshold, but there are many other local avenues that could be pursued. We would like to see that be made available also.

There are different tiers that you could put it on, that they could be handled locally up to this amount and then after that it becomes Federal. There are any number of things that you could do, but it has to be a joint team effort between local, municipal, State and Federal to be able to have a good loop, once you get this, that you can work with.

Senator CANTWELL. Can you or Attorney General Gregoire talk about the RICO section of the legislation that I am proposing because that obviously integrates at the Federal level? You mentioned it in your testimony, as well, as an added tool that you thought was beneficial.

Ms. GREGOIRE. I do, because you have got that it is a predicate offense to the application of RICO, and RICO is important to victims. If you are ultimately able to find the perpetrator, then they can go after the assets. Otherwise, they will forever struggle being

able to get anything back, either the business or the victim themselves getting anything back. This particular provision, I think, is an important aspect of being able to make whole the victims.

Senator CANTWELL. So you are saying if somebody stole my identity and went and purchased a new car or an expensive watch or something of that nature, this would allow both the business and the victim to have access to that asset as repayment?

Ms. GREGOIRE. Or to get at other assets that weren't even fraudulently gotten by the perpetrator to get after that individual's personal assets, which we think is important in this area.

Mr. CANNON. It is a tactic that is used throughout law enforcement when you seize the assets that are gained throughout it either legally or illegally, and then those assets can come back to the Federal Government or to the victims. Part of it could be divided up into a victims witness assistance fund, part of it to the business, part of it to fund the Federal legislation, or even to fund homeland security if you needed it.

Senator CANTWELL. Thank you. I don't have a question as much as a comment on your holding up Senator Feinstein's Web site or page. It reminded me of several years ago, prior to my being in the Senate, someone saying I can find out your credit card information within 24 hours. And I said, well, okay, prove it to me, and literally they did come back—I am not going to tell you what Web site does this, but they came back with my credit card information, everybody in my family's credit card information, my former employer's credit card information, all available in a report online.

So the issue here, Madam Chairman, is that the information available online has brought an anxiety that somehow all of these parts of our lives are somehow pieced together. Even the basic information that can be provided online can then be pieced together with other information to build this background, making someone who wants to steal an identity very enabled. That is why I believe that stronger laws and stronger coordination are very important.

Mr. CANNON. Let me just add that I just picked Chairman Feinstein's Web site. I could have picked anybody else's and done all of you or whatever. I will be working with your staff. There are just a couple of corrections we can make and your Web site will be safe and secure. The information will be there, but not in the manner that they can take it to use other places.

Chairperson FEINSTEIN. You are saying my Web site is such that they can do that?

Mr. CANNON. I was able to obtain enough information off your Web site to obtain a credit card.

Chairperson FEINSTEIN. Really?

Mr. CANNON. Yes, ma'am.

Senator CANTWELL. I just want to correct something. I meant Social Security number. I am sure there are ways to get credit card information. This was a report on Social Security numbers, which then led to people to get other information about credit cards.

Mr. CANNON. All you needed was the basic information. That basic information gives you access to another site that you can put the basic information that you got off the first site on that will feed you the additional information so that you can then get to your final destination.

I will meet with your staff afterwards.

Senator CANTWELL. I am not saying that that kind of information couldn't have been gathered in other ways, but some piece might be at the courthouse about your property.

Mr. CANNON. Correct.

Senator CANTWELL. And some might be somewhere else, and what is happening is all of this can be more easily compiled. That is why, again, better tools are needed.

Mr. CANNON. You are one hundred percent correct.

Senator CANTWELL. Thank you, Madam Chair.

Chairperson FEINSTEIN. Thanks, Senator.

Senator Sessions.

Senator SESSIONS. Thank you.

Senator Cantwell, I didn't mention your legislation, but I like it, too. I think it has got a lot of issues in it that are very important.

Attorney General Gregoire, you talked about getting your records back. Let's just be frank. Isn't it true that there is likely to be very little abuse, especially if you have to file an affidavit like this? Criminals are not likely to use this process to get someone's credit card number. They can get it in so many other ways. It would be easier, I think.

I am inclined to think, Senator Feinstein, that the language as you have it now is sufficient. I don't think we will have a real abuse of it, and if we go too far theoretically, trying to protect perfectly what could be an abuse of rights, we may make it so difficult for victims that we can't be successful.

Is that your best judgment on the matter?

Ms. GREGOIRE. Yes. We were so frustrated in our trying to do our legislation. One of the pieces that we thought was important that is in Senator Cantwell's bill is this issue of blocking, so that if this victim knows that they have taken a credit card and run up the bill, the practice of the credit card companies now is they simply flag that. So I am the next creditor and I look at it and I see she has been the victim; that means she is susceptible and I am going to deny her credit.

What we were trying to ensure is that be blocked so that the next creditor doesn't even see that she has been the victim of identity theft and thus become skeptical about her creditworthiness. In order to do that, the negotiations with business and the credit agencies—the only way we could get them to do that, raising this issue of someone will come in and take advantage and be fraudulent doesn't make a lot of sense to me, we had to do this extra step to which I referred.

Senator SESSIONS. Who was raising that objection? Was it the businesses or consumer groups raising the objection on the potential privacy violation?

Ms. GREGOIRE. It was the credit card agencies.

Senator SESSIONS. Did they oppose the legislation?

Ms. GREGOIRE. They did, until we ultimately agreed to this fingerprinting exercise. I think this is a much better tool, to be honest with you——

Chairperson FEINSTEIN. You mean an affidavit, a sworn affidavit should do it.

Ms. GREGOIRE [continuing]. By the FTC, where you can track nationally what is going on in the country. You can know exactly how many incidents of identity theft. I mean, this would be uniform throughout the country, rather than every State having one way of doing it.

It would be, to me, better for consumers. I think this is a much easier way for consumers. And yet it is exactly what you say, Senator Sessions. To expect one of these thieves to go in and further their crime by doing this I just don't think is realistic.

Senator SESSIONS. Another matter you raised I think is very critical, and that is the statute of limitations. Almost all Federal statute of limitations are at least five years. I don't know why they made this one two when these laws were passed, but I would definitely believe that it should be consistent with normal statute of limitations for $5,000 theft and interstate shipment. Those are all five years. You could have $50,000 through credit card fraud, so I really believe that should be changed.

I am inclined to think, as an attorney general and prosecutor, Ms. Gregoire, that historically we have gone from the date of the crime. There are some date of discovery statutes of limitations. My first impression is it might be better just to go to a five-year standard statute of limitations here rather than trying to go from the date of discovery.

How does that strike you in terms of your overall approach to criminal law?

Ms. GREGOIRE. What I know I am opposed to, Senator, is two years. When I look at this crime, that is just revictimizing the victim. I would be much more favorable to five years, but I am in favor of what the Senator has put forward, which is date of discovery, which, as you know, in civil cases is a typical statute of limitations.

In criminal cases, yes, a five-year statute of limitations. But this is in a civil case, and therefore I think——

Senator SESSIONS. For a civil case?

Ms. GREGOIRE. Yes, and I think date of discovery is the preferable way to go.

Senator SESSIONS. For most of the predicate offenses for identity fraud and credit card fraud, the statute is five, is it not, on criminal cases?

Ms. GREGOIRE. Right.

Senator SESSIONS. Well, I may have less concern about that.

Inspector Cannon, you talked about actually making these cases work and how to have it occur. My view is there is no substitute for Federal and State investigators who have been given special responsibility on identity theft cases meeting regularly, sharing information on that.

Ms. Foley, you mentioned that businesses are concerned. I mean, most of the time they end up paying the loss.

Ms. FOLEY. Actually, they don't.

Senator SESSIONS. They don't?

Ms. FOLEY. You and I do. They pass the costs along to consumers. There is no business in the world that can afford to absorb the types of losses we are talking about. We can get in terms of higher merchandise costs, higher service costs, financial charges,

and any other way they can pass it along the line. If we can minimize that bottom line in terms of loss, we may even see prices rolled back a little bit.

Senator SESSIONS. I think that is a good observation, but what I observed in our task force was that local financial institutions had a self-interest in helping. If police officers can't get the banks to give them the records for weeks and weeks, so they have no interest in providing information or working the alerts or getting the information out that their tellers have identified—they stopped somebody or rejected a fraudulent attempt—they may go right to the next bank and be accepted at the next bank and end up with an individual victim being stuck with a withdrawal from their account or an illegal debt.

So I guess my question is do you have any ideas about how we could further really intense cooperative efforts between Federal, State and local investigators within our communities throughout the country, and maybe even share the information in one city with what is going on in other cities because the same people tend to move around?

Mr. CANNON. There are any number of ways you could do it. You already currently have several task forces in place. Right now, because of 9/11, you have already enhanced coordination and communication, which is the most important thing between State, Federal and local people.

I would suggest or proffer to the committee that you could utilize several task forces that are already in place for the dissemination of information. There is currently the U.S. Attorneys' terrorist task force. And let's face it, identity theft is a form of terrorism. I think you would agree.

Also, I think that in many cases you probably would find terrorists that are utilizing this to fund some of their operations. So I think by utilizing the attorneys' terrorism task force which is already in place with the U.S. Attorney's office, you would find a mechanism that is already there. This could just be one more subdivision that they have there as far as dissemination and coordination.

Senator SESSIONS. I am not sure you want to burden that task force. I think we need to focus on the routine con man who is out there routinely day after day cheating people, causing all kinds of havoc in the system, disrupting people's lives.

Mr. CANNON. That is correct. You could also utilize the fraud network that is already in place that is linked through most major police departments and States. I think just about every State is linked through the fraud information unit.

Senator SESSIONS. Well, I won't pursue it any further, but trust me, it is not at the level we need it to be. One of the things that needs to be done is the Attorney General has simply got to make clear to the Federal prosecutors and the Federal investigators that this is an enterprise worthy of their time.

I know we have got to focus on terrorism and I know that is going to drain some of the Department of Justice's resources. But for most districts in America, they don't have active, major, ongoing terrorist cases and they need to be affirmed in the commitment to investigate financial crimes.

Also, of course, the Secret Service is a Department of the Treasury agency. It has jurisdiction over these kinds of crimes. I think that is an agency that could be empowered to be more aggressive. As I said, the investigative team in Mobile was led by the Secret Service and they really were successful.

At the time they started, we had very few of those cases. After that, they were just routine monthly. Many of these were repeat, dangerous con men, really. The rest of their lives, they were going to cheat people. That is how they knew how to live. So moving that up as a priority, even though the amount of loss in any one district may not meet some Department of Justice or U.S. Attorney's guideline, is the challenge for us.

I thank both of you for your leadership on this and I appreciate it.

Ms. Foley, maybe you had a comment.

Ms. FOLEY. I was going to mention, very similar to what you have done in Alabama, California has a number of regional task forces that are involved in financial crimes and they have been very successful. It has taken a definite effort in terms of allowing larger budgets, staff and training for the specialized type of investigation that is necessary, and there needs to be greater communication. But California is working very hard on that and putting together task forces that are going after it with combinations of different groups of law enforcement.

Senator SESSIONS. I would just say this: When you raise this with any agency, they always say they need more money. But they have already got a lot of investigators. I mean, what do they do everyday?

When we did the fraud task force, there was no extra money. It was just that the police department had several skilled investigators who tended to work those cases anyway. The FBI had an investigator, the Secret Service led. I committed a prosecutor. The State put a prosecutor in. The banks sent their security people, who were often the first to spot the fraud. I mean, we really didn't need a lot more money.

Now, we could put some money in to encourage this in some fashion, but you can do that with guns. The Department wants more money for gun prosecutions. Well, we can give them more money for gun prosecutions, but they have already got Assistant United States Attorneys doing something, I suppose. I hope they are doing gun cases already. So I think that is the key to it.

How we energize that I don't know. We could give some sort of financial incentive to task forces. We have done it by paying overtime on drug task force matters.

Ms. GREGOIRE. I have been reluctant to say this. I have to be honest with you. Your attitude is a welcome attitude, but the victims out there are told when they report to local law enforcement this is a paper crime. That is why they are not taking the reports, that is why they are not following up, and that is why these victims are the best cop on the beat and that is why they took two years of their own lives. The one individual I referred to earlier quit her job and for two years was her own private investigator.

What you just expressed is an attitude, and what you all are doing here is what we need to say to the Nation, that this is a real

crime with real victims and it isn't just money and it is damage to business. As a Nation, we need to step up and prioritize it and put together the kind of cooperative relationship—local, State, Federal law enforcement—and make it a priority so that we don't tell victims it is paper crime, you are on your own.

Senator SESSIONS. Well, I think that is what I was trying to say. It is a big deal. It is a huge crime that should not be ignored. If it goes to the average police officer who does not have expertise in the matter, they don't know how to maybe work through all the system to solve it. It is a tragedy if we leave it up to victims. We don't leave it up to victims to solve armed robberies. Why should they have to solve these kinds of cases?

Chairperson FEINSTEIN. I would like to make a suggestion. We actually have two very good bills here. What I would like to recommend is that we put them together, that our staff and Senator Kyl's and your staff work together in doing this, and that we particularly take a look at the RICO part of it to use the racketeering statute to really set a kind of Federal threshold, at which point it becomes a Federal crime.

You can't have every small amount of identity theft essentially a Federal crime, but once it becomes an issue of RICO with a substantial amount and we know that they are moving among the States doing that, then it seems to me it is a justifiable RICO use.

In any event, I would like to put the two bills together, have a markup as soon as we can and move it out to the full committee. Any advice that any of our witnesses could bring would be very useful. I think the point that the Attorney General raised about using the FTC affidavit is an excellent one and I think we ought to incorporate that in the legislation.

One of my concerns is there are many of these which are small, too, and a prosecutor on a State level, as well as on a Federal level—we are told that Federal prosecutors won't take these cases much under $25,000, and that becomes a real issue out there that we have to work on. But where the prosecutions can be State prosecutions, they should be, and where there are State laws, they should be. But where there is a national impact and a substantial amount of money lost, it seems to me it ought to be a Federal crime, subject possibly to RICO.

Senator SESSIONS. I think we need to talk about whether we want to make that a RICO crime, but I would be open to discussion on that.

Chairperson FEINSTEIN. Okay. Well, why don't we do that and try to set a time limit that we do it in the next couple of weeks? Then we will have a little markup.

Senator Cantwell, is that agreeable?

Senator CANTWELL. Yes, Madam Chairman, I think that is a good suggestion. I again want to show my appreciation for this hearing today and discussion of this issue because I think it is a very important issue.

When I think about what we have done here in discussing larger privacy legislation, we have tried to get our arms around the fact that we are at the tip of the iceberg of an information age, and how do we protect citizens on privacy? These two particular vehicles, I think, deal with what the public sees as the most urgent issue; that

is, the protection of their identity from being stolen. I think it is something we can get our arms around.

We have, because of Washington and California laws and the testimony that we have had today, some good implementation and expertise that I think gives us the basis for that. So I would concur with your recommendations.

Chairperson FEINSTEIN. Great. Then we will move in that direction.

Let me thank all of you. If you could again take a look at the bills with the idea of merging the two of them, and if you have any other thoughts, please let us know. We very much appreciate it. Thank you so much. It has been a very interesting morning.

The record will remain open, and the hearing is adjourned.

[Whereupon, at 11:50 a.m., the subcommittee was adjourned.]

[Submissions for the record follow:]

SUBMISSIONS FOR THE RECORD

Statement of Senator Charles E. Grassley
"Identity Theft: Restoring Your Good Name"
Subcommittee on Technology, Terrorism and Government Information
Wednesday, March 20th, 2002

Madam Chair, thank you for holding this hearing on the issue of identity theft.

I want to take this opportunity to reaffirm my personal commitment to finding a solution to the ever growing problem of identity theft in our country. I have joined with my colleagues Senators Feinstein, Shelby, Kyl and Corzine in the past for the introduction of the *Identity Theft Prevention Act of 2001,* a bipartisan solution aimed at clamping down on Identity Theft and I stand today ready to work with my colleagues on the Judiciary Committee to craft legislation protecting Social Security Numbers.

Having an imposter take over your good credit and good name is an egregious invasion of privacy. The damage that is often done takes months and sometimes years to correct. The emotional damage and fear lasts even longer. Law enforcement estimates range from between 350,000 to 750,000 cases of identity theft occurring in America each and every year. The identity theft occurs often times as a means to mask the commission of other serious crimes by the perpetrator. Identity thieves have engaged in everything from credit card account takeovers, to check and bank fraud, to adopting the identity of an innocent person to hide who they really are, hoping to evade arrest for the commission of violent offenses.

We need to make it harder for criminals to steal innocent people's identities. But, industry also plays a major role in helping us accomplish this. I encourage industry to adopt consumer-friendly business practices and further develop protections that maintain the integrity of Social Security Numbers and other personal information of our citizens.

Statement of Senator Orrin G. Hatch
Ranking Republican Member
Before the Senate Committee on the Judiciary
Subcommittee on Technology, Terrorism and Government Information Hearing on

"Identity Theft: Restoring Your Good Name"

Madame Chairwoman, I want to thank you for holding another hearing on this important topic -- identity theft. The incidence of identity theft appears to be increasing dramatically, and as a result, it is one of the leading concerns of Americans today. These hearings are generating much needed public discourse about this critical issue.

Identity theft is particularly offensive because where the "theft" is successful, the primary intended victim will be the one who appears to have committed the crime. The innocent victim will be left to face investigations by credit card companies, financial institutions, and law enforcement agencies, while the real offender remains behind the scenes, unless and until the victim succeeds in clearing his or her good name.

Although there are no comprehensive statistics on identity theft, we have learned from the General Accounting Office that the prevalence and the cost of identity theft appear to be increasing: consumer reporting agencies have reported an increasing number of fraud alerts on consumer files; the Federal Trade Commission has reported an increasing number of calls to its Identity Theft Data Clearinghouse; the Social Security Administration's Office of Inspector General has reported a substantial increase in calls relating to identity theft; statistics from federal law enforcement agencies also suggest identity theft is growing; and two major credit card companies, Visa and Mastercard, have documented a rise in credit card fraud losses from about $760 million in 1996 to $1.1 billion in 2000, an increase of about 43 percent. According to another recent study, 1 in every 50 consumers has been the victim of identity theft in the past year, while 1 in every 20 consumers has been the victim of credit card fraud. While these numbers are staggering, we must recognize, as the GAO testified at our last hearing, that it is extraordinarily difficult, if not impossible, to measure the precise number and nature of identity theft incidents that occur each year.

As we consider legislation to address this disturbing trend, it is important that we carefully identify the problems we seek to solve and tailor our legislative responses to them. We need to ensure that any response is a measured and informed one, taking into account the legitimate needs of this nation's businesses and law enforcement agencies, as well as the privacy interests of consumers. I look forward to hearing what our distinguished witnesses have to say about legislation Senators Feinstein and Cantwell each have proposed to remedy various problems posed by identity theft.

I understand that a number of credit card companies have already instituted, or are in the process of instituting, their own password based and other security measures. I applaud such efforts. I am convinced that many of the harms consumers experience today can best be prevented if industries develop effective internal security measures.

As I have said before, I am committed to working with Senator Feinstein, Senator Kyl, Senator Cantwell and the other members of this Subcommittee to develop legislation that strikes the proper balance between the privacy rights of consumers and the needs of industry and law enforcement.

Statement in Support of S. 1399, "Identity Theft Prevention Act of 2002"

to the United States Senate Committee on the Judiciary

March 18, 2002

Joanne McNabb, Chief, Office of Privacy Protection
Kathleen Hamilton, Director, California Department of Consumer Affairs

---

California has long been recognized for its leadership in privacy protection, ranking number one in a survey conducted by the respected *Privacy Journal*. California finished at the top of the list because our courts and our state constitution provide the strongest privacy protection in the nation and because of our strong laws protecting personal information, according to the *Journal*.[1] Since the time of the survey, Governor Gray Davis has signed a number of new laws that protect individual privacy and provide assistance for identity theft victims. We urge the Committee's approval of S. 1399, which would bring the benefits of many of California's identity theft laws to other states.

California recently created the Office of Privacy Protection in the California Department of Consumer Affairs, making California the first state in the nation to have an agency dedicated to protecting and promoting the individual privacy rights guaranteed in the state constitution. The Office's statutory purpose is to identify consumer problems in the privacy area and facilitate the development of fair information practices. We do this by, among other things, providing direct assistance to identity theft victims and others with privacy concerns, educating and informing consumers on privacy issues, coordinating with law enforcement on investigations of identity theft, and working with businesses and other organizations on best practices in the handling of personal information.[2] The office opened in November 2001.

Over half of the consumers who contact the Office of Privacy Protection do so because of identity theft, either out of general concern (18%) or because they are victims of the crime (33%). Identity theft is a growing crisis in the United States and is frequently cited as the fastest-growing crime in the nation. The General Accounting Office, in a report released this month, concluded that "the cost and prevalence of identity theft seem to be increasing," and reported that the losses to Visa and MasterCard in 2000 came to $1 billion.[3] Identity theft was the leading consumer fraud complaint to the Federal Trade Commission last year,[4] and the Gartner Group just reported that one in 50 consumers has been a victim of identity theft.[5]

Victims regularly report the frustration they experience as they wend their way through the lengthy and tortuous process necessary to undo the damage done to their names and their credit histories. Identity theft has rightly been called "the crime that keeps on taking." A recent California survey of identity theft victims identifies many of the obstacles they face.[6] Among the survey's findings are the following:

- Victims surveyed reported learning about the theft an average of 14 months after it occurred, and in one case it took 10 years to find out.
- Victims spent an average of 175 hours actively trying to resolve the problems caused by their identity theft. Seven respondents estimated that they spent between 500 and 1,500 hours on the problem.
- The average total fraudulent charges made on the new and existing accounts of those surveyed was $18,000, with reported charges ranging from $250 up to $200,000. The most common amount of fraudulent charges reported was $6,000.
- Victims reported spending between $30 and $2,000 on costs related to their identity theft, not including lawyers' fees. The average loss was $808, but most victims estimated spending around $100 in out-of-pocket costs.
- Victims most frequently reported discovering their identity theft in two ways: denial of either credit or a loan due to a negative credit report caused by the fraudulent accounts (30%) and contact by a creditor or debt collection agency demanding payment (29%).
- Less than two thirds felt that the credit bureaus had been effective in removing the fraudulent accounts or placing a fraud alert on their reports. Despite the placement of a fraud alert on a victim's credit report, almost half (46%) of the respondents' financial fraud recurred on each credit report.

Like the substantially similar provisions in California law upon which it is based, S. 1399 addresses many of the issues enumerated above. S. 1399 would provide meaningful consumer protection against identity theft by giving consumers in all states more control over the information released in their credit reports and by restricting the exposure of credit card numbers to possible abuse.

Change of Address on Credit Accounts

One practice of credit identity thieves is to take over someone else's credit accounts by changing the address on the account so that bills containing fraudulent charges will not go to the victim. Forty-two percent of the identity theft victims who contact the California Office of Privacy Protection report that a credit account was opened in their name or that someone else used their account. This is one of the reasons for an identity theft victim's failure to learn of the crime for many months or even years after the first incident, and it was the reason for the passage of a new California law that just took effect in January 2002. This law requires credit grantors using consumer credit reports to verify a consumer's address when the address given by the consumer does not match the address on the consumer's credit report.[7]

S. 1399's approach to this problem is to require credit card issuers to notify the cardholder when the issuer receives a request for an additional card on an existing account within 30 days of a change of address on the account. The bill requires the card issuer to notify the consumer at both the new and the former address and also to give the consumer a means of promptly reporting the address change as incorrect. In addition, the bill requires credit bureaus to notify those who order a consumer's credit report of any discrepancy between the address provided by the report requestor and the address in the report. Like the similar provisions in California law, S. 1399 provides protection against a common practice of identity thieves.

Fraud Alerts on Credit Reports

Although the three major credit bureaus have procedures for alerting prospective credit grantors to an identity theft situation, many identity theft victims find it difficult to stop the continued issuance of credit to the imposter. The California victim survey cited above found that almost half of the victims experienced the recurrence of fraud on their credit reports, demonstrating that the existing fraud alert system was not effective. That was the reason for the recent enactment of legislation in California to require the credit bureaus to comply with a consumer's request to post a security alert, and even a security freeze, on the consumer's credit file, and thereby to prevent further fraud.[8]

S. 1399 addresses this problem by requiring credit bureaus to include a fraud alert in the consumer's file and to notify all requestors of credit information on the consumer of the alert. The fraud alert requires pre-authorization by the consumer before any credit can be extended. This provision will help protect consumers from being repeatedly re-victimized by an identity thief.

Truncation of Credit Card Numbers on Receipts

The epidemic proportions of identity theft require us to develop new habits of protecting our vulnerable personal information. Thieves particularly seek out financial information, such as credit card numbers. One way to protect personal information is not to display it where it can easily be seen and stolen. A California law enacted in 1999 requires that electronically generated credit card receipts must display no more than the last give digits of a customer's account number. In order to allow retailers to phase out older machines that could not comply, the law applied to new machines only beginning in January 2001 and will not apply to machines in use before that date until January 2004.[9] The law has been implemented over the past year without reported problems.

S. 1399 mirrors the California law, with later effective dates and a provision allowing states to impose the same or similar requirements before the federal effective dates.

[1] See "Rankings of States in Privacy Protection" at <www.privacyjournal.net>.
[22] California Business and Professions Codes section 350-352. For more information on the Office of Privacy Protection, see <www.privacyprotection.ca.gov>.
[3] See the March 2002 GAO report at <www.gao.gov/new.items/d02363.pdf>.
[4] See <www.consumer.gov/sentinel/images/charts/top2001.pdf>.
[5] Reported on MSNBC, March 4, 2002. See <www.msnbc.com/news/718115.asp>.
[6] *Nowhere to Turn: Victims Speak Out on Identity Theft*, by Privacy Rights Clearinghouse and CalPIRG (2000), at <www.privacyrights.org /ar/idtheft2000.htm>.
[7] California Civil Code section 1785.20.3, effective 1/1/02, provides that upon discovery that the address in a consumer file does not match the address given by someone requesting credit, a user of a consumer credit report must take "reasonable steps" to verify the address. A law enacted earlier requires address verification in a narrower category of transactions. Civil Code section 1747.06, effective 7/1/00, requires a credit card issuer who mails an offer for a credit card to a consumer and receives a completed application with a different address must verify the change of address by contacting the person to whom the offer was made.
[8] California Civil Code section 1785.11.1, effective 7/1/02, provides that credit bureaus must place a security alert on a consumer's file and notify those who request credit information on the consumer of the alert. A security freeze, which has features similar to S. 1399's fraud alert, requires the consumer's express pre-authorization for any issuance of credit (Civil Code section 1785.11.2, effective 1/1/03).
[9] California Civil Code section 1747.9.

STATEMENT BY SENATOR STROM THURMOND (R-SC) BEFORE THE JUDICIARY SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION, REGARDING IDENTITY THEFT, WEDNESDAY, MARCH 20, 2002, SD-226, 10:00 AM.

Madame Chairwoman:

Thank you for holding this hearing on the enormous problems associated with identity theft. Privacy of personal information is important to all Americans, especially in an age when details of financial transactions can be sent all over the world in an instant. It is important that Congress enact legislation that will protect personal identifiers, but at the same time will allow for the legitimate conduct of the business community and government agencies. I hope to work with my colleagues to develop a comprehensive and reasonable piece of legislation that will deter identity theft and provide peace of mind to all Americans.

Identity theft occurs when an individual obtains the personal information of a victim, such as a social security number or a date of birth, and uses that information to open accounts and establish lines of credit. In effect, a person with access to another's social security number can pretend to be a different person. Usually, the victim does not discover the fraud before the identity thief has

substantially damaged the victim's credit. The victim must then go through a long and arduous process to correct the situation.

According to a May 2000 report by the California Public Interest Research Group and the Privacy Rights Clearinghouse, victims of identity theft spent an average of 175 hours attempting to restore their credit, and this effort often required spending a significant amount of money. In addition to the hassles of restoring a good credit rating, victims of identity theft may also be criminally investigated as a result of the identity thief's actions. According to a General Accounting Office report from March of this year, in approximately 1,300 complaints to the Federal Trade Commission, identity theft victims indicated that they had been subject to criminal investigation, arrest, or conviction.

Unfortunately, the crime of identity theft appears to be on the rise. According to Consumers Union, there were 500,000 to 700,000 victims of identity theft last year. Alarmingly, the number of complaints received by the FTC in December of 2001 was almost double the complaints received in March of the same year. Moreover, the Social Security

Administration has reported that allegations of Social Security Number misuse increased from 11,000 in FY 1998 to 65,000 in FY 2001. I am concerned by the increasing prevalence of identity theft crimes.

Congress has addressed this issue in the past. The Identity Theft Act of 1998 established identity theft as a distinct crime and provided for punishment of fines and jail time. This Act gave law enforcement an important tool in the prosecution of identity theft. While the 1998 Act was a momentous step, we must do more than prosecute the thieves. We must also make it more difficult for these lawbreakers to access personal information. Without access to personal information, there would be no identity theft, and thousands of Americans would no longer be victimized.

One of the primary ways in which identities are stolen is by use of the social security number. Unfortunately, the social security number is ubiquitous and is used for many purposes other than its originally intended use. It is routinely used as an identification number by health care professionals, educational institutions, and many private businesses. People are often pressured into providing this very sensitive number, never knowing who may ultimately be

given access to their personal information.

I am therefore strongly in support of several current proposals regarding social security numbers. For example, one suggested proposal would prohibit companies from selling social security numbers to the public. Congress should close all avenues to the sale of social security numbers to the general public and conduct appropriate oversight to ensure that violators are prosecuted. Another good proposal would require Social Security numbers to be redacted from public documents where feasible. Yet another suggested reform would prohibit private companies from denying service to individuals who refuse to provide social security numbers, with specific exceptions for transactions such as those that involve credit checks. Most businesses have no legitimate need for social security numbers. Rather, the numbers are used for purposes such as identification and filing. Surely, there are other identification methods that could be developed easily, ensuring that social security numbers are not available to persons who would misuse them.

We should also take a serious look at the statute of limitations that applies to causes of action brought against credit reporting agencies for negligently issuing credit

reports that have been improperly requested. Under the Fair Credit Reporting Act, the statute of limitations is two years from the date liability arises. By the time a victim of identity theft discovers the wrongdoing, two years may have already passed since the identity theft occurred. In this situation, the victim could not hold the reporting agency accountable for its negligence. We should consider extending the statute of limitations so that victims of identity theft have a reasonable amount of time to discover the crime and take action to protect themselves.

I am very interested in working with my colleagues to draft a comprehensive and reasonable bill that will deter future acts of identity theft. Identity theft is a growing crime, and we should act now. I thank the Chairwoman for taking an interest in this important matter, and I look forward to working with my colleagues.

March 19, 2002

Honorable Diane Feinstein
Chairman
Senate Judiciary Subcommittee on Technology, Terrorism and Government Information
224 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Feinstein:

I want to commend you, Ranking Member Kyl and the members of your Subcommittee for taking an active role in addressing the growing problem of identity theft. It is clearly one of the most important consumer, commerce, privacy and national security issues of our time.

To that end, I am writing to respectfully ask that the following white paper published by LexisNexis, entitled "Identity Fraud: Providing A Solution", be entered into the record for the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information Hearing to be held on Wednesday, March 20, 2002.

As the Chief Officer for Privacy, Industry and Regulatory Affairs for the LexisNexis Group and the Chairman of the National Fraud Center, I want to assist your efforts in educating consumers on the pressing issues surrounding identity theft and identity fraud. Our findings and suggestions are based on our years of experience and expertise studying and dealing with these issues.

Again, thank you in advance for your consideration and please do not hesitate to contact me if I can ever be of assistance to you on this issue.

Sincerely,

Norman Willox
LexisNexis

Released: February, 2002

IDENTITY FRAUD: PROVIDING A SOLUTION

BY: NORMAN A. WILLOX, JR., and THOMAS M. REGAN, ESQ.

ABOUT THE AUTHORS

Mr. Willox is the Chairman of National Fraud Center, Inc. and Chief Officer for Privacy, Industry and Regulatory Affairs for the Lexis-Nexis Group, a division of Reed Elsevier, Inc. Mr. Willox is an expert on identity fraud prevention and investigation, having devoted much of his professional career to devising solutions to this multifaceted problem.

Mr. Regan is a member of the law firm of Cozen O'Connor, and Chairman of the Privacy Law & Regulation Department. He is a former prosecutor and has litigated many cases involving commercial fraud matters. Mr. Regan has been aided substantially in the preparation of this paper by Matthew F. Henry, Esq. Mr. Henry is a 2001 graduate of Villanova Law School and he is an associate with Cozen O'Connor. He has demonstrated a particular aptitude for understanding the identity fraud problem.

This paper is the third in a series of articles that Mr. Willox and Mr. Regan have collaborated on. The first, "Identity Theft: Authentication As A Solution," (www.nationalfraud.com/IDENTITY%20THEFT%203.13.htm) was submitted at the National Identity Theft Summit, convened by the United States Department of the Treasury, in conjunction with the Federal Trade Commission and other federal agencies in March 2000. The second article, entitled "Identity Theft: Authentication As A Solution – Revisited," (www.lexisnexis.com/aoa) was released in October 2001.

INTRODUCTION

On September 11, 2001, 19 terrorists hijacked four jet airliners, crashing two of them into the World Trade Center Towers, one into the Pentagon and a fourth into a field in western Pennsylvania.[1] Two of the terrorists were Abdul Azziz Alomari and Ahmed Saleh Alghamdi.[2]

Alomari was in a group of five terrorists who hijacked American Airlines Flight 11, bound from Boston to Los Angeles, which ultimately crashed into the north tower of the World Trade Center in New York City.[3] Alghamdi was in another group of five terrorists who hijacked United Airlines Flight 175, bound from Boston to Los Angeles, which ultimately crashed into the south tower of the World Trade Center in New York City.[4] In addition to the obvious acts of terrorism, Alomari and Alghamdi were guilty of identity fraud.

About a month before the hijackings, Alomari and Alghamdi used an accomplice to approach a secretary of a Virginia lawyer.[5] They paid her to complete false Virginia identity affidavits and residency certifications.[6] The documents indicated that Alomari and Alghamdi had Virginia residences, when, in fact, they resided in Maryland motels.[7] Using the false documents, notarized by the Virginia secretary, Alomari and Alghamdi obtained Virginia state identification documents.[8] These identification documents were used by Alomari and Alghamdi on September 11 to board the ill-fated planes.[9]

Reports are replete that the terrorists responsible for the September 11 hijackings made wholesale use of false identities, fraudulent identification documents and fictitious social security numbers.[10] Purportedly, five of the terrorists, in addition to Alomari and Alghamdi, procured fraudulent Virginia identification cards.[11] Another five reportedly obtained fake social security numbers.[12] Authorities believe that, at one time or another, each of the 19 terrorists may have used false social security numbers.[13]

Identity fraud, that is, the criminal use of false identities or fraudulent identification documents, has been the subject of much discussion, debate and legislation during the recent

past. However, most of that attention has been in the context of its use as an instrument of fraud, such as in credit card fraud, securities fraud, and bank fraud. The activities of the September 11 terrorists now cause us to realize that identity fraud is not just the tool of the con artist. It is, when properly recognized, indigenous to any criminal enterprise, whether it be drug trafficking, alien smuggling or cyber stalking.

REDEFINING THE IDENTITY FRAUD PROBLEM

On October 30, 1998, following considerable debate about the deleterious effects of identity theft, the Federal government passed the Identity Theft and Assumption Deterrence Act of 1998 (ITADA).[14] It cast as an identity thief anyone who "[k]nowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[15] State governments have also prohibited identity theft, using a definition of identity thief that is substantially similar to that found in ITADA.

Identity theft, as prohibited in ITADA and the state equivalents, is limited to the use of the "[m]eans of identification of <u>another person</u>" (emphasis supplied).[16] This focus on the use of a real person's identifiers, is sometimes referred to as "true person fraud."[17] The term has its origins in the harm that the statute intends to proscribe, that is, to an existing person, whose identity is assumed by the identity thief.[18]

Identity theft, as the legislative history to ITADA amply demonstrates, is a serious problem. According to the United States Secret Service, of the approximate 10,000 financial crime arrests that its agents made during 1997, 94% involved identity theft.[19] The United States Postal Inspectors and the Secret Service have reported that organized criminal elements are using identity theft as part of their international enterprises, involving not only financial crimes, but

also drug-related, immigration and violent crimes.[20] The ITADA legislative history further documents the effect of identity theft to individuals and corporate victims. Master Card estimated that of its approximate $407,000,000 in fraud losses in 1997, 96% of it was attributed to identity theft.[21] The Secret Service estimated that in 1997 the losses caused by identity theft, for which it made arrests, amounted to $745,000,000, with the losses doubling from the previous two years.[22]

As daunting as the above identity theft statistics are, the fact is that they are only the tip of the iceberg. When we consider that the collective losses occasioned by credit card fraud, insurance fraud and health fraud are in the hundreds of billions of dollars per year, and that identity theft comprises a significant part of these crimes, we can conservatively estimate that identity theft accounts for at least tens of billions of dollars in losses.[23]

Identity theft has, indeed, shook our national consciousness. However, as devastating its harm, the scope of the identity theft problem does not capture the terrorists' use of false identities and false identification documents. Alomari and Alghamdi did not assume an existing person's identity. In fact, they continued to use their own names, albeit with false addresses supported by fraudulently obtained identification documents. To address this problem, from a prevention standpoint, requires that we consider not only identity theft true person fraud, but <u>any criminal use of false identifiers or false identification documents</u>.

Some of the recent accounts of the use of false identifications and false identification documents illustrate the extent of this problem. In Tuscaloosa, Alabama, an employee in the county license office was arrested and charged with selling or giving away outdated drivers' licenses.[24] According to Alabama Bureau of Investigation Lieutenant Mike Manlief, five to ten of the outdated licenses were given or sold to people under the age of twenty-one, so that they would be able to purchase alcohol.[25] In Elgin, Illinois, Sergeant Brad Entler of the police

department observed that fraudulent ID cases are "a total epidemic."[26] He expressed particular concern about gang member use of false identifications to purchase guns.[27] In Portland, Oregon, a raid of a suspected identity theft ring resulted in the seizure of powerful explosives, methamphetamines, stolen mail and fake drivers' licenses.[28]

The term "identity theft," with its connotation of true person fraud, is too narrow a concept to capture these divers uses of false identities and false identification documents. We must use a term that properly reflects the broader problem. Although "identity fraud" has been sometimes used interchangeably with "identity theft," we submit that, when properly used, "identity fraud" envelops the entire breadth of the problem.

Identity fraud is certainly a financial fraud problem. It is, as the Secret Service reports, a substantial part of the financial crimes that the Secret Service investigates, including bank fraud, computer and telecommunications fraud, access device fraud, advanced fee fraud, etc.[29] Law enforcement officials also identify social program fraud, tax refund fraud and mail fraud as containing intrinsic elements of identity fraud.[30] In fact, identity fraud permeates as many as twenty-five different financial fraud crimes.[31] However, identity fraud is more than just a financial fraud problem.

Identity fraud is certainly a terrorism and illegal immigration problem. Alomari and Alghamdi, and their co-terrorists, illustrate the use of identity fraud in committing acts of terror. Terrorists, though, do not limit their criminal activities to creating mayhem. As Dennis Lormel, Chief of the FBI's Financial Crimes Section, told the House Committee on Financial Affairs, last October, "[t]errorist cells often resort to traditional fraud schemes to fund the terrorists' activities."[32] Lormel included identity theft as one of the terrorists' "prevalent" fraud schemes.[33] He noted, "The ease with which these individuals can obtain false identification or assume the identity of someone else, and then open bank accounts and obtain credit cards, make these

attractive ways to generate funds."[34] However, as serious a component of terrorism identity fraud is, identity fraud is not solely a terrorism problem.

As the Postal Inspectors have reported, identity fraud is a drug trafficking problem.[35] It is also a cyber crime problem, as Web stalkers hide behind the Internet's anonymity.[36] It is a computer hacking problem, as Eastern European criminals assume or make up passwords and user IDs to steal sensitive consumer data, in order to extort unsuspecting companies.[37] It is an alien smuggling problem, a gun-running problem and a money laundering problem. It is, as law enforcement officials have confirmed, a problem at the core of many different types of organized crime, committed locally, nationally and globally.[38]

IDENTITY FRAUD SOLUTIONS – A METHODOLOGY

Since September 11, the country's focus has been in preventing terrorism, including the terrorists' use of identity fraud. Congressional hearings have been conducted; reports have been submitted; and the popular press has frequently provided commentary, on potential solutions.

Although the USA PATRIOT Act concerns the prevention of terrorism, it primarily focuses on increasing law enforcement powers to investigate terrorists and on promoting financial institution vigilance to root out money laundering.[39] Identity fraud, as a component of terrorism, is not directly addressed in the legislation.

We have witnessed, however, a virtual cornucopia of potential identity fraud solutions to the terrorism problem, from biometrics to national identification cards. Promoters of biometrics point to the history of law enforcement use of fingerprint science;[40] the use of facial recognition at last year's Super Bowl which was attended by some 60,000 people;[41] and the availability of hand geometry biometrics which have reportedly been successfully deployed since 1985 at airports, nuclear facilities, chemical plants and other facilities constituting the nation's critical infrastructure.[42] Proponents of national identification, including the prominent civil libertarian,

Professor Alan Dershowitz, support it primarily because they believe it is simply needed in this age of terrorism, as our existing means of identification, such as drivers' licenses, have proved ineffective.[43]

Detractors of biometrics point to, among other things, the cost of installation, absence of proof of effectiveness and, most importantly, their potential use as a means to aggregate personal information such as spending habits, medical treatment, etc.[44] National identifications are often criticized for substantially the same reasons. Katie Corrigan, legislative counsel on privacy for the ACLU, in testimony before a House committee, captured the privacy objection by stating, "Unlike workers in Nazi Germany, Soviet Russia, Apartheid South Africa and Castro's Cuba, no American faces the demand, 'Papers, please.'"[45]

The mutual force of the arguments on either side of the biometrics and national identification issues has evolved into a virtual equipoise. We know we need solutions, but we fear the results. Fundamentally, what is lacking is a framework, a rudder, to guide us to the appropriate solutions and, ultimately, we need facts, not suppositions, to resolve the inevitable tests.

UCLA Law Professor Lynn LoPucki provides a framework, in his discussion of "the currently prevailing theory of human identification."[46] Citing Professor Roger Clarke's "foundational article"[47] where Clarke defined human identification as "the association of data with a particular human being,"[48] LoPucki provides three basic means for making identifications. The first such means is "knowledge-based" where persons are "[r]ecognized by demonstrating that they are in possession of information which only that person would be expected to know."[49] The second basic means of human identification, according to LoPucki, is "token-based" identification, where a person is recognized by their possession of an item, such as a national identity card, or a driver's license, or a passport.[50] Each of these "tokens" bears a description of

the person that presumably would not match an imposter's person. The third means of human identification is "biometrics" which LoPucki states, quoting Clarke, refers to "a variety of identification techniques which are based on some physical and difficult-to-alienate characteristics."[51] All three means of identification should be considered when devising an identity verification solution. However, in certain identification environments, not all of the means of identification may be necessary, or even appropriate.

Undoubtedly, the most difficult identification environment is where the individual who is seeking identity verification is unknown to the verifier, and has not been previously verified. This initial phase of identity verification can only occur through a knowledge-based, authentication[52] solution. As indicated above, there has been much discussion about implementing an effective token, or biometric, based system, such as a national identification card or a more narrowly applied "trusted-traveler" card, which is presently being considered by the United States Department of Transportation for airline passengers.[53] However, no such systems presently exist and, even if they did, there would still need to be an initial authentication process founded in a knowledge-based solution. To utilize a biometric or token based system, without first authenticating an individual, simply provides an opportunity to an imposter to link a false name, or other false identifiers, with the imposter's biometrics or token.

There have been attempts in the past to use a knowledge-based system of identification, limited to discrete identifying information, such as a person's social security number, or a mother's maiden name. These systems have failed when the social security number or the mother's maiden name became widely circulated, leaving them accessible by identity thieves. However, successful applications have been made of knowledge-based identifiers, when a sufficient number of them are combined so that they can be statistically confirmed through the use of models and scores. The financial community is a good example of the successful

implementation of such knowledge-based authentication systems. First USA, a subsidiary of Bank One Corp., successfully used such a solution in its credit-card issuing process.[54] The challenge is to apply the knowledge-based authentication systems, predicated on models and scores, to other identification environments, such as the foreign visa issuance process, where the information and technology are not as developed as they are here in the United States.

In implementing a knowledge-based authentication solution, there are certain non-identification factors, driven by the identification environment, that must be considered. The first such factor is the time to conduct the identification process. For example, in a credit-granting environment, the credit applicant will not wait more than several minutes for the verification process to be completed. This time period, sometimes referred to as the "insult rate," may be significantly less in one identification environment than it is in another. However, invariably, there is an applicable insult rate, whether the process is foreign visa issuance, airplane travel or daycare employee applications.

Another significant non-identification factor to consider for any proposed solution is the intricacy of integration. For any solution to be successful, it must be cost effective. Ideally, the solution should be compatible with existing systems and it must be capable of being applied by existing staff. However, if the solution is not readily compatible with existing resources, the cost of application must be balanced against the particular need for positive identification.

The characteristics of the criminal committing identity fraud must also be taken into consideration. Since the criminal in an organized enterprise can possess significant intelligence, resourcefulness, adaptability and mobility, the contemplated solution must account for these traits. It must be a process that is not easily discernable, can be changed quickly and often and it must account for the international criminal, who knows no boundaries and respects no borders.

In summary, any proposed solution must meet established standards in proving that it can work effectively in a particular identification environment and respond appropriately to the characteristics of the prospective identity fraud. Such standards or tests will inevitably change from environment to environment, depending on the level of risk involved.

These tests, or studies, need to be conducted quickly, efficiently, and fairly. Because of the broad scope of the identity fraud problem, the studies should be supervised by the federal government, and conducted by a task force compromised of all interested parties in both the public and private sectors. The task force should consider all of the factors bearing upon the identity fraud problem and the prospective solutions, including the following:

(1.) All critical identification environments, including passport and visa issuance; drivers' license issuance; birth and death certificates; etc.

(2.) The effectiveness of all proposed solutions for particular identification environments;

(3.) The established ability of the solutions to satisfy the factors of time and integration;

(4.) The characteristics of the identity fraud criminal, including his resources, adaptability and global mobility;

(5.) The cost of implementation of any such solution, using a cost benefit means of analysis; and

(6.) The social impact of any solution, including its effect on the privacy of individuals.

CONCLUSION

Identity theft, the taking of a person's identity for the purpose of committing a criminal act, is a serious concern as it violates the individual victim and wreaks huge financial losses on the commercial victim. However, the crime of using false identifiers and false identification documents transcends identity theft, as it includes not only the identity thief, but also the drug

trafficker, the alien smuggler and the terrorist. One who commits this crime of identity fraud needs to be culled out and prevented through new, innovative and effective solutions.

Borrowing from the academic science of human identification, we have provided a framework for devising appropriate solutions. These solutions, we submit, can only be derived through the earnest efforts of all interested parties, through a task force organized under the auspices of the federal government.

---

[1] United States v. Zacarias Moussaoui, U.S.D.C., E.D. Va., Dec. 2001 term, Indictment, Paragraphs 104-107.
[2] Id. Paragraphs 104-105.
[3] Id. Paragraph 104.
[4] Id. Paragraph 105.
[5] United States v. Kenys A. Galicia, U.S.D.C. E.D. Va., Oct. 2001 term, Indictment, Paragraphs 7,8.
[6] Id. Paragraphs 7,8.
[7] Krim, Jonathan and O'Harrow, Robert Jr., "National ID Cards Gaining Support," Washington Post, December 17, 2001.
[8] See Galicia Indictment, supra, note 5, paragraph 9.
[9] See Krim article, supra, note 7.
[10] Id. See also, Bulkeley, William M., "Hijackers Deeds Highlight Issue of Rampant Fade Ids in the U.S.," Wall Street Journal, September 26, 2001; "Asset Freezes Against Terrorism Has Weak Track Records," Dow Jones Newswires, September 26, 2001; "New Terror Probe Suspect Arrested, But Doubts Grow Over Hijackers Identities," AFP, September 21, 2001; Shaw, E. Clay Jr., prepared remarks before the Committee on Ways and Means, Subcommittee on Social Security and Committee on Financial Services Subcommittee on Oversight and Investigations, hearing on "Preventing Identity Theft by Terrorists and Criminals," November 8, 2001, p. 1; Kelly, Sue W., prepared remarks before the Committee on Ways and Means, Subcommittee on Social Security and Committee on Financial Services Subcommittee on Oversight and Investigations, hearing on "Preventing Identity Theft by Terrorists and Criminals," November 8, 2001, p. 1.
[11] See Krim article, supra, note 7.
[12] Id.
[13] Id.
[14] Identity Theft and Assumption Deterrence Act, Public Law 105-318, 112 STAT. 3010, October 30, 1998, codified at 18 U.S.C. § 1028 (1999).
[15] 18 U.S.C. § 1028(a)(7).
[16] Id.

[17] General Accounting Office, "Identity Fraud: Information on Prevalence, Cost and Internet Impact is Limited," May, 1998, p. 41 (GAO/GCD-98-100BR) (stating that a Trans Union official categorizes an incident where someone assumes a "true" identity as "true person fraud").
[18] Identity Theft and Assumption Deterrence Act, S. Rep. No. 105-274, at 6 (1998) (noting that the Federal Trade Commission Testified that the identity theft victims "suffer real harm" with the effect of the theft being "significant and long-lasting").
[19] See GAO Report, supra, note 17, p. 29.
[20] See S. Rep. No. 105-274, supra, note 18, at 7.
[21] See GAO Report, supra, note 17, p. 44.
[22] Id. P. 28.
[23] In December 2000, the National Fraud Center directed the development of "The Growing Global Threat of Economic and Cyber Crime," (www.lexisnexis.com/risksolutions/conference/docs/cyber.pbf.), a report co-authored by Dr. Gary R. Gordon and Dr. George E. Curtis. In the report at page 9, we estimated identity theft losses at $50 billion per year. We admit that this estimate is a rough approximation but we believe that it is on the conservative side.
[24] "Worker Charged With Stealing Outdated Driver Licenses," MSNBC.com, December 13, 2001.
[25] Id.
[26] Keeshan, Charles, "Carrying a False ID isn't Just a Kiddie Game," Daily Herald, November 5, 2001.
[27] Id.
[28] Branton, John, "Raid on Identity Theft Ring Also Nets Drugs, Explosives," pdxguide.com, December 7, 2001.
[29] See GAO Report, supra, note 17, p. 29.
[30] Id. p. 17.
[31] At the National Fraud Center, our research into the classification of crime enabled us to identify 27 different crimes, listed in Appendix A, that are frequently committed through the use of identity fraud.
[32] Lormel, Dennis M., prepared remarks before the House Committee on Financial Services, hearing on "Dismantling the Financial Infrastructure of Global Terrorism," October 3, 2001, p. 6.
[33] Id. p. 6.
[34] Id. p. 6.
[35] See GAO Report, supra, note 17, p. 34.
[36] Byers, Stephanie, "Note: The Internet: Privacy Lost, Identities Stolen," 40 Brandeis L.J. 141, 143, Fall 2001. (citing Givens, Beth, "Identity Theft: How it Happens, Its Impact on Victims, and Legislative Solutions (visited Jul. 21, 2000) http://www.privacyrights.org/AR/idtheft.htm)).
[37] Sullivan, Bob, "Russian Linked to Massive ATM Fraud," MSNBC.com, November 29, 2001; "Forensic Detectives; Cybercops. Digital Sleuths," Computerworld, January 14, 2002.
[38] See, GAO Report, supra, note 17, p. 35.
[39] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Public Law 107-45, 115 STAT. 272, October 26, 2001.
[40] Kirkpatrick, Michael D., prepared remarks before the United States Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism and Government Information, hearing on

"How New Technologies (Biometrics) Can be Used to Prevent Terrorism," November 24, 2001, p. 3.

[41] Lau, Joanna, prepared remarks before the United States Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism and Government Information, hearing on "Biometric Identifiers and the Modern Fact of Terror: New Technologies in the Global War on Terrorism," November 24, 2001, p. 2.

[42] Huddart, Martin, prepared remarks before the United States Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism and Government Information, hearing on "Biometric Identifiers and the Modern Fact of Terror: New Technologies in the Global War on Terrorism," November 24, 2001, p. 1.

[43] Dershowitz, Alan M., "Why Fear National ID Cards?" New York Times, October 13, 2001; McCollum, Bill, prepared remarks before the United States House of Representatives Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations Committee on Government Reform, hearing on "Does America Need a National Identifier?" November 16, 2001, p. 4.

[44] See generally, Corrigan, Katie, prepared remarks before the United States House of Representatives Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations Committee on Government Reform, hearing on "Does America Need a National Identifier?" November 16, 2001.

[45] Id. p. 3.

[46] LoPucki, Lynn M., "Article: Human Identification Theory and the Identity Theft Problem," 80 Tex. L. Rev. 89, 95 (Nov. 2001).

[47] Clarke, Roger, "Human Identification in Information Systems: Management Challenges and Public Policy Issues," Info. Tech & People, Dec. 1994.

[48] Id. at 6,8.

[49] See, LoPucki, supra, note 46, at 95.

[50] Id. at 95-96.

[51] Id. at 96.

[52] In our previous papers, "Identity Theft: Authentication As A Solution," and "Identity Theft: Authentication As A Solution – Revisited," we explained that "authentication," as we use that term, means the process by which an identity verifier uses information provided by the individual, that pertains to the individual, in order to confirm that the individual is who he or she says they are.

[53] O'Harrow, Robert, "Intricate Screening of Fliers in Works," Washington Post, February 1, 2002; McCartney, Scott, "A 'Trusted Traveler' Pass May Be Required In the Cards for Frequent Fliers," Wall Street Journal, January 30, 2002.

[54] Mr. Willox described First USA's successful application of a knowledge-based authentication solution in his presentation at the Federal Trade Commission's Identity Theft Victims Assistance Workshop, October 24, 2000. (www.ftc.gov/bcp/workshops/idtheft/transcripts/001024-tech.htm).

THE IDENTITY THEFT PENALTY ENHANCEMENT ACT

TUESDAY, JULY 9, 2002

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY,
TERRORISM, AND GOVERNMENT INFORMATION,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:35 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Dianne Feinstein (chairman of the subcommittee) presiding.

Also present: Senators Feinstein and Kyl.

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

Chairperson FEINSTEIN. I would like to begin this hearing in the interest of time. I know Senator Kyl is on his way and will be here shortly. Today's hearing is on the Identity Theft Penalty Enhancement Act of 2002. I introduced this legislation in May with the ranking member, Senator Kyl, and Senators Sessions and Grassley, at the request of the Attorney General and the Bush administration. And I am very pleased to have been asked to do this.

Unfortunately, because of the proliferation of identity theft and its use in other crimes, some extraordinarily serious, the enhancement penalties have become, I think, necessary and important.

For me, combating identity theft has been a top priority, and I have worked closely in this committee with Senator Kyl both to crack down on identity thieves and make such crimes much more difficult to commit.

This legislation, we believe, will make it easier for prosecutors to target those identity thieves who steal an identity for the purpose of committing other serious crimes, including murder and terrorism. Identity theft, in fact, is often a precursor to other serious crimes, and I would like to give just a few examples.

Lotfi Raissi, the 27-year-old Algerian pilot from London who was believed to have trained four of the September 11th suicide hijackers, was identified in British court papers as having used the Social Security number of Dorothy Hanson, a retired factory worker from New Jersey who died in 1991.

The Justice Department recently prosecuted an Algerian national for stealing the identities of 21 members of a health club in Cambridge, Massachusetts, and subsequently transferring those identities to an individual convicted in the failed plot to bomb Los Angeles International Airport in 1999.

An administrator of Kmart Corporation's stock option plan is currently being prosecuted for stealing the identity of a Kmart executive and exercising 176,000 options in his name.

And, in another case, a Chicago man allegedly killed a homeless man to assume the victim's identity and avoid pending criminal charges for counterfeiting.

So here we have examples involving terrorism, involving murder, and involving major fraud, and identity theft became the enabler for these crimes. And the stories go on and on, and that is what makes this legislation so vital.

Now, what would the bill do? The bill would create a separate crime of aggravate identity theft for any person who uses the identity of another to commit certain serious Federal crimes. Specifically, the legislation would provide for an additional 2-year penalty for any individual convicted of committing one of the following serious Federal crimes by using the identity of another person, and the crimes are: illegally obtaining citizenship in the United States; obtaining a passport or visa; committing, bank, wire, or mail fraud; or stealing from employee pension funds; and then committing a variety of other serious Federal crimes, all of them felonies.

Secondly, the legislation would provide for an additional 5-year penalty for any individual who uses the stolen identity of another person to commit any one of the enumerated Federal terrorism crimes found in Title 18. These include: destruction of an aircraft; assassination or kidnapping of high-level Federal officials; bombings; hostage taking; and provide material support to terrorist organizations.

Thirdly, the bill also strengthens the ability of law enforcement to go after identity thieves and prove their case by allowing law enforcement to target individuals who possess the identity documents of another person with the intent to commit a crime. Current Federal law prohibits the transfer or use of false identity documents, but it doesn't specifically ban the possession of those documents with the intent to commit a crime. And, finally, increasing the maximum penalty for identity theft under current law from 3 to 5 years.

The bill also clarifies that the current 25-year maximum sentence for identity theft in facilitation of international terrorism also applies to domestic terrorism.

Now, I don't think I need to go into the background of identity theft. I think we have had a number of hearings in this subcommittee. We know that the average loss of an identity theft is now about $17,000. We know that fraud losses at individual financial institutions are running well over $1 billion annually. And, on an average, it takes a full year and a half for someone who has had their identity stolen to regain it.

So we have a very impressive panel today, and I will interrupt the testimony when Senator Kyl does come to receive his comments. But in the interim we will proceed, and the first one I would like to introduce is Mr. Dan Collins. Mr. Collins is currently the Chief Privacy Officer and Associate Deputy Attorney General at the Department of Justice. He previously worked as a partner at the Los Angeles firm of Munger, Tolles & Olson. From 1992 to 1996, he served as Assistant U.S. Attorney in the Office of the U.S.

Attorney in Los Angeles. He received his law degree from a great school, Stanford, in 1988, and he clerked for Supreme Court Justice Scalia.

If we could proceed with you, Mr. Collins, and then I will introduce the others seriatim.

STATEMENT OF DANIEL P. COLLINS, ASSOCIATE DEPUTY ATTORNEY GENERAL AND CHIEF PRIVACY OFFICER, U.S. DEPARTMENT OF JUSTICE

Mr. COLLINS. Thank you, Senator Feinstein. It is my pleasure to be here today to testify on behalf of the Justice Department in strong support of this legislation. As you have remarked, the bill that is now before the subcommittee was first unveiled at a joint press conference held by the Attorney General and Senator Feinstein on May 2nd, at which the Attorney General also announced a major nationwide crackdown that has resulted in the prosecution of scores of identity thieves. On behalf of the Attorney General, I wish to reiterate his sincere appreciation for the invaluable leadership you have shown on this important issue.

Identity theft is one of the fastest-growing crimes in the United States. No matter how you look at it, the numbers are very troubling. Estimates of one organization are that between 500,000 and 700,000 persons are victims of this crime every year. One organization estimates that the number may be as high as 1.1 million.

Criminals steal other person's identities in order to facilitate the commission of a wide range of serious underlying offenses that range from credit card fraud, bank fraud, fraudulent loans, thefts of benefits, even murder. Identity theft has also been used, as you have noted, in connection with planned terrorist activities.

In 1998, Congress enacted important legislation prohibiting a wide variety of identity theft offenses. The Department has vigorously enforced these laws as evidenced by the nationwide sweep announced by the Attorney General on May the 2nd. That sweep resulted in 73 criminal prosecutions against 134 individuals in 24 judicial districts from coast to coast. The underlying criminal violations involved in those cases ran the gamut, again, from credit card fraud to theft of employee benefits, to murder. These cases were the result of close and ongoing cooperation among Federal, State, and local law enforcement agencies, including the Federal Trade Commission, the Secret Service, the Postal Inspection Service, the Federal Bureau of Investigation, the Office of the Inspector General of the Social Security Administration, and the IRS Criminal Investigative Division, as well as State and local law enforcement agencies.

The second initiative announced by the Attorney General and yourself, Senator Feinstein, at the May 2nd press conference was the bill that has become S. 2541. That legislation has a number of important aspects.

First, the bill defines a new crime of aggravated identity theft that includes the most serious and harmful forms of this pernicious practice—and, again, working from the concept that people don't steal other person's identities for the sheer thrill of impersonation. They steal it to commit another crime. The bill takes cognizance of the fact that there usually is an underlying predicate felony. It

identifies the most serious forms of it and then says that if you commit that crime with someone else's identity, you will be charged with a separate crime and sentenced separately with an enhanced consecutive penalty for that. It will be a 2-year penalty for the general list of offenses that are established there and a 5-year penalty on top of the already severe underlying penalty for any terrorism offense.

In addition, the legislation makes a number of changes that improve and strengthen the usefulness of the 1998 legislation. In particular, the bill closes several gaps that have been identified in the 1998 law. As you have noted, it will cover possession and not just transfer and use of these documents, and it will also increase the maximum penalties for simple identity theft from 3 to 5 years. And then, building on the changes made by the PATRIOT Act, which now has a definition of domestic terrorism, the 25-year maximum for terrorism-related offenses now incorporates that definition so that it is now domestic and international terrorism.

These changes are important measures to make sure that prosecutors have the full range of tools available in order to combat this offense and to make sure that when Federal resources are deployed as part of the effort against this growing crime, that prosecutors are able to bring cases expeditiously, efficiently, and receive appropriate severe sentences for those serious crimes.

[The prepared statement of Mr. Collins follows:]

TESTIMONY OF DANIEL P. COLLINS, ASSOCIATE DEPUTY ATTORNEY GENERAL AND CHIEF PRIVACY OFFICER, DEPARTMENT OF JUSTICE

Chairman Feinstein, Senator Kyl, and distinguished members of the Subcommittee, I am pleased to testify on behalf of the Justice Department in strong support of this important legislation. The bill now before you was first unveiled at a joint press conference held by the Attorney General and Chairman Feinstein on May 2nd, at which the Attorney General also announced a major, nationwide crackdown that has resulted in the prosecution of scores of identity thieves. On behalf of the Attorney General, I wish to reiterate his sincere appreciation for the invaluable leadership you have shown on this important issue.

Identity theft is one of the fastest growing crimes in the United States today. The numbers tell the story. The Privacy Rights Clearinghouse estimates that between 500,000 and 700,000 people each year become victims of identity theft. Indeed, the Identity Theft Resource Center estimates that the number may be as high as 1.1 million. The Federal Trade Commission (FTC) recently reported that a whopping 42% of all of the consumer complaints it receives involve incidents of identity theft. Each week, the FTC receives an average of 3,000 calls on its ID theft telephone hotline, and another 400 complaints of identity theft over the Internet. Additional data recently gathered by the General Accounting Office (GAO) paint a similar picture. In response to a request made by the Chair and the Ranking Member of this Subcommittee—Senator Feinstein and Senator Kyl—as well as by Senator Grassley, the Government Accounting Office completed a report in March of this year in which it concluded that all available sources of information confirm that "the prevalence of identity theft is growing" and that the monetary losses to industry from identity theft continue to mount.

Numbers, however, do not tell the whole story. Identity theft inflicts substantial damage, not only on the economy, but also on hardworking Americans, who must expend the effort to undo the damage done to their credit records and their good names.

In order to respond to this growing problem, the Attorney General announced on May 2nd a two-prong initiative to combat identity theft. The first prong is a coordinated, nationwide "sweep" to prosecute cases involving identity theft. This sweep resulted in 73 criminal prosecutions against 134 individuals in 24 judicial districts. The underlying criminal violations involved in these cases run the gamut from credit card fraud to theft of employee benefits to murder. These cases were the result of the close and ongoing cooperation among federal, state, and local law enforcement

agencies, including the Federal Trade Commission (FTC), the Secret Service, the Postal Inspection Service, the FBI, the Office of the Inspector General of the Social Security Administration, the IRS's Criminal Investigation Division, as well as a range of state and local agencies. Acting through its Identity Theft Subcommittee, the Attorney General's White Collar Crime Council has worked hard to coordinate enforcement efforts in this area. The FTC, working with the Secret Service, has provided invaluable assistance in developing an identity theft case referral program that helps in identifying significant cases that warrant further investigation.

The second prong of the initiative announced on May 2nd is the development of new legislation to enhance significantly the penalties for identity theft. The Attorney General and Chairman Feinstein at that time jointly announced the outline of the legislation that is before you today. S. 2541, the "Identity Theft Penalty Enforcement Act," would greatly help to ensure that the Department has the tools it needs to prosecute effectively, and punish appropriately, the most serious forms of identity theft.

S. 2541 builds upon, and strengthens, the important identity theft legislation enacted by the Congress in 1998. The current federal identity theft statute (18 U.S.C. § 1028(a)(7)) makes it unlawful to "knowingly transfer[] or use[], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law," if the identification document in question was, or appears to be, issued by the United States or the offense involved the use of the mails or affected interstate or foreign commerce. The existing statute has a sweeping substantive breadth that reaches all identity thefts that have a federal interest—even those involving State law felonies. This breadth makes it a valuable part of the federal criminal code and an important part of the federal arsenal against crime. However, precisely because of its breadth, the existing statute groups a large and disparate class of behavior into a single category. For the same reason, it also imposes across-the-board proof requirements that may not make sense in certain cases.

Section 2 of S. 2541 addresses these concerns by proposing a new section 1028A to the criminal code. Section 1028A would define a class of "aggravated identity theft" that includes the most serious and harmful forms of this pernicious practice. The penalties for this newly defined crime of "aggravated identity theft" are significantly enhanced as compared to existing law, and the proof requirements are simplified.

In defining "aggravated identity theft," section 1028A—like the existing statute—uses the concept of predicate offenses. That is, identity theft generally is not committed for the sheer thrill of impersonation; it is almost always done for the purpose of committing *another* state or federal offense. Under S. 2541, the "aggravated" forms of identity theft are defined by the nature of the predicate offense, and include all of the most frequently occurring and most serious predicate offenses. *See* proposed section 1028A(a)(2), (c). Thus, anyone who uses another person's identity to commit one of the enumerated serious predicate offenses will be guilty of "aggravated identity theft." Because virtually all of the most serious forms of identity theft involve predicate criminal activity (*e.g.,* bank fraud, wire fraud, mail fraud) that is covered by *federal* law, S. 2541 does not include any State law predicate crimes in its definition of "aggravated identity theft." Compared to the general federal identity theft statute, S. 2541 applies to a focused and narrower set of predicate offenses.

In prescribing the penalties for this new offense, S. 2541 does not rely upon the Sentencing Commission or the Sentencing Guidelines. This approach is the most sensible one in light of the unusual fact that identity theft is an entirely *derivative* offense. That is, as explained above, identity theft is virtually always committed in connection with the commission of another offense. The Sentencing Guidelines, however, are generally designed and intended to be "charge-neutral:" the sentence depends on the underlying "relevant conduct" and not on the particular offense charged in the indictment. Thus, the Guidelines will generally ignore the fact that two offenses have been charged (a derivative offense and a predicate offense); the same sentence would be imposed in such a case as would be imposed even if only the predicate offense had been charged. Consequently, application of the Guidelines would mean that there would be virtually no practical advantage to charging the derivative criminal offense. Prosecutors would have to charge more and prove more without obtaining any additional punishment.

S. 2541 avoids this problem by fashioning a penalty scheme for the derivative offense of aggravated identity theft by relying upon the existing model that the criminal code itself provides for another wholly derivative offense: 18 U.S.C. § 924(c), Section 924(c) makes it a federal offense to use or carry a firearm "during or in relation to" a crime of violence or a drug trafficking crime. Because an underlying predicate

crime must be proved—either a crime of violence or a drug trafficking crime—application of the guidelines would have collapsed the sentencing for the § 924(c) offense together with the underlying predicate offense. Section § 924(c) avoids this by instead providing for an *additional* prescribed term of imprisonment over and above that imposed on the underlying offense. Because "aggravated identity theft" is, like § 924(c), an unusual derivative offense, a similar approach makes sense here.

Accordingly, S. 2541 provides that, if a person commits aggravated identity theft by stealing someone's identity in order to commit a serious federal predicate offense, that person will be sentenced to an additional two years' imprisonment over and above the sentence for the underlying offense. *See* proposed section 1028A(a)(1), (b)(2). If the predicate offense is a terrorism offense, the additional punishment is increased to five years. *See* proposed section 1028A(a)(2), (b)(2). S. 2541, however, properly departs from the § 924(c) model in one critical respect. The Supreme Court has held that multiple counts under § 924(c) that are charged in the same indictment must run consecutively to each other. *Deal v. United States,* 508 U.S. 129 (1993). This mandatory cumulative stacking of sentences, if applied here, could result in unduly severe and inflexible sentences. S. 2541 thus leaves it to the discretion of the sentencing judge whether to run consecutively or concurrently any multiple counts of aggravated identity theft that are sentenced at the same time. *See* proposed section 1028A(b)(4). In order to avoid unwarranted disparities in the excuse of this discretion, the Sentencing Commission is explicitly authorized to issue guidance concerning whether and to what extent such multiple sentences would be concurrent or consecutive. *Id.*

S. 2541 would also substantially simplify the proof requirements for "aggravated identity theft." The existing identity theft statute contains multiple mental-state elements. In addition to proving all of the elements of the predicate crime (including the scienter element), prosecutors also must establish that the defendant "knowingly" transferred or used the information "with the intent to commit" a federal or state crime. S. 2541 would streamline the proof by requiring proof of only that level of scienter that is already required by the underlying predicate offense and the knowing use of another's identity. Moreover, because "aggravated identity theft" is defined with reference only to *federal* predicate offenses, there is no need for any additional proof of a federal jurisdictional connection. Accordingly, the additional federal jurisdictional showing required under § 1028(a)(7) is properly not carried over into this new offense.

This new offense defined by section 2, with its streamlined proof requirements and its enhanced penalty structure, will provide invaluable assistance to the Department in ensuring that significant identity theft crimes can be effectively prosecuted and properly punished.

In addition to enacting a new offense of "aggravated identity theft," S. 2541 strengthens the existing 1998 identity theft law in multiple ways. Section 3 of the bill closes several gaps in the coverage of the existing identity theft prohibition (18 U.S.C. § 1028(a)(7)) and increases the penalties for certain violations of that section.

As currently drafted, section 1028(a)(7) punishes anyone who "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet" any violation of Federal law or any State or local felony. This bill would amend this provision to prohibit, not just the "transfer or use" of someone else's identity information, but also the *possession* of such information with the requisite criminal intent.

The bill would also add language to this provision that would extend its coverage to those criminals who steal someone's identity "in connection with" another crime.

The bill also amends section 1028(a)(7) to increase from three to five years the maximum term of imprisonment for ordinary identity theft and for possession of false identification documents.

Lastly, section 3 of the bill would amend section 1028(b)(4) to impose a higher maximum penalty for identity theft used to facilitate acts of domestic terrorism. In doing so, section 3 builds upon the USA Patriot Act's new definition of "domestic terrorism" and authorizes a 25-year maximum penalty for identity theft committed to facilitate an act of domestic terrorism.

Let me again extend the Department's gratitude to Chairman Feinstein and Senator Kyl for your leadership on this issue and for your prompt action on this legislation. We strongly support this bill and urge its swift enactment.

That concludes my prepared remarks. At this time, I would be pleased to answer any questions you may have.

Chairperson FEINSTEIN. Thanks very much, Mr. Collins.

Next I am going to go to Dennis Lormel. He is the chief of the Financial Crimes Section of the FBI. Actually, it's chief of the Ter-

rorist Financial Operations Section in the Counterterrorism of the FBI—I will give you your full title—which has responsibility for tracking, investigating, and disrupting terrorist-related financial activity. Previously, Mr. Lormel served as the chief of the Financial Crimes Section in the Criminal Investigative Division at the FBI headquarters. He has been a special agent with the FBI for 26 years and has extensive experience with white-collar matters.

Mr. Lormel, welcome.

STATEMENT OF DENNIS M. LORMEL, CHIEF, TERRORIST FINANCIAL REVIEW GROUP, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, D.C.

Mr. LORMEL. Thank you, Senator, and like my colleagues, we appreciate the opportunity to participate today and applaud your efforts in this regard.

I have submitted a written statement for the record, and in addition to that, I would like to make some comments.

As the Senator pointed out, prior to September 11th I was the chief of the Financial Crimes Section of the FBI, and over time we had recognized the increased articulation of identity theft as a significant problem, and we participated in a number of forums involving business and different segments of the government and recognized that an initiative to address it was certainly warranted, and this legislation would really vastly aid that.

In that regard, just prior to September, we undertook an investigative initiative involving all of our field divisions to identify cases where identity theft played a collateral or important role in facilitating other crimes ranging through the whole white-collar gamut to include fugitives and other violent crimes where we have seen some problems. And, unfortunately, September 11th came and that particular project was held in abeyance. And since September, I have served in another capacity, as the chief now of the new section in the Terrorism Division, specifically addressing terrorist financing. And an area of concern to us is, as you pointed out with two of the anecdotes that you had, there is the use of identity theft and false identification in furtherance of terrorism, and that is certainly a big concern to us.

We traditionally have not in the Bureau tracked identity theft as a crime problem or as a classification. In August of last year, we initiated a program to try to monitor or identify cases where identity theft was an element, and in that regard, we have identified 954 investigations that are pending with elements of identity theft, which include 14 terrorism investigations.

Chairperson FEINSTEIN. Federal?

Mr. LORMEL. Yes, ma'am, 14 Federal FBI-led terrorism investigations are included in that amount, 6 of which are intelligence-driven and 8 of which are criminal in nature. And I think any one of those cases just heighten the significance and dramatize the importance of your legislation.

Also, as a follow-up to your comments, the 19 hijackers of the events of September 11th, it is important to recognize they did not use identity theft in furtherance of their activities, and that group is sort of an anomaly in terms of how terrorist groups generally work in that many of the cells that we have looked at or are cur-

rently investigating use the theft of identity to facilitate other crimes or, more importantly, to derive sources of funding for themselves. And an example of that is a cell we are looking at in Spain, in Madrid. That particular cell, which the Spanish authorities are working in conjunction with us, demonstrates how the theft of credit cards facilitates terrorist acts.

Yesterday, I met with representatives from Europol, and they were concerned that in the U.K., for instance, the identity theft involving credit cards, stolen credit cards, is a significant problem. And it is starting to permeate throughout the European Union. And in conjunction with that, there were a number of passports, a significant number of passports stolen in Brussels and, again, finding their way into terrorist circles. And one of our concerns is the obvious capability of the transient nature of some of these people to come to the U.S. using that type of identity and certainly the availability of the credit cards in furtherance of acts.

Here in the U.S. we have had demonstrated instances where stolen credit cards have been used, and particularly the use of telephone calling cards that have been stolen and used in false identities. We have had a number of instances—and, in fact, funding that the 19 hijackers did receive, the primary funds that were transferred to the U.S. were done using aliases and false identification from people facilitating their operations. So that was certainly another area of concern for us.

We have got an ongoing project right now involving stolen and the misuse of Social Security numbers, which is significant. As an example, early after September we established kind of a terrorism financial—terrorist—financing database, and from that database we ran a sampling of Social Security numbers. And we came up with over 400 Social Security numbers that appeared to be misused, and it included two individuals that were detained shortly after September, one of which was charged down in Austin, Texas, on the Amtrak train. Ayub Khan was one of them, and he had false identity that he has been charged with, and I believe convicted of, if I am not mistaken. Those are some examples of the problems we have encountered.

So, again, Senator, we thank you for your efforts, and that certainly will help provide deterrence that is sorely needed in this area.

[The prepared statement of Mr. Lormel follows:]

STATEMENT BY DENNIS M. LORMEL, CHIEF, TERRORIST FINANCIAL REVIEW GROUP, FEDERAL BUREAU OF INVESTIGATION

Good afternoon Madam Chairman and members of the Subcommittee on Technology, Terrorism and Government Information. On behalf of the Federal Bureau of Investigation (FBI), I would like to express my gratitude to the Subcommittee for affording us the opportunity to participate in this forum and to provide comment to the Subcommittee regarding the proposed legislation in S. 2541. The FBI is very supportive of this bill which enhances the penalties for convictions on certain felony violations where identify theft was used in relation to the offenses and adds some wording to Section 1028 of Title 18, United States Code.

As this Subcommittee is well aware, the FBI, along with other federal law enforcement agencies, investigates and prosecutes individuals who use the identities of others to carry out violations of federal criminal law. These violations include bank fraud, credit card fraud, wire fraud, mail fraud, money laundering, bankruptcy fraud, computer crimes, and fugitive cases. These crimes carried out using a stolen identity makes the investigation of the offenses much more complicated. The use of

stolen identity enhances the chances of success in the commission of almost all financial crimes. The stolen identity provides a cloak of anonymity for the subject while the groundwork is laid to carry out the crime. This includes the rental of mail drops, post office boxes, apartments, office space, vehicles, and storage lockers as well as the activation of pagers, cellular telephones, and various utility services.

Identity theft is not new to law enforcement. For decades fugitives have changed identities to avoid capture and check forgers have assumed the identity of others to negotiate stolen or counterfeit checks. What is new today is the pervasiveness of the problem. The Federal Bureau of Investigation does not view identity theft as a separate and distinct crime problem. Rather, it sees identity theft as a component of many types of crimes which we investigate.

Advances in computer hardware and software along with the growth of the Internet has significantly increased the role that identity theft plays in crime. For example, the skill and time needed to produce high-quality counterfeit documents has been reduced to the point that nearly anyone can be an expert. The same multimedia solfware used by professional graphic artists is now being used by criminals. Today's software allows novices to easily manipulate images and fonts, allowing them to produce high-quality counterfeit documents. The tremendous growth of the Internet and the accessibility it provides to such an immense audience coupled with the anonymity it allows results in otherwise traditional fraud schemes becoming magnified when the Internet is utilized as part of the scheme. This is particularly true with identity theft related crimes. Computer intrusions into the databases of credit card companies, financial institutions, on-line businesses, etc. to obtain credit card or other identification information for individuals have launched countless identity theft related crimes. This proposed legislation would act as a strong deterrent to not only those committing the initial intrusion, but to the vast potential users of that information who would utilize it to commit their own criminal fraud schemes.

The impact is greater than just the loss of money or property. As the victims of identity theft well know, it is a particularly invasive crime that causes immeasurable damage to the victim's good name and reputation in the community; damage that is not easily remedied. The threat is made graver by the fact that terrorists have long utilized identity theft as well as Social Security Number fraud to enable them to obtain such things as cover employment and access to secure locations. These and similar means can be utilized by terrorists to obtain Driver's Licenses, and bank and credit card accounts through which terrorism financing is facilitated. Terrorists and terrorist groups require funding to perpetrate their terrorist agendas. The methods used to finance terrorism range from the highly sophisticated to the most basic. There is virtually no financing method that has not at some level been exploited by these groups. Identity theft is a key catalyst fueling many of these methods.

For example, an Al-Qaeda terrorist cell in Spain used stolen credit cards in fictitious sales scams and for numerous other purchases for the cell. They kept purchases below amounts where identification would be presented. They also used stolen telephone and credit cards for communications back to Pakistan, Afghanistan, Lebanon, etc. Extensive use of false passports and travel documents was used to open bank accounts where money for the mujahadin movement was sent to and from countries such as Pakistan, Afghanistan, etc.

The FBI has implemented a number of initiatives to address the various fraud schemes being utilized by terrorists to fund their terrorist activities. One involves targeting fraud schemes being committed by loosely organized groups to conduct criminal activity with a nexus to terrorist financing. The FBI has identified a number of such groups made up of members of varying ethnic backgrounds which are engaged in widespread fraud activity. Members of these groups may not themselves be terrorists, but proceeds from their criminal fraud schemes have directly or indirectly been used to fund terrorist activity and/or terrorist groups. By way of example, the terrorist groups have siphoned off portions of proceeds being sent back to the country from which members of the particular group emigrated. We believe that targeting this type of activity and pursuing the links to terrorist financing will likely result in the identification and dismantlement of previously unknown terrorist cells. Prior to 9/11, this type of terrorist financing often avoided law enforcement scrutiny. No longer. The FBI will leave no stone unturned in our mission to cut off the financial lifeblood of terrorists.

Another initiative has been the development of a multi-phase data mining project that seeks to identify potential terrorist related individuals through Social Security Number misusage analysis. The FBI, through its Terrorist Financial Review Group, is taking SSNs identified through past or ongoing terrorism investigations and providing them to the Social Security Administration for authentification. Once the va-

lidity or non-validity of the number has been established, investigators look for misuse of the SSNs by checking immigration records, Department of Motor Vehicles records, and other military, government and fee-based data sources. Incidents of suspect SSN misusage are then separated according to type. Predicated investigative packages are then forwarded to the appropriate investigative and prosecutive entity for follow-up.

Given the alarming nature of the threat posed by identity theft and the potential nexus to terrorism, the FBI is grateful for the efforts of Congress and this Subcommittee in pursuing this legislation which will considerably aid law enforcement efforts to address the threat. Enhancing the penalties for identity theft makes it clear that identity theft is a serious crime with serious consequences. It will encourage law enforcement to more aggressively investigate this type of crime and for it to be prosecuted. All of which will likely serve as a deterrent and slow the growth rate of identity theft related crimes. Thank you.

Chairperson FEINSTEIN. Thank you very much, Mr. Lormel.

We have been joined by the distinguished ranking member, Senator Kyl, who is the cosponsor of this legislation.

Senator we have heard from Mr. Collins and Mr. Lormel. There is one more to go, but I would like, if you would like to make a statement——

Senator KYL. No, no. Please continue.

Chairperson FEINSTEIN. All right. I will proceed then and introduce Howard Beales III, the Director of the Bureau of Consumer Protection at the Federal Trade Commission. Mr. Beales began his career at the FTC in 1977 as an economist specializing in consumer protection problems, and now as director, he oversees the work of some 152 lawyers and a $77 million budget. His major areas of expertise and interest include law and economics and aspects of Government regulation of the economy.

Mr. Beales, welcome.

STATEMENT OF HOWARD BEALES, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. BEALES. Thank you, Madam Chairman and Senator Kyl. I really am pleased to be able to testify today and express the Commission's support for S. 2541, the Identity Theft Penalty Enhancement Act.

Every day, through our toll-free hotline and our online complaint form, we are able to advise hundreds of people on how to repair the damage to their credit and their reputations that is caused by identity theft. As you know, we also collect data from these consumers to share with law enforcement through our Consumer Sentinel Network. These data support the prosecution of ID theft by identifying suspects and helping to spot trends. Measures like S. 2541 that deter and punish those who would engage in identity theft thus serve our common goal of reducing this pernicious crime.

Our partners in law enforcement tell us that identity theft is often committed in furtherance of other crimes. This bill would enhance the penalties when identity theft is committed in furtherance of some of the most damaging and serious other crimes, including those that facilitate domestic terrorism. Specifically, the bill would impose greater penalties on defendants who commit identity theft in order to obtain a firearm, steal another employee's benefits, obtain documentation of citizenship, or commit mail, wire, or bank fraud, among other offenses.

The bill would also streamline proof requirements by including the possession of identifying information with intent to commit identity theft as an element of the crime.

These proposed improvements in the ID theft enforcement scheme will make identity theft cases easier to investigate and easier to prosecute successfully. Ultimately, the goal of the bill is to develop more fruitful prosecutions. We, too, are making efforts to encourage prosecutions under both Federal and State identity theft laws. In March, we launched a nationwide training program for investigating ID theft in cooperation with the Secret Service, the Department of Justice, and with support from the International Association of Chiefs of Police.

To date, we have trained more than 440 law enforcement officers from over 100 local, State, and Federal agencies. We have held sessions in D.C., Des Moines, Chicago, and San Francisco, and have an upcoming training session scheduled for Dallas in August.

The training includes presentations on how to use the Consumer Sentinel ID Theft Clearinghouse, the value of cooperative enforcement through regional task forces, and the ins and outs of both high-tech and traditional identity theft. We have been encouraged by the healthy turnout at the events and plan to follow up with a program to train the trainers, if you will. By reaching key officers, especially in areas with a high prevalence of identity theft, we hope to enable even more law enforcement agencies to join the fight against identity theft.

I would like to briefly address what our data indicate about some of the aggravated identity theft crimes that are the subject of S. 2541. In 2001, our clearinghouse received just over 86,000 identity theft complaints. The most common type of identity theft involved fraudulently obtained credit. Forty-two percent of the victims experienced this type of fraud. In most cases, this involves activity that could be charged as mail, bank, or wire fraud, depending on the facts of the particular case. Thus, the most common forms of theft would be targeted by the provisions of S. 2541.

One word of caution about this data. Because our clearinghouse is based mostly on self-reported data, it reflects what the victim knows. This may not fully reflect the prevalence of some of the predicate felonies under the bill. For example, credit fraud is often quickly apparent to the victims through contact by the card-issuing bank or evidence of fraudulent accounts on their credit reports.

That is not the case for other types of identity theft. For example, only 6 percent of the complaints we received in calendar year 2001 involved fraud with respect to Government documents or benefits, and less than 3 percent reflected falsely obtained driver's licenses. Does this mean there is not much Government document fraud? Well, probably not. It is simply less likely that the victim will learn about this type of fraud. Indeed, the victim may never become aware that someone obtained proof of citizenship or made a false statement to obtain a firearm in their name. However, these types of serious violations are often uncovered once investigators begin a more detailed review of the suspect's conduct.

We are encouraged to see the aggressive steps taken by our colleagues in criminal law enforcement to target ID theft. The FTC will continue to do all it can to assist law enforcement through our

training programs and through the use of our clearinghouse data. And we believe that the enhanced penalties envisioned by S. 2541 will increase the likelihood that those who exploit an innocent person's good name will receive appropriate punishment.

Thank you, Madam Chairman, and I will be happy to answer any questions.

[The prepared statement of Mr. Beales follows:]

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON THE IDENTITY THEFT PENALTY ENHANCEMENT ACT OF 2002

I. INTRODUCTION

Madam Chairman and members of the Committee, I am Howard Beales, Director of the Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on the importance of strengthening the tools available to law enforcement as a means to both prevent and deter the crime of identity theft.

In March of this year, I had the opportunity to testify before the Subcommittee on the serious consequences that can result from identity theft.[2] In that testimony, I described three main components of the FTC's identity theft program: our Identity Theft Data Clearinghouse (the "Clearinghouse"); our consumer education and assistance resources, including our toll-free hotline, website, and educational brochures; and our collaborative and outreach efforts with law enforcement and private industry. Today, I would like to focus on the various ways the FTC works with law enforcement in order to facilitate their investigation and prosecution of identity theft crimes, and to express the Commission's support for the Identity Theft Penalty Enhancement Act, which will help achieve that goal.

The FTC has committed significant resources to assisting law enforcement, and fully intends to continue to do so in the future. Investigation and prosecution not only stop the offender from destroying another person's financial well being, but can also deter would be identity thieves from committing the crime.

II. THE IDENTITY THEFT PENALTY ENHANCEMENT ACT—S. 2541

Since the enactment of the Identity Theft and Assumption Deterrence Act of 1998 ("Identity Theft Act")[3], we have learned more about how this pernicious crime works. Our colleagues in criminal law enforcement have seen how identity theft can further many types of financial fraud and even terrorism. The Identity Theft Penalty Enhancement Act, S. 2541, provides for enhanced charging and sentencing when identity theft occurs in connection with these other serious crimes. The Commission supports S. 2541 and its goal of increasing criminal penalties for the most damaging forms of identity theft.

The sentencing enhancements that S. 2541 envisions would, if enacted, step-up the penalties for the most serious forms of identity theft, and strengthen prosecutors' ability to bring these cases. In particular, the proposed legislation would define a new crime of "aggravated identity theft" that includes the most deleterious forms of identity theft, and which would carry greater penalties. Many of the predicate offenses that are included in the definition of "aggravated" identity theft, including identity theft for the purpose of defrauding employee benefit plans or committing bank fraud, have predictably serious consequences to both the individual and institutional victims of the crime. Each of these would carry a two-year consecutive enhancement to the sentence. Enhanced five-year consecutive penalties would result if a terrorist or terrorist-related offense is involved.

S. 2541 also streamlines proof requirements by including the possession of identifying information with intent to commit identity theft as an element of the crime. These provisions, together with the enhanced sentences for aggravated identity theft, will make identity theft cases easier to investigate and to prosecute successfully.

---

[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.

[2] See Testimony of J. Howard Beales, Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information (March 20, 2002).

[3] Pub. L. No. 105–318, 112 Stat. 3010 (1998).

III. THE COMPLAINT CLEARINGHOUSE

The Identity Theft Act directed the FTC to, among other things, log the complaints from victims of identity theft and refer those complaints to appropriate entities such as appropriate law enforcement agencies. Before launching our complaint system, the Commission took a number of steps to ensure that it would meet the needs of criminal law enforcement. For example, in April 1999, representatives from ten federal law enforcement agencies, five banking regulatory agencies, the US Sentencing Commission, the National Association of Attorneys General and the New York State Attorney General's Office met at the FTC to share their thoughts on what the FTC's complaint database and comprehensive consumer education booklet should contain. The roundtable participants also established a working group that provided feedback throughout the construction of the database. The FTC opened the consumer hotline and began adding complaints to the resulting Clearinghouse in November 1999. Law enforcement organizations nationwide who were members of our Consumer Sentinel Network (the FTC's universal fraud complaint database) gained access to the Clearinghouse via our secure Web site in July of 2000.

To ensure that the database operates as a national clearinghouse for complaints, the FTC has solicited complaint entry from other critical sources. For example, in November 2000, the International Association of Chiefs of Police (IACP) unanimously passed a resolution in support of curbing identity theft that, among other things, calls upon local police to refer identify theft victims to the FTC's hotline so that their complaints will be available to law enforcement officers nationwide through the Clearinghouse. In February 2001, the Social Security Administration Office of Inspector General (SSA–OIG) began providing the FTC complaints from its fraud hotline, significantly enriching our database. As a result of these efforts, the Clearinghouse has become a key element in identity theft investigations.

Many of the agencies that collaborated on the development of the Clearinghouse also participate in the Attorney General's White Collar Crime Task Force's Subcommittee on Identity Theft. Subcommittee members and other Consumer Sentinel users have told the FTC that the Clearinghouse is used primarily in two ways: to initiate new investigations, and even more often, to identify additional victims, suspects, addresses, phone numbers and criminal activities related to an ongoing investigation.

The Clearinghouse provides a much fuller picture of the nature, prevalence, and trends of identity theft than was previously available.[4] In 2000, our first full year of operation, we entered more than 31,000 consumer complaints into the database. In 2001, that number grew to 86,168. As of the end of May this year, only five months into the calendar year 55,000 complaints have already been added to the database. These numbers reflect complaints only, and do not include the tens of thousands of consumers who contacted us with questions on how to prevent identity theft or how to handle the loss or theft of a purse or wallet. This growth means that the Clearinghouse will continue to become a richer source of data for law enforcement, both in terms of developing and enhancing cases, and in providing information about the overall patterns and trends in identify theft.

Data from the Clearinghouse also assist law enforcement in other important ways. FTC data analysts aggregate the data to develop statistics about the nature and frequency of identity theft. Law enforcement and other policy makers at all levels of government use these reports to better understand the challenges identity theft presents. For instance, we publish the charts showing the prevalence of identity theft by states and by cities. The data also demonstrate general trends. The first twelve months of data revealed that over thirty-five percent of victims who called us reported that they had not been able to file police reports. Following the November 2000 IACP resolution that called upon local police to write reports for all incidents of identity theft, the number of victims who were unable to file a report fell by almost half to eighteen percent.

Since the inception of the Clearinghouse, forty-six separate federal agencies and three hundred and six different state and local agencies have signed up for access to the database. Among the agencies represented are over half the state Attorneys General as well as law enforcement from a number of major cities including Baltimore, Dallas, Los Angeles, Miami, San Francisco, and Philadelphia. We want to encourage even greater participation. To that end, since March of this year, we have been conducting outreach and law enforcement training and demonstrating the efficacy of the Clearinghouse at law enforcement conferences around the country. We have seen positive results from these efforts. For example, within three weeks after

[4] Attached are charts that summarize 2001 data from the Clearinghouse. These data are posted at *www.consumer.gov/idtheft* and *www.ftc.gov/sentinel*.

our training seminar in Chicago, held this May, approximately a third of the participating agencies without prior access to the Clearinghouse had signed up, and we continue to receive applications. As a core component of our program, we will continue to focus resources and to devise new methods for expanding law enforcement access to the database.

IV. PARTNERSHIP WITH THE SECRET SERVICE

The Clearinghouse is essentially a tool for criminal investigators and prosecutors. The US Postal Inspection Service,[5] the United States Secret Service (the "Secret Service") the SSA–OIG, the Department of Justice (DOJ), and the IACP, along with many other agencies, are outstanding partners in this effort, consistently communicating the availability and advantages of the Clearinghouse to their colleagues.

The Secret Service has made a particularly strong commitment to making the Clearinghouse the centralized investigatory tool for identity theft crimes nationwide. The Secret Service has just begun its second year of detailing a Special Agent to the FTC's identity theft program. This partnership has provided numerous benefits. In addition to the day-to-day assistance of an experienced law enforcement officer with expertise in investigating identity theft crimes, the Secret Service has also provided the FTC with access to powerful data mining and clustering software tools, the research capabilities provided by its financial crimes analysts, and its network of task forces throughout the country.

A. Investigative Referrals

The Clearinghouse, which now contains over 170,000 victim complaints, can be searched with more precision using the Secret Service's data mining and clustering software tools. Taking the results of a search, the Special Agent works with FTC staff to develop the most significant case leads into full investigative reports. As part of that effort, the Secret Service runs the leads through the additional intelligence databases it uses in its own criminal investigations. Since last June, we have been referring the investigative reports to Financial Crimes Task Forces or other appropriate law enforcement entities. In other instances, law enforcement agents from around the country directly contact the FTC with requests for an enhanced database search on a lead they currently have under investigation.

B. Law Enforcement Training

Recognizing that investigating identity theft often presents unique challenges, the FTC in conjunction with the Secret Service, DOJ, and IACP planned and directed training seminars for state and local law enforcement around the country in Washington, DC, Des Moines, Iowa, Chicago, Illinois, and in San Francisco. More than 440 people from over 100 different government departments and agencies have attended these seminars since we began them in March. Over three-quarters of the attendees were from state and local law enforcement and prosecuting authorities. An additional training program is planned for Dallas, Texas on August 14.

The training is designed to provide officers with technical skills and resources to enhance their efforts to combat identity theft. The training draws on the talent of local police and prosecutors, in addition to the core training staff from the FTC, DOJ and the Secret Service. While particular details may vary between venues, we stress two basic elements in the first half of the day: the value of Task Forces and the utility of the Clearinghouse to build and augment cases. The training also touches on the consumer educational and informational aspects of the FTC's identity theft program, because many law enforcement departments use our booklet, When Bad Things Happen To Your Good Name, as part of their victim assistance effort.

The training then moves to segments providing practical advice and demonstrating hands-on tools to help improve investigational strategies. In addition, presentations are geared towards familiarizing the attendees with the many different resources available to them from the federal, state and local government, and also from private industry, for investigating identity theft. Local prosecutors identify the key components they are looking for to bring successful identity theft actions. The feedback we have received has been very positive, and has enabled us to fine-tune each subsequent seminar.

---

[5] The Postal Inspection Service was the first agency to detail a law enforcement officer to work with the FTC's data sharing program. The Inspection Service detailed an inspector who, for over one year, managed our Consumer Sentinel system. These partnerships allow us to share expertise and also maintain open and ongoing communication.

V. CONCLUSION

The Commission supports S. 2541, the Identity Theft Penalty Enhancement Act of 2002, and embraces its goal of increasing the prosecution and criminal penalties when the identity theft facilitates particularly pernicious crimes. When these crimes are committed under someone else's identity, it stigmatizes an innocent person who must struggle to clear his or her name from association with an exceptionally horrific misdeed. It is only just that such a crime should carry an additional penalty. The FTC will continue to do its part to support the prevention, investigation, prosecution and mitigation of identity theft by providing law enforcement with education, training, access to the Clearinghouse, and case referrals.

Chairperson FEINSTEIN. Thank you very much. That completes our testimony.

Senator do you wish to make a statement?

STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator KYL. Yes, thank you, Madam Chair. I will simply say that it has been a pleasure to work with you in developing this legislation, and to make the point that we have all been increasingly frustrated by the fact that we have now acted twice, and this will be the third time we have affirmatively taken action to try to deal with this problem of identity theft and have dealt with it, and yet it continues apace. And until we are so serious about it that there is a real threat to the people that are committing it, it is going to continue. And that is why the enhanced penalties in here I think make a great deal of sense.

I am going to have a couple of questions that deal with the elements of it that I will ask when my turn comes here, but I thank the three of you for being here to help us understand what we need to do, and I really appreciate your commitment in helping to crack down on identity theft.

Thank you.

Senator FEINSTEIN. Thanks, Senator.

Mr. Collins, my first question is of you. According to the FTC, the average identity theft case reported to the clearinghouse involved about $8,000 in losses. That is average. However, many Federal prosecutors require a minimum theft amount of $25,000 before they will investigate a case. We have found this true in California, too.

Given that many identity theft crimes don't reach that threshold, what recommendations would you have to encourage Federal prosecution in these cases? I think that would go a long way to sending a clear signal.

Mr. COLLINS. Well, I think there are two points to make in that regard, and one relates specifically to the legislation. But before I get to that, first, the Attorney General and working through the Attorney General's Subcommittee on Identity Theft, which is an interagency task force that works as a coordinating clearinghouse for State and local task forces and other organizations, has worked throughout the country to get information out to make available the FTC Consumer Sentinel, to make people aware of that resource, and they are engaged in activities to educate U.S. Attorney's Offices about the importance of this crime.

For example, last fall, in October, they sent a package of materials to every U.S. Attorney's Office in the country with a model indictment and model jury instructions on the existing law.

The Attorney General has also by his actions in May indicated that this is a priority for the Department and is of importance. So I think that that message is getting out there. We have had receptivity from the U.S. Attorney's Offices.

Now, clearly, given the kinds of numbers of victims that we have mentioned and that have appeared in both the GAO studies, the FTC reports, you are talking about a very large number of victims. Now, clearly, that is a number of cases that could not be handled by Federal law enforcement alone. They have to work in partnership with coordinating activities with State and local task forces, and they are doing that.

But when a case is taken federally, it is important that it be one where the penalty is going to be commensurate with the fact that it warrants Federal resources, and that is where this legislation comes in, because this says, if a case is going to be taken federally, if you are committing a serious Federal felony and stealing someone's identity in doing it, you are going to get a sufficiently severe sentence. You are going to get this penalty you would have gotten under the underlying predicate crime plus 2 years, mandatory, no fiddling with the underlying sentence to offset it, 2 years tacked right onto it.

That is a substantial uptick if you look at the Sentencing Guidelines and how they score white-collar offenses.

Chairperson FEINSTEIN. Let me be more precise. I question an office having a $25,000 threshold. I don't know what Mr. Raissi in Great Britain—the level of his theft, but it could well be under $25,000. And so it seems to me that really a theft level isn't appropriate, but the magnitude of the kind of crimes that surround it might be better taken.

Mr. COLLINS. Well, my experience when I was an AUSA in Los Angeles is that the approach to guidelines, the smart approach to guidelines, is to use it as a guide and not as an inflexible rule.

Chairperson FEINSTEIN. Is it today a guideline, $25,000?

Mr. COLLINS. I don't know—different districts have different judgments as to when they think a case should or should not be taken federally. My experience was that we used guidelines to tell us when a case was likely to warrant Federal attention. If it was below the guidelines but there were other countervailing Federal interests that warranted taking that case, that was something that we would look at.

That is the kind of approach. Obviously, if someone is committing serious identity fraud in connection with what may be some serious terrorist activity, some other thing where there is a clear Federal interest, the fact that it is below a particular dollar amount should not cause someone to decline what would otherwise be an appropriate Federal case.

Senator FEINSTEIN. One last quick question, and then I want to turn to Senator Kyl, on the possession language. I think I mentioned that current law prohibits the transfer of false identity documents, but doesn't specifically ban the possession. And our bill would prohibit possession of these documents so that if a law en-

forcement officer were to discover a stash of false identity documents and can prove that the individual who possesses those documents intended to use them for, let's say, a terrorist act, that individual would be subject to prosecution simply for possession.

To what extent has the lack of a penalty for possession up to this point been a problem?

Mr. COLLINS. It takes away flexibility, Senator, under 1028(a)(3), if you had possession of five or more identification documents, which is much more narrowly defined than "means of identification," which was the key term that was inserted in the 1998 legislation that enacted the current ID theft provision at 1028(a)(7); (a)(7), though, only says transfer or use. So you get the broader definition of means of identification, and now with S. 2541, you would have possession. That gives you the flexibility. It adds another arrow to the quiver, that if there is a serious case where this is an element of the criminal conduct, that that is something that you can now charge. And when we were sort of assessing, looking at where there were gaps and consulting with the identity theft task force to see where we were getting feedback that there were areas that could be covered, this was identified as one area where there could be supplementation made to the 1998 legislation to strengthen it and give additional flexibility to prosecutors.

Chairperson FEINSTEIN. Now I am more confused because I have the actual statute. 1028(a)(4) says "knowingly possesses an identification document (other than one issued lawfully for the use of the possessor) with the intent such document be used to defraud the United States." I guess what we are doing here is we are broadening it.

Mr. COLLINS. The current provision has sort of a patchwork. Possession is only covered in limited cases.

Chairperson FEINSTEIN. Right.

Mr. COLLINS. It is covered if it is Government fraud. It is covered if it is five or more. What your legislation would do is say it is covered, period, and that is really where we should be.

Chairperson FEINSTEIN. Right.

Mr. COLLINS. Provided there is an appropriate Federal jurisdictional nexus. That is already in the existing law and is incorporated.

Chairperson FEINSTEIN. I understand. Thank you.

Senator Kyl.

Mr. LORMEL. Excuse me, Senator?

Chairperson FEINSTEIN. Yes, please.

Mr. LORMEL. May I make an observation? Since September, we have found that the U.S. Attorney's Offices have been much more flexible so the timing of your legislation is tremendous because it certainly does add additional backing to prosecutors. But, clearly, where these cases were really never addressed because of resource constraints, the U.S. Attorney's Offices have been much more sensitive to them.

Chairperson FEINSTEIN. I am delighted to hear that. I think that is extraordinarily important because prior to that, I know we were having troubles, particularly in California, getting some of this addressed. So I am delighted to hear it.

Senator Kyl.

Senator KYL. Thank you, Senator Feinstein, and the reason for that, I presume, is because of the degree to which this kind of crime is being used in connection terrorism, as you pointed out in your testimony.

Mr. LORMEL. Yes. In part, Senator, Yes.

Senator KYL. One of my two areas of inquiry is a direct follow-up on Senator Feinstein's question regarding possession. This is a little bit like the cell phone cloning bill that we did several years ago where there was absolutely no legitimate purpose for having a cloned—the equipment to make a cloned cell phone. Unless you were the phone company, you were a crook if you had it. And so you didn't have to use it. All we had to do is find it in your possession, and we did that, and it has worked out, I think.

Here it is the same thing, is it not? You have got in your possession these falsified documents which serve no earthly purpose except to then commit a fraud if you sell them to somebody and then that person commits the fraud directly. So I think that is the rationale for this.

My question here goes directly to whether or not there are instances, cases, and I will ask you, Mr. Collins, where had you had this broader definition of mere possession rather than transfer or sale, you could have made the case or solved the crime or charged the person, whereas with the existing statute it just wasn't possible to do that. Are there actually cases where that is so?

Mr. COLLINS. I am sure that there have been. I don't have cases at my fingertips that fell in this particular crack, but I know that when we were looking at the issue of identity theft and where there were gaps in the law, this was one that was reported back that, look, we really should have the flexibility to be able to charge a possession, so long as we can show the requisite intent and that is preserved. But that should really be part of the package of tools that are available, but I don't have a particular case at this moment.

Senator KYL. Okay. Well, just on to the point that somebody might raise that we are just being too liberal here in the expansion of language that you merely have to possess rather than actually transfer the documents, what would your response to that be as a practical matter with respect to the state of mind of the individual and the potential for the commission of a crime?

Mr. COLLINS. There are a variety of other offenses in other contexts, for example, in the Immigration and Nationality Act, where there is regulation of possession of false documents already. Why the particular limitations that we see in 1028(a) are there, that it is covered here a little bit and there a little bit, I am not quite sure.

But the direct answer is that we still have to prove under the law as amended by S. 2541 that they possessed the identification with the intent to commit or to aid or abet any unlawful activity that constitutes a violation of Federal law or a felony under State law. So this is not someone who is saving the, you know, driver's license of their late mother as a memento. This is someone we find who has a collection and stash of identification documents or even has just one particular document that reflects that they have opened an account but they haven't yet acted on the account. We

don't need to wait for that. They are guilty just based on the possession of that false document, so long as we can show beyond a reasonable doubt that it is done with that intent.

Senator KYL. Now, is the intent what is known in law as the scienter requirement?

Mr. COLLINS. Yes.

Senator KYL. And that is the ability to prove that there was a knowing intent to—or a knowledge of and knowing intent to commit the crime?

Mr. COLLINS. That is correct.

Senator KYL. Or to commit a crime.

In your testimony, you talk about the fact that, in addition to proving all of the elements of the predicate crime, including scienter, prosecutors must also establish that the defendant knowingly transferred or used the identification with the intent to commit a Federal or State crime, and that S. 2541 would streamline the proof by requiring proof of only that level of scienter that is already required by the underlying predicate offense and the knowing use of another's identity.

So is that what you are talking about here with respect to having to prove scienter even though there hasn't been a transfer or a sale?

Mr. COLLINS. The potentially multiple layers of scienter that are in the existing law come from the fact that if you look at 1028(a)(7) is says "knowingly transfer," and now that would be "transfer or possess or use," and then "with the intent to commit," and then it is a further violation. And then we actually sat down and wrote out the jury instructions, it becomes apparent because the first element is knowingly; second is with intent to commit; and then you have to give all the elements of the underlying offense, which may itself have a scienter.

Now, you don't have to prove the underlying offense. It is intent to commit. But, nonetheless, we are potentially at three levels of scienter depending on what kind of predicate is used.

Now, having this broad a statute is clearly very valuable, and we have gotten very good feedback on this. But that is the idea behind the aggravated identity theft, is let's pick out the most serious forms, let's streamline this, the proof requirements, so that it is basically knowing possession, underlying offense, and we are done and then clarify the penalty structure as well.

Senator KYL. And can you describe any cases that you may be familiar with, or either of the other witnesses here, to illustrate this point to us? It is unfair to ask you, I know. I didn't ask you to bring the cases when you came to the hearing.

Mr. COLLINS. The Attorney General at his press conference identified a number of different cases that were part of the sweep. One of them involved someone who was attempting to avoid a Federal prosecution by attempting to murder someone else and then assume his identity.

Now, actually that is sufficiently infrequent that murder is not one of the underlying aggravated predicates. What is more common is someone steals mail—and there were several cases announced by the Attorney General that fit within this pattern that is actually a distressingly common pattern, someone steals an item of mail

that contains a Social Security number or credit card information, opens an account, and then begins siphoning off money from the person.

We had the case involving the exercise of stock options. We had another case from Texas that involved two individuals who attempted to loot several persons of almost a quarter of a million dollars. So there were significant dollar amounts on some of these offenses, but they go the full range of the creativity of the criminal mind.

Senator KYL. Well, thank you, and what I was trying to do was obviously bring this right home to people so they can see practically why we are trying to do this. And your point also is that this is not unprecedented. What we are doing here fits in with some other statutes, and that essentially we are taking a variety of provisions and conforming them to one standard which will be useful in the prosecution of these crimes.

I am appreciative of the Justice Department and the other agencies' support, but also helping us identify those areas of the statute that we need to clean up. And I have said this to FTC representatives in the past, since probably you are on the front line and you are going to get more initial contact, whatever you see in the way of events occurring that would suggest changes, either in statutes or other things that we need to do, whether it is the Justice Department or anybody else or FTC, we want to hear about that so we can continue to try to stay a step ahead of these people, because right now it appears like they are a step ahead of us.

Thank you.

Chairperson FEINSTEIN. Thanks, Senator Kyl.

I have just got a couple of questions. The first is to Mr. Lormel. If I understand it right, 6 of the 19 hijackers from September 11th were using Social Security numbers illegally. Do you know how they got them?

Mr. LORMEL. No, ma'am, actually, they didn't use Social Security numbers. They made up numbers for account purposes when they were filling out bank applications. So, in actuality, they had no intent—I don't think they understood the system, those particular people. So they just filled in numbers.

Chairperson FEINSTEIN. So they just made them up?

Mr. LORMEL. Yes.

Chairperson FEINSTEIN. And that went through?

Mr. LORMEL. Yes.

Chairperson FEINSTEIN. Wow. How does that happen? Nobody checks?

Mr. LORMEL. I think from the standpoint of lessons learned, that was a valuable lesson that has been learned. But I also think that those instances were very limited, and I think people took too much for granted in the application process prior to September 11th.

Chairperson FEINSTEIN. Now, banks now know that?

Mr. LORMEL. Oh, yes, ma'am. We have had an aggressive outreach program, and we have ongoing dialogue with a number of the major banks, and they are well aware of some of the problems.

Chairperson FEINSTEIN. Do they then report to you made-up Social Security numbers?

Mr. LORMEL. That would be reported through the suspicious activity reports to FinCEN, and I am sure there is a better vigilance there.

Chairperson FEINSTEIN. The interesting thing of this is that at least we have been led to believe that there was very little communication among the 19 hijackers. Therefore, having six of them doing the same thing would indicate to me that there may well be others doing the same thing.

Mr. LORMEL. The 19 hijackers, in that regard, though, you may have had a few of them who were the leaders. They basically would typically, if they were going to open up bank accounts or things, go in groups where perhaps one of them acted as a leader for three or four. So those——

Chairperson FEINSTEIN. Do you know that for a fact? Because—question: Do you know that for a fact?

Mr. LORMEL. Yes, ma'am. We had indications that they were acting in certain regards in groups, if I understand your——

Chairperson FEINSTEIN. In other words, that they met or communicated—I am talking about the 19 specific people.

Mr. LORMEL. Right. They were kind of compartmentalized and three or four of them acted together, would travel together.

Chairperson FEINSTEIN. But this is six.

Mr. LORMEL. Right, but—I am not sure if I have followed what you were saying, but they——

Chairperson FEINSTEIN. No. What we have been led to believe—and I think, you know, this has been in the public press—is that one of the reasons the operation was what it was is because they didn't really know each other for the most part. They lived all—maybe two together, but separately. There was no communication among them.

Mr. LORMEL. That is kind of complex in the sense that they were in kind of four groups. So I think it is a matter of semantics, yes and no, and I don't mean to be evasive on that. But there was a certain level of communication, and, you know, they acted—even though they were compartmentalized in individual, but you had like your flight teams, so you had—the way I look at it from a financial viewpoint—and, you know, I don't mean to speak out of school with the terrorism side. But from our financial standpoint, we kind of lumped them into four groups, and from a financial transactional standpoint, I could link them together differently. And in opening the bank accounts and just following the financial flows, you could see that one led three or four.

Now, I don't know what the direct level of communication between them was other than, you know, following the financial activity, so to speak.

I have just confused you more.

Chairperson FEINSTEIN. No, you haven't. For me, what you said was rather significant. We will have to take that up at another place and another time.

Mr. LORMEL. Yes, definitely. I think what you need to do in this regard—and I don't mean to get far from what your intent here is. What we are doing from a financial investigative standpoint is collateral to and in support of the terrorism investigation. So we kind of overlap the terrorism side. So I think it would be important then

to sit with the folks who conducted the actual terrorist side of the investigation with our financial investigators. I think our terminologies conflict a little bit, even though we are saying the same thing.

Chairperson FEINSTEIN. All right. Let me ask just one other quick question, and then I am through, and that is on the subject of jurisdictional issues. Supposing somebody steals your financial information in Las Vegas and then opens fraudulent accounts in San Francisco, Chicago, and Boston. What problems do multi-jurisdictional crimes pose? Who would take the lead in this kind of case?

Mr. COLLINS. That is the kind of issue where, number one, there have been some complaints in the past even about State and locals refusing to take police reports. Now, the statistics from the Federal Trade Commission show that in the year from 2000 to 2001 there was a 50-percent reduction in that noncompliance rate, shall we say, of State and locals. Now, that may be in part due to the fact that we have seen a growing increase at the State level of enactment of laws on identity theft so that we now have over 44 States that have laws. So now there is a crime at the State level at which the local police can take a report.

But that is where you need the sort of flexible coordination that comes from the Identity Theft Subcommittee and from the task forces that the Secret Service works with because they have the primary enforcement jurisdiction for many of these offenses. And it would just be an evaluation, you know, of which of the particular—if it was going to be taken federally—which U.S. Attorney's Office was best positioned to bring that prosecution and take the lead and move forward with it. If it was thought that that was something that could be done more effectively at the local level, then whatever assistance was necessary would be provided.

But that is why what we currently have now is a relatively flexible, informal structure in the Identity Theft Subcommittee in order to serve a coordinating and supportive role and not a directing role that attempts to manage what is really a significant amount of coordination from Washington.

Chairperson FEINSTEIN. But who would make that decision?

Mr. COLLINS. I don't know that there would be a single person or a committee. It is not that formalized. Obviously, if a crime comes up in a particular area and, you know, there are a number of different task forces or jurisdictions that would be involved in a particular case, then the representatives of those particular agencies would obviously have to communicate with one another to make that decision.

So, again, it is hard to say that there is a particular process. The process that we have set up with the Identity Theft Subcommittee emphasizes informality and flexibility because, again, most of these prosecutions are going to be at the State and local level.

Chairperson FEINSTEIN. Thank you.

I would just like to put a couple of statements in the record. The ranking member of the full committee, Senator Hatch, has a statement, and Senator Cantwell would like to submit a statement to the record, also some questions. So the record will remain open for one week.

Chairperson FEINSTEIN. Senator Kyl?

Senator KYL. I have just one last question. I sort of said we want to continue to hear from everybody if you have suggestions, but specifically to you, Mr. Beales, is there anything at this time that the FTC would like to recommend, since I think your office probably receives the most number of direct communications regarding the level of identity theft violations around the country and gives out the 1–800 numbers and so on. Is there anything else that we should be focused on right now that you can think of?

Mr. BEALES. I don't think there are other things that we have seen that have pointed to a specific need for legislation or that we have seen as identifying a specific need for legislation. We are monitoring on a pretty continuous basis the kinds of complaints we are getting and trying to watch the trends. And if we see changes that we think suggest that legislative solutions would be useful, we would certainly bring them to your attention.

Senator KYL. Great. Okay. I appreciate that. Again, I thank all of the witnesses.

Chairperson FEINSTEIN. Yes, thank you all very, very much. This was very helpful, and it was short so we both appreciate that.

Thank you very much, and the hearing is adjourned. [Whereupon, at 3:30 a.m., the subcommittee was adjourned.]

[Submissions for the record follow:]

STATEMENT OF SENATOR ORRIN G. HATCH, RANKING REPUBLICAN MEMBER

Madame Chairwoman, I want to commend you once again for holding another hearing on this critical topic. We are all aware that identity theft is one of the fastest growing and most sinister crimes in America. Rarely do criminals appropriate personally identifiable information for the sole purpose of impersonating another; rather, such information is often used to commit a wide range of other, often serious, crimes. Recently, we learned that an Algerian national allegedly stole the identities of health club members and sold to an Algerian who was convicted in a failed 1999 plan to bomb the Los Angeles International Airport.

This year to date this Subcommittee has focused its attention on legislative proposals that would assist victims in clearing their good names and reduce the prevalence of social security numbers and other sensitive personal information. To stem the growth of identity theft, however, we need to attack the problem on all fronts. Strengthening the tools of our criminal justice system is an essential part of this process.

Senators Feinstein and Kyl have both been champions of legislative reforms in this area. In 1997, Senator Kyl authored a bill that eventually became "The Identity Theft and Assumption Deterrence Act". While this act represented an important step in our effort to curb identity theft, we must continue to refine and supplement our criminal enforcement tools in this area.

The "Identity Theft Penalty Enhancement Act", S. 2541, which Senators Feinstein, Kyl, Sessions and Grassley introduced last year, with the support of the Administration, does just that. Most significantly, S. 2541 creates a class of "aggravated" identity theft offenses that includes the most serious forms of identity theft; such offenses would be subject to stiff mandatory penalties and simplified proof requirements. The bill also increases the maximum penalties that would apply to a variety of identity fraud offenses, I support such provisions, and I look forward to hearing what our distinguished witnesses have to say about the particular crimes that are listed in S. 2541 as predicate offenses, as well as the simplified proof requirements that apply to such offenses.

I also invite our distinguished witnesses to share their views regarding additional criminal measures we should consider to stem the disturbing trend of identity theft. In particular, I am interested in whether we should amend 18 U.S.C. § 1028(b) to include mandatory penalties that would apply to those who traffic fraudulent or stolen identification documents in large numbers. I am also interested in whether we should expand 18 U.S.C. § 1028(a) to apply to those who "procure, obtain or receive"

identification documents and to those who "seek, cause or direct" the unlawful production of identification documents.

I am committed to strengthening our criminal statutes and penalties to ensure that the perpetrators of identity theft crimes are adequately deterred and punished. I look forward to working with members of the Judiciary Committee and the full Senate, on a bi-partisan basis, to accomplish this worthy goal during this Congress.

STATEMENT BY SENATOR STROM THURMOND

Madame Chairman: Thank you for holding this hearing today regarding S. 2541, the Identity Theft Penalty Enhancement Act. I am pleased that we are addressing the growing problem of identity theft, and I commend both you and Senator Kyl for your leadership in this area.

The crime of identity theft is a growing national problem. According to a March, 2002, report by the General Accounting Office, the prevalence of identity theft is increasing. The GAO identified several disturbing trends over the past few years. For example, in March of 2001, the Federal Trade Commission's Identity Theft Clearinghouse received just over 2,000 complaints of identity fraud per week. By December of that same year, the number of complaints and skyrocketed to 3,000 per week. The Social Security Administration also reported an increase in the number of identity theft-related calls to its Fraud Hotline. The number of calls alleging the misuse of Social Security numbers increased from 11,000 in Fiscal Year 1998 to 65,000 in Fiscal Year 2001.

The two major credit card associations, MasterCard and Visa, have reported increased losses due to fraud. According to the GAO, losses increased from $700 million in 1996 to approximately $1.0 billion in 2000, representing in increase of about 45%.

However, the big losers are the individual victims themselves, who often face a difficult and arduous process of cleaning up their credit records. According to a 2000 survey conducted by the California Public Interest Research Group and the Privacy Rights Clearinghouse, vicitims of identity theft spent an average of 175 hours attempting to clear their credit and prove their good names.

I am pleased that the Bush Administration has made a commitment to stemming the tide of identity theft crimes. The Attorney General has announced an increased emphasis on the prosecution of these crimes and has actively pursued a coordinated approach between Federal and state law enforcement agencies. With this renewed commitment to prosecuting identity thieves, it is important that the Congress provide the Department of Justice with improved criminal statutes that will allow for the appropriate prosecution and punishment of lawbreakers.

The Identity Theft Penalty Enhancement Act of 2002 is a significant step in the right direction. This bill would create the crime of aggravated identity theft and would provide for enhanced penalties. Aggravated identity theft would be defined as the unlawful and knowing transfer, possession, or use of a means of identification of another person while in the course of specific felony violations. These felonies would include, among others, theft from employee benefit plans, bank fraud, and fraud relating to passports and visas.

Due to the nature of the most damaging identity theft crimes, the creation of a new offense of aggravated identity theft would be sensible. Because a person's identity is often stolen in connection with another crime, prosecutors would only be required to prove that a thief knowingly stole an identity during the commission of the underlying, or predicate, crime. Therefore, criminal intent would only have to be proved for the predicate crime, which would streamline the jobs of prosecutors in bringing these criminals to justice.

In addition to the creation of the new offense of aggravated identity theft, the bill would also increase the maximum term for ordinary identity theft and for identity theft committed in the course of an act of domestic terrorism. Furthermore, the bill would also make an important change in the statute by making it unlawful to merely posses a means of identification, such as a Social Security number, with the intent to commit a crime. Current law only makes the transfer or sale of a means of identification unlawful, but not the possession.

I am encouraged by the goals of the Identity Theft Penalty Enhancement Act. I agree that we would punish those who commit identity theft with enhanced sentences. However, I have concerns about the particular sentencing requirements of this bill. As written, S. 2541 would require an additional two-year term of imprisonment for the commission of identity theft in the course of other specified felonies. This kind of approach, if adopted on a widespread basis, could begin to erode the

structure and purpose of the Federal Sentencing Guidelines. Instead of allowing a judge to enhance a sentence based on the particular circumstances of the case, the bill would impose a rigid two-year requirement for all categories of cases. In many circumstances, the additional penalty of two years may be too low. I hope that this Committee will carefully consider the implications of the sentencing provisions of this bill. The Sentencing Guidelines have been very successful, and the approach incorporated into this bill has the potential to interfere with the proper operation of the guidelines.

This problem could be addressed by imposing a maximum penalty for the offense of aggravated identity theft. Then, the Sentencing Commission would incorporate the new crime into the guidelines as is done with most other Federal offenses. In order to make sure that the identity theft results in an enhanced sentence over the predicate crime, the bill could also direct the Sentencing Commission to structure the guidelines in this manner.

Madame Chairman, thank you again for holding this hearing on the critical issue of identity theft. Congress must provide new tools to law enhancement if we are to stop this growing problem. The Identity Theft Penalty Enhancement Act is an important step in the right direction. I look forward to working with you on this bill, and I welcome our witnesses here today.

○