S. HRG. 106–902

IDENTITY THEFT: HOW TO PROTECT AND RESTORE YOUR GOOD NAME

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

ON

PREVENTING CRIMINALS FROM USING TECHNOLOGY TO PREY UPON SOCIETY, FOCUSING ON IDENTITY THEFT PREVENTION MEASURES AND THE IMPLEMENTATION OF THE IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT (PUB. LAW 105–318)

JULY 12, 2000

Serial No. J–106–97

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
69–466 CC WASHINGTON : 2001

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

STROM THURMOND, South Carolina	PATRICK J. LEAHY, Vermont
CHARLES E. GRASSLEY, Iowa	EDWARD M. KENNEDY, Massachusetts
ARLEN SPECTER, Pennsylvania	JOSEPH R. BIDEN, JR., Delaware
JON KYL, Arizona	HERBERT KOHL, Wisconsin
MIKE DEWINE, Ohio	DIANNE FEINSTEIN, California
JOHN ASHCROFT, Missouri	RUSSELL D. FEINGOLD, Wisconsin
SPENCER ABRAHAM, Michigan	ROBERT G. TORRICELLI, New Jersey
JEFF SESSIONS, Alabama	CHARLES E. SCHUMER, New York
BOB SMITH, New Hampshire	

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

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

JON KYL, Arizona, *Chairman*

ORRIN G. HATCH, Utah	DIANNE FEINSTEIN, California
CHARLES E. GRASSLEY, Iowa	JOSEPH R. BIDEN, JR., Delaware
MIKE DEWINE, Ohio	HERBERT KOHL, Wisconsin

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

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

CHRONOLOGICAL LIST OF WITNESSES

ALPHABETICAL LIST AND MATERIAL SUBMITTED

IDENTITY THEFT: HOW TO PROTECT AND RESTORE YOUR GOOD NAME

WEDNESDAY, JULY 12, 2000

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

The subcommittee met, pursuant to notice, at 10:03 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Jon Kyl (chairman of the subcommittee) presiding.

Also present: Senator Feinstein.

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

Senator KYL. Good morning. This hearing of the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information will come to order. The subject of our hearing this morning is "Identity Theft: How to Protect and Restore Your Good Name."

As chairman of this subcommittee, it has been my goal to prevent criminals from using technology to prey on society. There are few clearer violations of personal privacy than having your identity stolen and used to commit a crime. Criminals often use Social Security numbers and other personal information to assume the identity of law-abiding citizens and take their money. It is high-tech theft.

To combat this, I sponsored the Identity Theft and Assumption Deterrence Act, which prohibits the stealing of a person's identity. The aim of the Act, which is now law, is to protect consumers and safeguard people's privacy. Almost 2 years after passage of the Act, identity theft unfortunately continues to grow, particularly as the Internet grows in popularity.

Teachers, housewives, doctors and, yes, even U.S. Senators have been recent victims of identity theft. It can happen to anyone.

Well, how does it happen? Technology enables new, sophisticated means of identity theft. Using a variety of methods, criminals steal Social Security numbers, credit card numbers, drivers' license numbers, ATM cards, telephone calling cards, and other key pieces of a citizen's identity. Victims are often left with a bad credit report and must spend months and even years regaining their financial wholeness.

In the meantime, they have difficulty writing checks, obtaining loans, renting apartments, getting their children financial aid for college, even getting hired. Victims of identity theft need help as

they attempt to untangle the web of deception that has allowed another individual person to impersonate them.

The key to prevention is businesses establishing responsible information handling practices and for the credit industry to adopt stricter application verification procedures and to put limits on data disclosure. One provision in a bill that Senator Feinstein and I have proposed would require a credit card issuer to confirm any change of address with the cardholder within 10 days. This could prevent the common method of identity fraud where a criminal steals an individual's credit card number and then obtains a duplicate card by informing the credit issuer of a change of address. Credit bureaus would be required to disclose to credit issuers that an address on the application does not match the address on the credit report.

Another provision of this legislation would ensure that conspicuous fraud alerts would appear on credit reports, and also it would impose penalties for non-compliance by credit issuers and credit bureaus. Another provision would require the credit issuers and credit bureaus to develop a universally recognized form for reporting identity fraud. Victims could then fill out one form and one affidavit to supply to the numerous companies and entities involved in reporting an identity theft.

These legislative changes, and the willingness of many here to adapt to best business practices, will help victims to detect errors on their credit history, report the errors efficiently, and to act quickly to recover their good name.

Now, just a couple of statistics before we begin. I think it is interesting that in fiscal year 1999, the Social Security Administration's Office of Inspector General hotline for fraud and abuse reported more than 62,000 instances of misuse of Social Security numbers, something that Senator Feinstein has been working on. Since November 1999, the FTC hotline and website have logged more than 20,000 calls and 1,500 e-mail complaints regarding identity theft. So this is an ongoing, serious, significant problem.

Today, our subcommittee will hear from six witnesses about the effect of identity theft and the help that victims of identity theft can expect. On the first panel, we are glad to welcome back Jodie Bernstein, who is the current Director of the Bureau of Consumer Protection of the Federal Trade Commission. She will discuss how the FTC has responded to identity theft in carrying out its duties under the 1998 law. She will also discuss what legislative and non-legislative measures have been taken and what could reduce criminals' access to sensitive data.

James G. Huse, the current Inspector General of the Social Security Administration, is our next witness. He will discuss how Social Security numbers are used in the commission of identity theft, what steps can be taken to reduce the role of Social Security numbers in identity theft, why Social Security numbers can be purchased on the Internet for as little as $40, current undercover operations to prevent the sale of Social Security numbers on the Internet, and what is the most common source of Social Security numbers used for identity theft.

I will just mention who we will have on the second panel, then call upon Senator Feinstein and our first panel to begin its presentation.

Michelle Suzanne Brown will be one of the witnesses on the second panel. She is a victim of identity theft, and she will talk about her case and will share with us the very difficult experience that she has had in clearing her good name through endless telephone calls and correspondence with various credit bureaus, credit card companies, her landlord, property manager, police departments, the courts, and other government officials. She will also discuss her ideas about how to streamline the victim reporting process and how to recover and protect from this crime.

Beth Givens, of the Privacy Rights Clearinghouse, will be another witness on our second panel. The Clearinghouse has a new report, called "Nowhere to Turn," which describes common obstacles experienced by identity theft victims and what measures can be taken to reduce criminal access to sensitive personal information, and how to better provide services to identity theft victims.

Steve Emmert is the current president of the Individual Reference Services Group, the IRSG, and the director of the information company LEXIS–NEXIS. The IRSG is composed of 14 leading information industry companies that provide data to help identify, verify, or locate individuals. President Emmert will testify how the IRSG members limit the transmission of personal information to prevent criminal misuse, and testify about the progress of self-regulatory efforts, present some statistics on enforcement, compliance, and monitoring of member groups.

Finally, Stuart Pratt, executive vice president of Government Relations for the Associated Credit Bureaus, the ACB, will describe the use of fraud alerts within the credit bureau industry, addressing the duration of the alert, how credit card issuers use alerts, and he will testify about the resources of the ACB, what it has available for identity theft victims, and its plans to work with credit card issuers to streamline reporting of identity theft.

I want to thank all of our witnesses for being with us today. Before calling on our first panel here, I would like to again thank Senator Feinstein for her leadership in helping to get the identity theft bill passed into law and her continuing interest in seeing that it is enforced properly, and to help determine whether it goes far enough and whether we need to do some additional things now that we have some experience with it to ensure continued protection for consumers. It is always a pleasure to work with her.

I would also like to make this brief announcement. They are working on the air conditioning and I hope that we get it fixed before this hearing is over.

Senator Feinstein.

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

Senator FEINSTEIN. Thanks very much, Mr. Chairman, and let me thank you for your leadership. Let me thank the panelists, some of whom have come from California for this hearing. I think it is very important and I am just delighted that you are here.

Identity theft really deserves our committee's very close and careful attention. It is, I believe, one of the fastest growing crimes in the Nation.

Now, what is identity theft? It occurs when one person uses 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 potential victim's name. In other words, you steal someone's identity, credit documents, and then go out and commit fraud against them.

Identity thieves get personal information in a myriad of ways. They steal wallets and purses containing identification cards. They use personal information they can buy on the Internet. They steal mail, including pre-approved credit offers and credit statements. They fraudulently obtain another's credit reports, or they get another's personnel records.

Every 60 seconds in this country, an American becomes the victim of identity theft. Some estimates of the theft run as high as 700,000 cases a year. The chairman has quoted the Social Security Administration's concerns, but the U.S. Postal Inspection Service also reports that 50,000 people a year have become victims of identity theft since that Service first began collecting information of the crime in the mid-1990's. Treasury estimates that identity theft annually causes $3 billion in credit card losses.

Identity theft victims have actually been calling our office with story after story of these crimes, and let me give you a couple of examples.

My constituent, Kim Bradbury, of Castro Valley, reported that an identity thief obtained a credit card in her name through the Internet in just 10 seconds. The false application only had her Social Security number and birth date correct. As a matter of fact, my staff has compiled a list of about 12 different Internet websites where personal information can be purchased for as little as $25. Let me read their comments on one website called digdirt.com.

Here is one that is not online access, per se, but it will blow your mind as to what they offer. You hire them, they do the work, they get back to you—medical records, phone numbers, assets, et cetera. I am not going to say the names of all these websites, but I would like to enter them into the record, if I might, Mr. Chairman.

Senator KYL. Without objection.

[The information referred to follows:]

LIST SUBMITTED BY SENATOR FEINSTEIN

An analysis of the services anyone can use on the World Wide Web indicates that many sites sell Social Security numbers.

The following is just a short list of example sites that traffic in personal information.

(1) www.fastbreakbail.com
(2) www.infoseekers.com
(3) www.e-backgroundchecks.com
(4) *www.infotel.net*
(5) *www.docusearch.com*
(6) *www.1800ussearch.com*
(7) *www.locateme.com*
(8) *www.informus.com*
(9) *www.loc8fast.com*
(10) *www.merlindata.com*
(11) *www.digdirt.com*

Senator FEINSTEIN. Let me give you another example—Lynn Kleinenberg, of Los Angeles. Her husband was an executive at Cedars Sinai Medical Center. He died last December. The identity thief in her case used her husband's obituary to get the maiden name, then went to the Internet, and purchased various identification documents. The thief attempted to charge $200,000 in diamonds against her account. This included a $160,000 wire transfer which she was fortunately able to head off when the bank called her about her request.

Another person, Amy Boyer, a 20-year-old dental assistant from Maine, was killed last year by a stalker who bought her Social Security number off the Internet for $45 and used the number to locate her work address. Incidentally, some of these websites provide that you can buy the Social Security number for $25 now.

I have two proposals pending before the Congress today, and I hope we can discuss them. The first one prohibits the sale of Social Security numbers. The Administration supports this legislation. I am hopeful we can pass it. It is Senate bill 2699, entitled "The Social Security Number Protection Act." That would restrict the sale and purchase of Social Security numbers. It has some exceptions.

I am also right now writing legislation to amend that to provide for the same stipulations to a driver's license, to personal medical information, and personal financial data, and to provide an opt-in. In other words, the Internet site would have to get the permission of the individual before using their Social Security number, their driver's license, their personal medical information, or their personal financial information.

Now, this is very controversial, and we have met with many of the companies. They want to put the obligation on the individual. Well, if you put that obligation on me, I really wouldn't know where to turn or how to opt out. I think if somebody is going to make a profit off of my personal financial data, my Social Security number, my driver's license, they ought to ask me, find me and ask me if they can use it. I very deeply believe that, and I believe that enough reputable companies now are beginning to do it, so that it is not something very extreme to do.

Senator Kyl, you and I and Senator Grassley have also introduced a bill, S. 2328, entitled "The Identity Theft Prevention Act." This bill is supported by the Federal Trade Commission. It has gone to the Banking Committee. I doubt very much the Banking Committee is going to move the bill, but it is widely supported. The bill's measures aim to prevent identity theft. They give credit card holders written notice at their original address if a new card is requested to be sent to a different address.

The bill would impose penalties on credit issuers who ignore fraud alerts on a credit report. That is another problem. People just ignore it, you know, don't go and check. It also directs credit bureaus to notify credit issuers if there are inconsistencies in a credit application. This legislation would also authorize the development of a single reporting form that an identity theft victim could fill out to notify creditors of fraudulent charges in their name, and it would provide an individual with a free annual credit card report. Six States already guarantee free access to these reports.

I think there is really nothing so sacred as an individual's good name, and that is one of the reasons why identity theft is so devastating. It robs people of their reputation and their security that they often spent years building, and it can present untold problems. I believe we have one witness today who will tell a story of being detained at the airport, because of a crime committed in her name by the identity thief. She had left the country for vacation, and upon her return, Customs wouldn't let her back into the country. She is an innocent victim.

So, Mr. Chairman, the bottom line is I think we need to move and pass these bills, particularly the Social Security number. The Social Security number is our No. 1 personal identifier. It is meant for personal identification. It is not meant as a barter tool to be able to encourage commerce, and I think it is appropriate for the Federal Government to take some action to set some strict restrictions on the use of this national personal identifier.

So I would be hopeful that we would see fit, you and I, to move that particular bill. And I hope to introduce tomorrow the one that would add to the Social Security number also the driver's license, personal financial data, and personal health data. There are exceptions which we will put in which I think kind of cover, for example, research that is done without revealing the personal identity of the person. So for bona fide medical purposes, it could be used, or bona fide credit rating purposes it could be used, but not to reveal to the public at a purchase price the individual data.

Thank you very much.

Senator KYL. Thank you very much. As we discussed, I agree, and we will try to move, whether we need to do it in the subcommittee and the full committee. We should also talk to the Banking Committee, and we will do that.

I really appreciate all of the witnesses being here today. Let's begin with Ms. Bernstein, and then Mr. Huse will follow that.

PANEL CONSISTING OF JODIE BERNSTEIN, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, WASHINGTON, DC; AND JAMES G. HUSE, JR., INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION, BALTIMORE, MD

STATEMENT OF JODIE BERNSTEIN

Ms. BERNSTEIN. Thank you very much, Mr. Chairman. Thank you for including us. I am pleased to be able to present the Commission's testimony, but I also wanted to let you and Senator Feinstein know just how important your attention on this in terms of holding hearings has been for us. It has focused attention on American consumers so that they can take steps when they can to prevent these occurrences. And, importantly, other parts of the Congress have been supportive of our efforts, and I really do believe it is because of the attention that you have focused on this issue. So thank you for that as well.

I thought what I would do today would be to update you on what our complaint data tells us about ID theft and how we can all perhaps do a better job of trying to reduce identity theft and fraud. As Senator Feinstein mentioned, we, the Commission, has sup-

ported the legislation that you all have introduced, and we thank you for that as well. We think that will be a great help.

So here is what we have been able to do, and I think we have made great strides in victim assistance and in data-sharing. We do have a slide. I have my—I call her my technical guru, but at another hearing she was asked to testify. So perhaps I shouldn't introduce her that way, but she is presenting the slides.

We distributed more than 83,000 copies of our popular brochure, "When Bad Things Happen to Your Good Name." Our colleagues at the Social Security Administration distributed 115,000 copies on their own, and our Web version has been viewed by over 110,000 consumers. The ID theft website, www.consumer.gov/idtheft, has received about 110,000 visits. These are very positive trends because we know that informed consumers can protect themselves from some of the harm caused by identity theft.

During my testimony in March, I also spoke about our complaint clearinghouse, the central repository of identity theft complaints, pursuant to the legislation passed earlier. We pushed this project forward and we have had really terrific results, I think.

First, we made the complaint data a click away for the law enforcement officers that will prosecute the crimes. Law enforcement officers can easily access complaints on Consumer Sentinel, and that is a web-based system linking more than 250 agencies to a single and central body of consumer fraud complaint data. The system now has more than 200,000 consumer fraud complaints and has resulted in hundreds of successful civil and criminal prosecutions. Consumer Sentinel users have to sign a confidentiality agreement and then they have access to the ID theft clearinghouse data.

Using a password, law enforcers use a desktop PC to link to a secure website from which they can search for ID theft perpetrators or victims in their backyards and seek out trends and patterns. As you can see from the slide, we have developed different ways to search for the data to enable law enforcement users to customize their searches and to retrieve precisely the data they are looking for. For example, users can also place alerts on certain records, flagging a target as under investigation or as an open file. In addition, FTC investigators and data analysts will be scrutinizing the data and we will refer cases to appropriate agencies. I think what you can see from this is we have been trying to be at least as smart as the ID thieves are in using the new technology, and hopefully we will succeed.

We launched the web availability of our system just last week, and already Social Security's Inspector General, Jim Huse, sitting with me, the Postal Inspection Service, the Department of Justice, and State attorneys general are on the system, reviewing and analyzing the data through the website.

We are also finalizing an agreement with Social Security—I think we will do it probably very shortly—to transfer their complaint data into the central clearinghouse, which will then enrich the clearinghouse. It will be increasingly valuable as it grows. Since its creation, the launching of the online complaint form, and the establishment of our toll-free consumer complaint line, we have received more than 20,000 telephone calls and 1,500 consumer complaints via our online complaint form. That was a very signifi-

cant development for people to be able to use the form right on the website.

In March, I told you that we have received 400 calls a week to the toll-free number. That number has doubled, to about 800 to 850 calls a week. We expect the rate to continue to climb, and we expect and hope we will be able to manage the new volume of calls.

The other clearinghouse news to share is what we have learned from the data, and again we have a slide. Half of the ID theft complaints report credit card fraud; that is, the thief either opened a new account in their name or took over an existing account. Approximately a quarter report that identity theft opened up telephone, cellular, or other utility services in their name. Bank fraud is the third category, and about 16 percent reported that a checking or savings account had been opened in their name, and or that fraudulent checks had been written. Approximately 11 percent reported that identity theft obtained a loan, such as a car loan, in their name.

These figures have been consistent across geographic regions in the country, and the top sources of complaints in the Nation, as well as in your States, are also shown on our reports; that is, Senator Feinstein, for example, you can get the complaints that are from the State of California, and we expect to be able to provide that to law enforcement officials in those States.

So what about these trends? With credit card fraud appearing in more than half of the complaints, it is time, we think, to take a good hard look at business practices. As you know, the Commission has supported the recent legislative proposals that require credit grantors to take extra steps to verify change of address requests for credit accounts.

We also endorse requiring credit bureaus to tell a consumer when a credit application is made in the consumer's name but with a different address. Each of these measures will help cut back on the top category of complaints. Those are account takeovers and fraudulently opened credit accounts. Free annual credit reports may also encourage consumers to review their credit reports and allow them to detect early warnings of fraud. There are additional requirements in 2328 that I won't detail because we have already discussed them. We think they will be very, very helpful.

In closing, I would add that there are steps that we at the FTC would like to implement to streamline and simplify the process of reporting and responding to ID theft. We want to implement an electronic notification system so that when a consumer tells us that their identity has been stolen, we can transmit that information to one of the three or all of the three credit reporting agencies and they can enter a prominent fraud alert on that consumer's file, on all three of them.

We can only take on this project and others like it by working together with you, with the public, and the private sector groups toward this common goal. We think it would go a long way, and we remain prepared to do that if we receive that cooperation from the industry involved.

I would be happy to answer any questions you may have, I presume, following Jim's testimony. Thank you.

[The prepared statement of Ms. Bernstein follows:]

PREPARED STATEMENT OF JODIE BERNSTEIN

Mr. Chairman Kyl, and members of the Subcommittee, I am Jodie Bernstein, 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 important issue of identity theft, and to describe to you the impressive strides we have made in implementing the Identity Theft and Assumption Deterrence Act.[2]

The fear of identity theft has gripped the public as few consumer issues have. Consumers fear the potential financial loss from someone's criminal use of their identity to obtain loans or open utility accounts. They also fear the long lasting impact on their lives that results from the denial of a mortgage, employment, credit or an apartment lease when credit reports are littered with the fraudulently incurred debts of an identity thief.[3]

The Identity Theft and Assumption Deterrence Act ("the Identity Theft Act") has raised the public's appreciation for the hardship suffered by identity theft victims. The Identity Theft Act's focus on the individual as the victim—rather than just the financial institutions that often absorb the bulk of the financial loss—has brought focus to business practices that may place consumers at higher risk of having their identities stolen. It has heightened consumers' awareness of the ways they can change their everyday practices to minimize the risk that they will be victimized. The Federal Trade Commission has worked to strengthen these measures through our responsibilities under the Act. In particular, we have expanded our consumer education campaign, encouraged increased use of our toll-free help line, made our Identity Theft Clearinghouse available to law enforcement through a secure website, continued to forge partnerships with other law enforcement offices, and reached out to private industry to help identify ways to establish identity theft prevention best practices. By letter dated June 1, 2000, we also conveyed our support for S. 2328, a bill introduced by Senator Feinstein, Chairman Kyl and Senator Grassley, that seeks to protect consumers by providing them with access to credit-related information that may reveal indicia of identity theft. The bill would also restrict the release of information through the sale of "credit header" information, and entitle consumers to free annual credit reports.

The Commission's participation in the March Summit on Identity Theft, hosted by the Department of Treasury, marked the beginning of a new dialogue among government, private sector and consumer groups on these critical issues. We continue to look for ways to expand on these efforts.

I. MEETING THE GOALS OF THE IDENTITY THEFT ACT

In earlier testimony before this Committee, the Commission described the ways in which we have carried out our responsibilities under the 1998 Identity Theft Act.[4] Since that time, we have built on these achievements.

A. Centralized Complaint Handling—877 ID THEFT

The Commission established its toll-free telephone number, 1–877–ID THEFT (438–4338) to help consumers avoid or resolve identity theft problems. The Identity Theft Hotline phone counselors also enter information from the consumer complaints into the centralized Identity Theft Data Clearinghouse. In operation since November 1, 1999, the Identity Theft Hotline now receives between 800 and 850 calls per week.[5] About two thirds of the calls are from victims, the remaining calls coming from consumers who are looking for information on ways to minimize their risk of identity fraud.

The telephone counselors provide victims of identity theft with specific information about how to try to prevent additional harm to their finances and credit histories. The phone counselors advise callers to contact each of the three consumer

---

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

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

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

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

[5] That figure has doubled since March, when we reported 400 calls a week. To date, the hotline has received more than 20,000 calls.

reporting agencies to obtain copies of their credit reports and request that a fraud alert be placed on their credit report.[6] Fraud alerts request that the consumer be contacted when new credit is applied for in that consumer's name. We advise consumers to request copies of their credit reports, and explain how to review the information on the reports carefully to detect any additional evidence of identity theft. Because the credit reports of identity theft victims often reflect the fraudulent accounts opened or other misinformation, the counselors inform callers of their rights under the Fair Credit Reporting Act and provide them with the procedures for correcting their credit report.[7] The counselors advise consumers to contact each of the creditors or service providers where the identity thief has established or accessed an account, and to follow up in writing by certified mail, return receipt requested. Where the identity theft involves "open end" credit accounts,[8] consumers are advised on how to take advantage of their rights under the Fair Credit Billing Act, which, among other things, limits their responsibility for unauthorized charges to fifty dollars in most instances. Consumers who have been contacted by a debt collector trying to collect on debts incurred by the identity thief are advised of their rights under the Fair Debt Collection Practices Act, which limits debt collectors' practices in their collection of debts.

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

B. Outreach and Consumer Education

The FTC also reaches consumers through the Internet. The FTC's identity theft website—www.consumer.gov/*idtheft*—gives tips on how consumers can guard against identity theft, warns consumers about the latest identity theft schemes and trends, and provides access to consumer education materials on identity theft. This website has received more than 108,000 hits since November, 1999. The site also links to a secure complaint form on which identity theft victims can enter the details of their complaints online, allowing consumers to contact the Commission at all times. After review by FTC staff, these complaints are entered into the Clearinghouse. To date we have received more than 1500 complaints through this electronic form.

The Federal Trade Commission continues to distribute the comprehensive consumer guide: *ID Theft: When Bad Things Happen to Your Good Name.* Developed in consultation with more than a dozen federal agencies,[9] this booklet provides consumers with practical tips on how best to protect their personal information from identity thieves, summarizes the various federal statutes that protect consumer victims of identity theft, and details the victim assistance mechanisms available. The Federal Trade Commission has distributed more than 83,000 copies of the booklet, and is in the process of revising the booklet for a second, and larger printing. The Social Security Administration has also printed and distributed 115,000 copies of *When Bad Things Happen.*[10]

C. Identity Theft Clearinghouse—Launched Online

The Identity Theft Act authorized the Commission to establish a central repository of consumer complaints about identity theft, and refer appropriate cases to law

---

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

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

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

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

[10] The FTC has provided the booklet on zip disk to other agencies who are interested in printing additional copies.

enforcement for prosecution. The Identity Theft Complaint Database, which was activated in November 1999, provides specific investigative material for law enforcement and larger, trend-based information providing insight to both private and public sector partners on ways to reduce the incidence of identity theft. Currently, the Clearinghouse contains the data from consumers who contact the FTC through the toll free number or website. We are pursuing ways to collect complaint data from other agencies and private sector entities to allow Clearinghouse users from law enforcement agencies to see as much complaint data on identity theft as possible.[11]

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

The Identity Theft Act also authorized the Commission to share complaint data with appropriate entities,"[12] including specifically the three major consumer reporting agencies and others in the financial services industry.[13] The Commission does not envision providing access to the complete database for these private sector entities. Unfettered access could interfere with law enforcement efforts. FTC data analysts can, however, identify patterns that reveal a business or business practice that exposes consumers to a high risk of identity theft. We will forward appropriate information about these complaints to the entities involved so they can evaluate and revise those practices.[14] Similarly, we plan to share limited complaint data with a business if data reveal that that business fails to respond to legitimate consumer complaints about identity theft or frustrates their efforts to correct misinformation on their credit reports.

II. WHAT THE CLEARINGHOUSE TELLS US ABOUT IDENTITY THEFT

The Identity Theft Act recognized the importance of creating a single repository for identity theft complaints. Accordingly, the Commission established the Identity Theft Clearinghouse to collect and consolidate these complaints. We are already seeing the fruits of this effort. Our basic complaint data show that the most common forms of identity theft reported during the first seven months of operation were:

• *Credit Card Fraud.*—Approximately 54 percent of consumers reported credit card fraud—i.e., a credit card account opened in their name or a "takeover" of their existing credit card account;

• *Communications Services.*—Approximately 26 percent reported that the identity thief opened up telephone, cellular, or other utility service in their name;

• *Bank Fraud.*—Approximately 16 percent reported that a checking or savings account had been opened in their name, and/or that fraudulent checks had been written; and

• *Fraudulent Loans.*—Approximately 11 percent reported that the identity thief obtained a loan, such as a car loan, in their name.

Not surprisingly, the states with the largest populations account for the largest numbers of complainants and suspects. California, New York, Florida, Texas, and Illinois, in descending order, represent the states with the highest number of complainants.[15] About 55 percent of victims calling the identity theft hotline report their age. Of these, 40 percent fall between the 30 and 44 years of age. Approxi-

---

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

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

[13] The unique role of the consumer reporting agencies in resolving the problems of identity theft victims is discussed below.

[14] S. 2328, introduced by Senator Feinstein, Chairman Kyl and Senator Grassley of this Subcommittee, identifies a set of best practices that would minimize consumers' exposure to identity theft. For example, S. 2328 would require that creditors notify consumers if they receive a change of address notification.

[15] Texas and Illinois had an equal number of complaints.

mately 26 percent are between age 45 and 64, and another 25 percent are between age 19 and 29. About 7 percent of those reporting their ages are 65 and over; and slightly over 2 percent are age 18 and under.

The data also reveal information about the perpetrators. Almost 60 percent of the caller-complainants provided some identifying information about the identity thief, such as a name, address, or phone number. More than one quarter of those victims reported that they personally knew the suspect. We also are assessing the data on the monetary impact of this theft. Some complainants provided estimates of the dollar amounts obtained by the thief, because they have received the resulting bills or been notified of the resulting bad debts. The range of dollar amounts reported varies widely, with approximately 34 percent of complainants reporting theft of under $1,000; approximately 35 percent of complainants reporting theft totaling between $1,000 and $5,000, approximately 13 percent of complainants reporting theft totaling between $5,000 and $10,000, and approximately 18 percent of complainants reporting theft of over $10,000.

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

The Clearinghouse data also reveal that consumers are often dissatisfied with the consumer reporting agencies. The leading complaints by identity theft victims against the consumer reporting agencies are that they provide inadequate assistance over the phone, or that they will not reinvestigate or correct an inaccurate entry in the consumer's credit report. In one fairly typical case, a consumer reported that two years after initially notifying the consumer reporting agencies of the identity theft, following up with them numerous times by phone, and sending several copies of documents that they requested, the suspect's address and other inaccurate information continues to appear on her credit report. In another case, although the consumer has sent documents requested by the consumer reporting agency three separate times the consumer reporting agency involved still claims that it has not received the information.

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

Callers to the hotline are not limited to identity theft victims. Indeed, approximately 36 percent of the callers simply requested information on identity theft. Many felt they were vulnerable to identity theft because, for example, their wallets had recently been lost or stolen (23 percent); someone had attempted to open an account in their name (19 percent); or they had given out their personal information to someone they did not know (7 percent).[16]

III. NEXT STEPS

The Commission has made great strides in assisting consumers and law enforcement to combat identity theft, but recognizes that much remains to be done. As mentioned earlier, the Identity Theft Act authorizes the Commission to refer consumer identity theft complaints and information to the three major national consumer reporting agencies and other appropriate entities. The Commission envisions a streamlined process that would decrease the amount of time spent by consumer victims correcting credit report errors. Paramount among these efforts would be the ability of a consumer to make a single call to report him or herself as a victim of identity theft to the FTC or one of the three major national consumer reporting agencies, and to have a fraud alert posted on the credit reports from each of the reporting agencies. Currently, a victim of identity theft must notify each of the three national consumer reporting agencies separately, and then typically make additional calls to the FTC and to all creditors. The Commission looks forward to working with

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

the three major national consumer reporting agencies to develop a complementary process to allow identity theft victims to share the details of their complaints simultaneously with the FTC and the national consumer reporting agencies.

Further, the Commission will soon begin sharing certain limited information from its Identity Theft Clearinghouse with businesses whose practices are frequently associated with identity theft complaints. Our goal is to encourage and enable industry and individual companies to develop better fraud prevention practices and consumer assistance techniques. To that end, the Commission, in conjunction with the Department of Treasury and the other federal agencies who participated in the Identity Theft Summit, will convene a workshop for law enforcement and industry on Identity Theft victim assistance and prevention in the fall of 2000.

IV. CONCLUSION

The Identity Theft Clearinghouse, our toll free number, and the consumer education campaign have helped us begin to address the serious problems associated with identity theft. Heightened awareness by consumers and businesses will also help reduce the occurrences of this fraud. We look forward to continued collaboration and cooperation in these efforts. The FTC also looks forward to working with the Subcommittee to find ways to prevent this crime and to assist its victims.

Senator KYL. Thank you very much, Ms. Bernstein. That is a great update, and it shows both what is happening as a result of our legislation and what more needs to be done, exactly what we are all about here this morning.

Mr. Huse, thank you for being here.

STATEMENT OF JAMES G. HUSE, JR.

Mr. HUSE. Thank you, Mr. Chairman, Senator Feinstein. I want to thank you both for holding this hearing which focuses on the victims of identity fraud. While it is the victims for whom the Identity Theft Act was originally passed, and for whom we are all working to stem the tide of identity theft, it is also the victims whose plight is sometimes overlooked in the day-to-day business of enacting and enforcing these laws.

We are each faced with a challenge in combatting identity theft and protecting its victims. The challenge facing my office is to reduce the number of victims by preventing these crimes in the first instance, and punishing their perpetrators when they do occur. The challenge facing the Congress is to provide offices such as mine with the necessary tools to do so successfully.

The importance of meeting these challenges was evident in a survey reported in the June 13 issue of Investor's Business Daily, in which the Chubb Group of insurance companies found that 44 percent of 1,000 Americans polled had been victims of identity fraud. This is a staggering statistic, but one which is not surprising, as even at its simplest level the use of a Social Security number to commit identity fraud leaves a trail of victims in its wake.

Let me tell you about Waverly Burns, a Supplemental Security Income recipient from Milwaukee whose story I have used in the past as a classic identity fraud illustration. Mr. Burns stole another person's SSN and used it to secure employment as a cleaning crew supervisor. By hiding his work behind this new identity, he could continue to draw his SSI benefits under his own Social Security number. He went on to steal over $80,000 in computer equipment from the Wisconsin Supreme Court, obtained a State of Wisconsin identity card using the stolen SSN, opened bank accounts in the name of his victim, and filed fraudulent tax returns.

Our special agents arrested Mr. Burns in Chicago. He was sentenced to 21 months in prison and ordered to pay over $62,000 in restitution, including the full amount of benefits fraudulently obtained from SSA. Mr. Burns' case illustrates not only the central role of the SSN in identity theft crimes, but how a single such crime can have multiple victims. In Mr. Burns' case, the victims included the Social Security Administration, the Wisconsin Supreme Court, the financial institutions involved, the Internal Revenue Service, the State of Wisconsin, and the proper owner of the Social Security number.

In all likelihood, other ancillary victims included credit reporting agencies and other members of the public, including each of us in this room, who will have to bear the costs of Mr. Burns' misdeeds. Identity theft is a crime in which we are all victims.

My office employs an investigative staff of fewer than 300, and our primary responsibility must be to the programs and operations of the Social Security Administration. We alone cannot hope to stem the tide of SSN misuse and identity fraud. We are, however, taking every step we can in that direction.

A year ago, our Office of Investigations launched an SSN misuse pilot project in five cities across the Nation, working jointly with Federal and State law enforcement agencies to target perpetrators of identity crimes and SSN misuse. By joining forces with other law enforcement agencies in a task force environment, we were able to pool resources and share information aimed at fighting identity fraud.

Some of the accomplishments of those offices and the steps they are taking to aid identity theft victims are discussed in my written testimony, but already the pilot projects have been an unparalleled success. In their first year, 197 investigations have been opened resulting in 61 convictions. U.S. attorneys' offices and outside law enforcement entities have enthusiastically welcomed these pilots and have thanked us for taking the investigative lead.

Because of the increased role that the Internet is playing in SSN misuse and identity theft, we have expanded the scope of these pilots to include the sale of Social Security cards over the Internet. Using undercover purchases of Social Security cards, we can determine which vendors actually provide buyers with fraudulent documents and which merely take the money and run. We are very optimistic that we will be able to shut down several important Internet distributors of false identification documents through this initiative.

On the other side of e-commerce, we have recently launched another operation targeted not at those who sell false identification documents over the Internet, but at those who buy them. This effort has two goals. First, we can locate and stop those who purchase counterfeit Social Security cards that might be used in identity theft crimes. And, second, it will enable us for the first time to determine both the scope of Internet trafficking in false identification documents and the many ways one can use a false SSN.

Our efforts have been considerable and are aimed at maximizing the impact of limited resources through collaborative efforts with other agencies, particularly the Federal Trade Commission. Still, I would be remiss if I did not point out that there still exists a legis-

lative void that to some extent fosters the misuse of SSN's for purposes of identity theft.

Senate bill 2328, introduced by Senator Feinstein, together with you, Mr. Chairman, and Senator Grassley; Senate bill 2554, introduced by Senator Gregg, together with Senator Dodd; and Senator Feinstein's amendment to Senate bill 2448, which would prohibit the sale of Social Security numbers, all represent significant steps in the right direction.

Together, these bills create front-end limits on the use of Social Security numbers, and authorize criminal and civil sanctions and administrative penalties when violations occur. My staff would be happy to assist you in combining all of this legislation into a comprehensive bill that would enable us to bring the full authority of the U.S. Government to bear against those who would buy, sell, or otherwise misuse SSN's.

I welcome your interest in filling this legislative void, one aspect of which was the subject of a recent op ed column by the distinguished New York Times columnist William Safire, in which he expressed shock that no law prohibited compelling an individual to disclose his or her SSN. I am no less concerned than Mr. Safire that this and other acts, such as the sale, purchase, and public display of SSN's, remain legal. My office shares your concern for the victims of identity theft and is committed to providing those victims with the surest form of assistance, ensuring that the crime never occurs in the first place.

I welcome the subcommittee's continued support of our efforts and would be happy to answer any questions.

[The prepared statement of Mr. Huse follows:]

PREPARED STATEMENT OF JAMES G. HUSE, JR.

Good Morning Mr. Chairman and members of the Subcommittee. I want to thank you for holding this hearing on identity theft. Previously our attention concentrated on the challenges we faced in implementing the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act). Today, we focus on ways to prevent identity theft and how individuals can protect themselves from this crime, or if already victimized, repair the damage that has been done. Too little attention has been paid to the victims of this increasingly prevalent crime and there are other witnesses appearing today who can address the personal aspects of identity theft. My office is committed to ensuring that this type of crime is prevented, and if not prevented, then detected and sent forward for prosecution.

SSN misuse and the crime of identity theft are becoming so pervasive in our society, that it has become the subject of polls and an issue in the current presidential campaign. A June 13, 2000 article in Investor's Business Daily reported that an identity theft survey by the Chubb Group of Insurance Companies showed that 44 percent of those polled had been victims of identity theft. In fiscal year 1999, our Fraud Hotline received over 75,000 allegations with about 62,000 of these involving SSN misuse. Specifically, 32,000 had SSN misuse implications involving SSA programs and an additional 30,000 represented SSN misuse with no direct program implications. I am sure you will agree that these are alarming statistics.

THE EVOLUTION OF THE SSN INTO A TOOL FOR IDENTITY FRAUD

The Social Security number (SSN) is frequently the starting point for identity theft crimes. The SSN was created 65 years ago for the sole purpose of tracking the earnings of working Americans in order to implement and maintain the new Social Security system. The SSN was never intended to be the *de facto* national identifier that it has slowly become. For example, it was not until 1967 that the Department of Defense adopted the SSN in lieu of a military service number for identifying Armed Forces personnel. The SSN quickly became an integral part of enrolling in school, receiving financial assistance, applying for drivers' licenses; opening bank accounts, applying for credit, and myriad other activities. Today, Americans are asked

for their Social Security number as a part of any number of transactions in both the public and private sectors. The SSN has grown to become one of the most critical pieces of personal information.

REASONS BEHIND THE INCREASE IN SSN MISUSE

Perhaps the most obvious reason for the increase in SSN misuse is because people come from all over the world to take advantage of our free enterprise system. There are no realistic numbers available on how many tourists, students, and migrants remain in this country after their visas expire and work under a false SSN. The popularity and availability of the Internet in this day and age provides for an international marketplace for the sale of SSN's and if one is enterprising a new identity.

CRIMES COMMITTED WITH FRAUDULENT SSN'S

We have only begun to scratch the service in discovering the innovative ways in which the SSN is used to commit identity theft crimes. The most obvious example is the assumption of another person's name and SSN for purposes of committing simple financial crimes—today's version of the wild west bank robberies.

For example, our Special Agents, working as part of the Delaware Financial Crimes task force, investigated Zaid Gbolahan Jinadu as he schemed to defraud several federally insured financial institutions. He solicited the assistance of bank employees to obtain SSN's and other identifying data to open fraudulent credit card and bank accounts. These compromised employees also helped him to take over current accounts, make fraudulent wire transfers, receive cash advances, and negotiate numerous checks. Mr. Jinadu was indicted by a Federal grand jury in the District of Delaware on October 26, 1999 on four counts: one of bank fraud, one of identity theft, one of fraud in connection with access devices, and one of SSN misuse. On December 20, 1999, Mr. Jinadu and his co-defendants entered a guilty plea to the bank fraud and identity theft counts. Mr. Jinadu is responsible for fraud losses totaling approximately $281,122. The total known losses to financial institutions due to the actions of Mr. Jinadu and his claimed associates over the past 4 years exceeds $4 million.

The use of SSN's to commit identity theft can have a direct impact on SSA programs. Waverly Burns, a Supplemental Security Income (SSI) recipient in Milwaukee, stole another person's SSN and used it to secure employment as a cleaning crew supervisor. By taking on a new identity, he continued to draw SSI payments based on disability while also drawing a salary which would disqualify him as a benefit recipient. Under his new identity, Mr. Burns stole over $80,000 in computer equipment from the offices of the Wisconsin Supreme Court, used the stolen SSN to obtain a State of Wisconsin identity card, to open bank accounts in the victim's name, and filed fraudulent tax returns. Office of the Inspector General (OIG) Special Agents arrested Mr. Burns in Chicago. He was sentenced to 21 months in prison and ordered to pay over $62,000, *including the full amount of benefits fraudulently obtained from SSA.*

Mr. Burns' case illustrates how identity theft through the use of SSN's can have many victims—in his case SSA, the Wisconsin Supreme Court, the financial institutions, the Internal Revenue Service, the State of Wisconsin, and the proper owner of the SSN were all victims. In all likelihood, other ancillary victims included credit reporting bureaus and other members of the public who will have to bear the cost of Mr. Burns' misdeeds. Identity Theft is a crime in which we are all victims.

These examples show how the SSN is at the core of assuming the identity of another or establishing wholly fictitious identities. Unscrupulous individuals can hide behind either while committing a broad range of crimes. I would like to inform you of the initiatives this office has taken and how we expect to keep pace, if not a step ahead, of this escalating problem.

EXISTING AND FUTURE INITIATIVES

The OIG's efforts in combating the use of SSN's to commit identity theft crimes is widespread, but our small investigative staff, whose primary responsibility must be to the programs and operations of the Social Security Administration, cannot hope to stem the tide. This is not to say, however, that we are not taking all available steps in that direction. A year ago, our Office of Investigations launched an SSN misuse pilot project in five cities across the Nation, working jointly with Federal and State law enforcement agencies to target perpetrators of identity crimes and SSN misuse. By joining forces with other law enforcement agencies in a task force environment, we are able to pool resources and share information aimed at fighting identity fraud. In St. Louis, we have entered into a Memorandum of Understanding with the United States Attorney's Office, under which a Federal prosecutor

has been assigned to our task force, facilitating additional prosecutions. In Cleveland, in addition to its investigatory function, the task force is developing a letter to inform individuals whose identities have been compromised of actions they can take to minimize the effects of the crime. And in Milwaukee, the task force is making presentations to local law enforcement agencies, educating and sensitizing them to the array of identity theft crimes.

Pilot projects are in the early stages in two additional cities, and further expansion is planned. Already, the pilot projects have been an unparalleled success; in the first year we have opened 197 investigations which have already resulted in 61 convictions. United States Attorneys' Offices and outside law enforcement entities have enthusiastically welcomed such pilots and have thanked our office for taking the investigative lead.

Because of the increasing role that the Internet is playing in SSN misuse and identity theft, we have expanded the scope of these pilots to initiate programs in this area. Specifically they are investigating the sale of Social Security cards over the Internet. Using undercover *purchases* of Social Security cards, we can determine which vendors actually provide the documents and which ones take the money and run. Under either scenario, working with Federal, State and local authorities allows us to take action that extends beyond our stated mission of SSA program fraud and will prevent the conduct of identity theft crimes. We are very optimistic that we will be able to shut down several important Internet distributors of false identification documents.

On the other side of e-commerce, we started another operation targeted not at those who *sell* false identification documents over the Internet, but at those who *buy* them. This effort has two goals. First, we can locate and stop those who purchase counterfeit Social Security cards that might be used in identity theft crimes. Second, it will enable us, for the first time, to determine both the scope of Internet trafficking in false identification documents *and* the many ways one can use a false SSN.

THE NEED FOR LEGISLATION

While our efforts have been considerable, and are aimed at maximizing the impact of limited resources through collaborative efforts with other agencies, I would be remiss if I did not point out that there still exists a legislative void that, to some extent, fosters the misuse of SSN's for purposes of Identity Theft. Senate Bill 2328, introduced by Senator Feinstein, together with Senators Kyl and Grassley, Senate Bill 2554, introduced by Senator Gregg, together with Senator Dodd, and Senator Feinstein's amendment to Senate Bill 2448, which would prohibit the sale of Social Security numbers, all represent significant steps in the right direction. Together, these Bills create front-end limits on the use of Social Security numbers and authorize criminal and civil sanctions and administrative penalties when violations occur. My staff would be happy to assist you in combining all of this legislation into a comprehensive Bill that would enable us to bring the full authority of the United States Government to bear against those who would buy, sell, or otherwise misuse SSN's. Until there are criminal statutes, civil sanctions, and administrative penalties available to combat the many forms of SSN misuse that we see on a daily basis, we are ill equipped to bring this epidemic under control.

In a recent Op/Ed piece in the *New York Times,* columnist William Safire expressed surprise that Federal law does not currently prohibit the compelled disclosure of SSN's. We should be no less surprised.

CONCLUSION

Because the SSN is instrumental in perpetrating identity theft crimes this office, by virtue of its congressional mandate, must be a key player in the fight to control these crimes. The task is made all the more difficult by the broad range of crimes that fall within the identity theft category, the new role of the Internet in perpetrating identity theft, and the difficulty inherent even in determining where the crime begins, what course it takes, and who is the primary victim. Nevertheless, we have put in place, and continue to implement, strategies aimed at both better understanding and combating the use of SSN's to commit identity fraud crimes. I thank the Subcommittee for inviting me here today, and for its concern of this very real threat to every American.

Senator KYL. Thank you very much, Mr. Huse. Just with respect to the last point you were making about the monitoring of the sale and purchase over the Internet of Social Security numbers, what

are the current prohibitions on purchase, as well as sale, of someone else's Social Security number?

Mr. HUSE. There are no current prohibitions on the sale or purchase of someone's Social Security number at all, and that is the alarming issue here.

Senator KYL. And what are the prohibitions on the use of the Internet to therefore fraudulently sell or purchase somebody else's Social Security number?

Mr. HUSE. Again, Mr. Chairman, there are none.

Senator KYL. And, finally, a point that I think you just made, what is the current prohibition on forcing someone to tell you what their Social Security number is, other than IRS or Social Security?

Mr. HUSE. There are no prohibitions there either.

Senator KYL. Well, we could say case closed and get to work on the legislation, but I think that illustrates a very, very important point, and I appreciate your making that point very clearly.

Ms. Bernstein, in your testimony, and also before, you mentioned the practice of skimming, in which identity thieves use sophisticated devices to intercept personal information on credit cards and ATM cards. What is being done to combat this practice, and what could we do to help combat that?

Ms. BERNSTEIN. To the extent that we are able to get information about those practices—that is, consumers who have been victimized—and put it in our data base, we are trying to compile it to get to the appropriate law enforcers in order to try to make that a part of the criminal conduct; that is, it would be part of identity theft. It would be one way in which the thief could obtain the necessary information to pursue the identity. There is no specific prohibition that I know of in the criminal laws that makes that a specific crime, and it perhaps could be addressed in legislation to make it more specific.

Senator KYL. Right. Could you describe the practice specifically for those who hadn't heard your previous testimony?

Ms. BERNSTEIN. Well, at least from our anecdotal evidence that we have gathered from the complaint data, they have techniques of observing when you use your credit card to enter the ATM or to use your other information that may be observable by a thief.

For example, your telephone credit card has been used very widely to begin the process of reconstructing your identity by someone looking over your shoulder in an airport lounge, for example. It was widely used until people became aware of it. It still is an entry point for people because, from that number, often through other data bases you can begin to compile all the additional information that you need in order to be "Senator Kyl" and enter either your other credit or your bank account.

Senator KYL. Just as an aside, I serve on the Intelligence Committee and it is amazing to me how completely information about someone or something can be reconstructed starting with just one number, a telephone number, a Social Security number, a birth certificate, whatever it might be.

There are so many different entities in the country that have access to different kinds of data, now that we have the Internet, that it can be done literally with a click, as you point out. That is why we are trying to identify the different kinds of entry points, the

places where there could be a crime committed, especially where it is not yet a crime and we may need to consider making it such. So, that is another area, in addition to those that I talked to Mr. Huse about.

Just one more thing, you have talked about novelty Social Security cards. Talk a little bit about that and just explain the phenomenon to the subcommittee, if you would.

Mr. HUSE. Well, Mr. Chairman, on the Internet there are many companies that sell false identification documents. They call them novelties. There is a disclaimer, if you purchase these, when they arrive at your home. They could be anything. There is nothing that can't be counterfeited today. With the State of the art in terms of desktop publishing and computer graphics, you can counterfeit anything. So they can replicate any kind of a document, certificate, diploma. It makes no difference.

These arrive at your home, if you purchase them over these sites, with little pull-off stickers. The stickers, of course, say "this is a novelty, not to be used for identification." That, of course, covers the entity that is selling these, but there is a plethora of these on the Net. I mean, you can become anything you want today.

Senator KYL. Well, obviously, we will have to look into how to try to define around those kinds of techniques of avoiding a criminal situation, and we will have to work with you very carefully on doing that, I am sure.

Senator Feinstein.

Senator FEINSTEIN. Mr. Chairman, when I introduced the Social Security bill, and it was S. 2699, it went to Finance, where it has sat. Then I introduced the amendment to 2448 that Mr. Huse spoke about. That is an amendment to the Hatch Cyber Crime bill, and the Social Security bill was redrafted to involve Justice so that it could come to this committee.

I am trying to think of a way to at least control the Social Security number as kind of a first step because that is so much in the Federal domain. I would be interested in any of your views in that regard. I think maybe just to stay with the amendment to the Hatch Cyber Crime bill, put that on the Hatch bill, if he will have us.

Senator KYL. He will have us, I am sure. Yes, we will work together to make this happen.

Senator FEINSTEIN. All right, good. That is great.

Let me ask this question. With respect to the Internet, do either one of you have any views on the opt-in versus opt-out issue? Every time I discuss this, at least, with Silicon Valley people, it always comes down to opt-in versus opt-out.

Ms. BERNSTEIN. I could just offer a little bit of experience we have had, Senator, with what I call the Kids Act, COPA, the Children's Online Protection Act, which the Congress passed 18 months ago and we have implemented through rulemaking. It is now in effect. There is a requirement for verifiable consent for parents before an operator can obtain any information about an under-age consumer.

Senator FEINSTEIN. So that is an opt-in?

Ms. BERNSTEIN. It is opt-in, and we had a considerable discussion both before the Act was passed and in the rulemaking context,

and I think have worked out methods by which the consent can be obtained from parents, and I think it has worked quite well to date. We are trying to encourage them, and there have been some efforts to really develop technology that would make it easier to go opt-in instead of opt-out, because I think in the end that is probably the only real impediment, is how do you get it done.

So we have had a positive experience in that area and it has really worked quite well. So I don't believe that it would shut down the Internet if you have opt-in for certain kinds of use or misuse of very sensitive information. Medical/financial, of course, are generally considered by most Americans as very sensitive. In other words, you could make some discreet differences, considering what kind of information was being obtained or used.

Mr. HUSE. I endorse everything that Jodie said, but I would just like to take it from another tangent. We all know that the Social Security number has become our own personal identifier and, in fact, it is the national identifier. We all know it was never intended to be that, but *de facto* it has become that.

Since it is synonymous with our name and our own reputations, I personally believe that the biggest weakness we have is this consent piece. If we build that in, all the rest of legitimate commerce can go on. But I think every one of us should have a personal right to decide whether and how our financial information that is under the tent of this number, and all the other uses of the SSN—we should have the right to yes or no. And I think that is the piece that we really need to work on. If we could fix that, the rest will follow. So I agree, opt-in is really the way to go.

Senator FEINSTEIN. So you are saying that the most important part is the Social Security number. Now, with respect to the Social Security number, at least in the legislation I have submitted, there is no opt-in/opt-out. You are prohibited from using it for commercial purposes——

Mr. HUSE. Unless there is opt-in.

Senator FEINSTEIN [continuing]. With certain exceptions, and the exceptions are very carefully crafted.

Mr. HUSE. Right, and I think that is the right way to go.

Senator FEINSTEIN. You think that is the right way to go?

Mr. HUSE. I do, because I think that that forces a positive act on the part of anybody who wants to engage in commerce to get your permission. I think that part of the victim violation here is that none of us have any control over this.

Senator FEINSTEIN. In the legislation as it is drafted, and I believe this is correct, permission isn't part of it with respect to the Social Security number.

Mr. HUSE. No.

Senator FEINSTEIN. It is, with consent. I beg your pardon.

Mr. HUSE. That was my understanding.

Senator FEINSTEIN. You were right. I was wrong.

Mr. HUSE. That is OK. You are there and I am here. [Laughter.]

Senator KYL. If they only knew how frequently we were wrong. [Laughter.]

I think they do know.

Senator FEINSTEIN. I think they do, too.

Ms. BERNSTEIN. Your secret is safe with us, Senator.

Senator KYL. Us and C–SPAN, right?

Ms. BERNSTEIN. Yes.

Senator FEINSTEIN. In any event, with Senator Kyl's enormous help, we may just be able to move that legislation.

Mr. HUSE. I think it is really important, I do. It would be a tremendous step forward.

Senator KYL. Can I interrupt?

Senator FEINSTEIN. Yes, please.

Senator KYL. I have also been curious, though, about the need. If we are going to do this, which seems to me a very big step in the right direction, as you point out, don't we also need to make the Social Security card itself as counterfeit-proof as possible, and what is your view with respect to that? Obviously, if you protect against one type of theft but it is very easy to steal it in another way, then you simply move the people from type A to type B crime.

Mr. HUSE. The Senate has been focused on the Social Security card itself for some time, and the Social Security Administration has done an extensive study. There are implications, of course, of improving the current card to a point where it is more counterfeit-proof, and then we stray into an area of actually, again, *de facto* adding more underpinning to the use of the Social Security number as a national identifier.

That has policy implications that, you know, is a greater dialog than what we are talking about here.

Senator FEINSTEIN. Such as, for example?

Mr. HUSE. Well, if it becomes a national identifier, then we have a national identity card and——

Senator FEINSTEIN. But all he was saying is making it counterfeit-proof. All Senator Kyl was saying—we weren't getting into anything other than that. I mean, my Social Security number is on a little piece of cardboard, you know.

Mr. HUSE. Sure. But probably the folks who get a card today have—there have been improvements to that card over time. But as you add in more security features, then we need to add in a better business process underpinning that type of a card. There are tremendous costs involved to shift from the system we have now to one—would you add a photograph? I mean, there are all kinds of implications embedded in this that are a broader discussion.

I think it is a dilemma because we are crossing a line until this time we have never had to deal with in this country. But some of it is being driven by technology and it certainly is worthy of debate, but I don't have the answer right here.

Senator FEINSTEIN. I guess what I understand him saying is when you go into making it counterfeit-proof, you go into what you use to make it counterfeit-proof, which ergo expands its application into a more formal identifier than it is now. I mean, the number is effectively our national identifier.

Mr. HUSE. Right. It is the number, not the card.

Senator FEINSTEIN. But we don't have a national identification card, per se.

Mr. HUSE. No, but by adding this strengthened number to a better card, we are adding in the ingredients for something I don't know that you want, or maybe you do. We are right on the precipice here of an entirely different issue, and that is the conundrum.

Senator KYL. But we are there. I am not taking a position one way or the other, because we had this debate with regard to the Immigration Act and the possibility of a prototype. We had a couple of demonstration projects for the purpose for which Social Security is intended, namely indicating that you have a number and therefore you are permitted to work in this country. And even that raised huge questions.

But when we talk about opt-in and opt-out, what are we talking about? We are talking about opt-in and opt-out of allowing your number to be used for commercial purposes, OK? We are there, and so the fact that you make the card tamper-proof or fraud-proof doesn't force you to use it for commerce. It may make it easier to use for commerce, but that is again only if you agree that it be used in commerce, and you are already being asked whether you will agree to allow your number to be used in commerce. So we are there.

But, again, that is a subject with much larger implications than we intended to cover in this hearing. I appreciate your point about that, and I just asked the question for information purposes and I think at some point maybe it would be worth exploring further.

Mr. HUSE. Adding any kind of security features to the card, of course, makes it a better—we are in a better place enforcing the law. I mean, I can give you a simple answer to that, too.

Senator KYL. It doesn't, of necessity, take you into commercial uses. It simply makes it a better product for commercial use. Is that correct?

Mr. HUSE. Yes, Mr. Chairman.

Senator KYL. Anything else for this panel?

Senator FEINSTEIN. No, Mr. Chairman.

Senator KYL. I know we need to move on to the next panel, so I want to thank both of you again. You have been tremendously helpful. We really appreciate your testimony.

Mr. HUSE. Thank you.

Senator KYL. I was just trying to determine here a proper order, and I think just for ease of doing it, if we would start with Ms. Michelle Suzanne Brown and just move down the table this way, Beth Givens next, Steve Emmert, and then Stuart Pratt, that will make an easy transition from one to the other. I want to thank each of you for being here today as well. We really appreciate your willingness to share your experiences with us and we look forward to your testimony.

Michelle Suzanne Brown, why don't you begin?

PANEL CONSISTING OF MICHELLE BROWN, IDENTITY THEFT VICTIM, LOS ANGELES, CA; BETH GIVENS, DIRECTOR, PRIVACY RIGHTS CLEARINGHOUSE, SAN DIEGO, CA; STEVEN M. EMMERT, DIRECTOR, GOVERNMENT AND INDUSTRY AFFAIRS, REED ELSEVIER, INC., AND LEXIS–NEXIS, AND PRESIDENT, INDIVIDUAL REFERENCE SERVICE GROUP, WASHINGTON, DC; AND STUART K. PRATT, VICE PRESIDENT, GOVERNMENT RELATIONS, ASSOCIATED CREDIT BUREAUS, INC., WASHINGTON, DC

STATEMENT OF MICHELLE BROWN

Ms. BROWN. Thank you, Senator Kyl, Senator Feinstein. If I could ask one thing before I speak, I have one request. If we could redact my middle name from anything of record, is that a possibility?

Senator KYL. Absolutely.

Ms. BROWN. I don't know where that came from, but I appreciate that to be suppressed.

I am pleased to be in your presence today, and I genuinely thank you for the opportunity to elevate the invasive crime known as identity theft. This is a topic, unfortunately, that I am intimately familiar with.

My name is Michelle Brown. I am 29 years old and have been working in the international banking field for the last 7 years. I am an ambitious and hard-working individual. I am certain that I much like any of your cousins, your nieces, your daughters, your sisters. I believe that I strongly represent any average, respectable citizen of the United States.

However, there is one clear-cut issue that separates me from nearly the rest of the population. I have lived and breathed the nightmare of identity theft. I will tell you firsthand this is a devastation beyond any outsider's comprehension, a nearly unbearable burden that no one should ever have to suffer.

Imagine establishing credit at age 17 and building a perfect credit profile over the next 11 years. Imagine working consistently since age 15 and helping to finance your education at an accredited university to advance your future success in life. Imagine never having been in trouble with the law.

Now, imagine the violation you would internalize as you realize some vile individual you have never met nor wronged has taken everything you have built up from scratch to grossly use and abuse your good name and unblemished credit profile. That is precisely what happened to me.

I discovered this new, blackened reality on January 12, 1999, when a Bank of America representative called me inquiring about the first payment on a brand new truck which had been purchased just the previous month. I immediately placed fraud alerts on my credit reports, canceled all credit cards, and even placed a fraud alert on my driver's license number. From that day forward, I unearthed the trail of this menace's impersonation, and attempted to work with a current faulty system to protect myself from any further abuse. The system clearly failed me.

To summarize, over a year-and-a-half, from January 1998 through July 1999, one individual impersonated me to procure over

$50,000 worth of goods and services. Not only did she damage my credit, but she escalated her crimes to a level that I never truly expected. She engaged in drug trafficking. This crime resulted in my erroneous arrest record, a warrant out for my arrest, and eventually a prison record, when she was booked under my name as an inmate in a Chicago Federal prison.

The impersonation began with the perpetrator's theft of my rental application from my landlord's property management office in January 1998. Immediately, she set up cellular telephone service, followed by residential telephone and other utility services, and attempted to obtain time-share financing and department store credit cards. She was successful in purchasing a $32,000 truck, had nearly $5,000 worth of lyposuction performed to her body, and even rented properties in my name, including signing a year lease.

Not only did this person defraud the Department of Motor Vehicles by obtaining a driver's license with my name and number in October 1998, but she even presented herself as me with this identification to the DEA and before a Federal judge when she was caught trafficking 3,000 pounds of marijuana in May 1999. She remained a fugitive for almost 6 months while still assuming my name, and was finally turned in by an acquaintance in July 1999.

Months later, after she was already in prison, in September 1999, I was stopped at LAX Customs after returning from a vacation in Mexico. While I explained my innocence to several agents in a stream of tears, and as I attempted to clearly distinguish this Michelle Brown from the other Michelle Brown with a criminal record, I was blatantly treated with strong suspicion. I was, as is typical for an identity fraud victim, guilty until proven innocent. I was finally let go after an hour, after the police were called to vouch for me.

This situation reinforced my fear that I may be wrongly identified as the criminal, which could end with my arrest or, worse yet, being taken into custody and serving time in jail. After having seen so many inefficiencies and blatant errors in the system, I feel no assurance, nor can I receive any concrete evidence from authorities that this type of insane mix-up would never happen again.

It was tormenting to know someone was, in essence, living the good life at my expense, and I was left with the taxing chore of proving my innocence. The restoration of my credit and my good name was a seemingly never-ending process. I was forced to make literally thousands of phone calls, fill out various forms, submit all sorts of documents, and have many documents notarized.

Without a doubt, I was entirely consumed with the whole painstaking process. I gained nothing from putting over 500 hours into the chore of restoration. All in all, it was an exhausting waste of a good person's time and a massive drain on my life and energy. At one point, I even feared for my safety after I learned that the perpetrator had been linked with a convicted murderer. The whole identity fraud experience was by far the darkest, most challenging and terrifying chapter of my life.

I faced many difficulties in clearing my name, and I still face the fear that I will forever be linked with her criminal record. I have encountered widespread inefficiency and general insensitivity at nearly every turn. I know that there are most definitely not enough

dedicated resources and governmental authorities to assist victims and to simplify the burdens on the innocent's life.

Clearly, changes need to be made. The Government not only needs to promote initiatives to shorten and simplify restoration of one's name and credit, but also to facilitate early detection and termination of an abused person's name, and most importantly to deter criminals from the allure of such an easy crime by enforcing swift and severe punishment.

I think that Senator Feinstein's Identity Theft Prevention Act of 2000 is definitely a positive initiative and will put the legislation in the right direction to fight this crime. I support the two corresponding bills and recommend the enforcement of such initiatives.

I came here today because I feel responsible to limit the abuse of other victims' names. I know how terribly tormenting it is to be a victim. I am living proof that identity theft is a very real crime with very real victims and true life-altering consequences. It is astounding that my life-long discipline to be a law-abiding citizen and to have the diligence to establish perfect credit was reversed so easily, so quickly, simply because I represent the perfect victim in another's eyes.

This crime is clearly on the rise, and no one at this time is completely protected from becoming the next victim. I realize the scenario of becoming an identity fraud victim seems entirely farfetched and implausible to many of you. I know the feeling; I was once in your shoes.

I thank you for your time and for the opportunity to present my story and views today. I hope it is clear now that many changes need to be effected to the current system to combat this crime and protect victims. This fact is crystal clear in my mind.

Thank you.

Senator KYL. Ms. Brown, thank you very, very much for your testimony. It is compelling and we appreciate it very much. It is precisely the kind of sacrifice that you have made to come here that will help us to prevent this happening to other people, and you are to be commended for it. Thank you.

Ms. BROWN. Thank you.

[The prepared statement of Ms. Brown follows:]

PREPARED STATEMENT OF MICHELLE BROWN

Mr. Chairman and Members of the Committee, it is my pleasure to submit testimony to your committee today and hope that my presence will shed some light on the invasive crime known as Identity Theft.

My name is Michelle Brown, I am 29 years old, and currently reside in a respectable community in the surrounding area of Los Angeles, California. I have been gainfully employed in international banking for the last 7 years since my graduation from a University in California. I am much like most other hard-working, conscientious individuals, eager to get ahead in life and to make a respectable living; however, one thing clearly sets me apart from the rest of the crowd. I have endured the trying chores of realizing that I have become, and subsequently, have been painstakingly trying to break free from being, an identity fraud victim.

It was a scenario I had only previously known through unbelievable stories painted in Hollywood: someone becomes you, erases your life, and through their destructive behaviors, complicates your own existence to an extreme level where you no longer know how to just live day after day. Your life becomes the life consumed by unraveling the unthinkable acts that your perpetrator has done in your perceived skin.

I discovered on January 12, 1999, the existence of this shadow identity that I have been anxiously trying to expel from my life ever since. To be truthful, I don't think I will ever be able to close the books entirely on this menace's activities. I dearly wish I could, but what I know now translates to the fact that I will always be dealing with this alter reality I am plagued with.

Over the course of a year and a half, my name, personal identifiers and records were grossly misused to obtain over $50,000 in goods and services, to rent properties, and to engage in federal criminal activities—namely drug trafficking. During the course of 1999, I spent countless sleepless nights and seemingly endless days, dedicating my valuable time, energy, peace of mind, and what should have been a normal life, trying to restore my credit and my life.

I filed various statements and affidavits, had documents notarized, made thousands of phone calls to creditors, governmental authorities, etc., and continually set in motion the next level of protection for further follow up and monitoring. I alerted all the proper authorities, filed all the right papers, made the right phone calls, and diligently remained actively adamant to restore my perfect credit and my good name. I would estimate that the time lost toward clearing my credit, attempting to clear my criminal record, and to sever myself free from this menacing being, amounted to somewhere in excess of 500 hours of my time. At the time, the burden seemed like it cost me a lifetime.

In the course of restoring my credit and my name, I realized that I was victimized by someone without conscience. This person was not a normal, socially responsible individual and would stop at nothing. In restoring my name, I discovered the following about her and her fraudulent activities:

The perpetrator: Heddi Larae Ille, is currently 33 years old, and thankfully, is serving both state (2 years) and federal (73 months) prison time for illegal acts she performed while assuming my name. She is a Caucasian female, standing at about 5 foot 7 inches, weighing about 200 pounds, brown hair, and brown eyes. I am Caucasian, height 5 foot 9 inches, weight 125 pounds, brown hair, hazel eyes. I believe we look nothing alike in physical appearance.

January 1998: Just after I filed an application to rent a property, the perpetrator stole my rental application from my landlord's property management office. She apparently was at one time an acquaintance of my landlord's; to this day, I still have never met her and do not know her in any fashion.

February 1998: Heddi set up a wireless telephone service at my then current address, and quickly switched the address within less than a week. After 3 weeks, Pacific Bell deemed this account as fraud and disconnected the service. Due to their fraud determination, this account was never alerted to me.

March 1998: Heddi set up residential telephone service at a property in L.A., which remained on for about 4 months; $1,443 remained late and unpaid, therefore the service was finally shut off. This account eventually hit my credit report in the form of a credit inquiry through a credit bureau. [Of note, I simultaneously had telephone service in my name for years non-stop through the same provider (GTE); even though Heddi established the service through the same provider, with my name, Driver's License Number, and Social Security Number, I was never alerted of this new account, nor was this account cross-referred to mine, even as it was in serious delinquency.]

July 1998: Heddi attempted to obtain timeshare financing. The application was never activated, and when I spoke to the timeshare financing company, they did not have a "Fraud" division set up and could not tell me what happened with the application. I was later informed that she was required to serve 45 days in jail (on a separate fraud charge) shortly after the application was filed; likely this is the reason nothing had been pursued.

July 1998: Heddi attempted to get a credit card through Target (a "home/everything" type store); the application was denied.

August and September 1998: Heddi served 45 days in jail.

October 1998: Heddi got a duplicate drivers license at a Fullerton, CA Department of Motor Vehicles, in my name, my drivers' license number, but an alternate address, and with her picture. The DMV issued the duplicate, even though at the time, she weighed 40 pounds more than me and was two inches shorter, and completely different in physical appearance. The requirement of her fingerprint enabled the authorities to clearly distinguish our different identities and made things much easier for me to clear my credit, and to clearly establish the fact that I was the victim of identity fraud and impersonation.

October 1998: Heddi rented a property in San Diego, CA, in my name, set up utilities, and shortly thereafter vacated.

October 1998: Heddi signed a year lease at another property in San Diego, in my name.

December 1998: Heddi filed applications for and received the following: a $32,000 2000 Quad Cab D2500 Dodge Ram Pick-Up (zero down lease), and $4,800 worth of liposuction in Long Beach, CA (she paid $1,400; the rest was financed through a line of credit established in my name).

January 12, 1999: I received a message at home from a Bank of America representative inquiring about the new Dodge pick up. I returned the call to tell them they had the wrong person and I knew nothing of the truck. They explained they must have the wrong Michelle Brown, all the numbers listed on the application were not working, and a previous address was listed in my city; so they reached me via my 411 listing. I asked them for the SSN to ensure it wasn't mine, they couldn't release it; I gave them mine and they told me that was in fact the one used on the application.

January 12, 1999: I instantly put fraud alerts on all credit reporting agencies, filed a police report, cancelled all of my credit cards, put heightened security on all bank accounts, called the DMV to find out if a duplicate drivers license was issued (it had been) and subsequently put a "pink flag" fraud alert on my License number. Subsequently filed another local police report, called the Postmaster, Social Security Agency, U.S. Passport Agency, etc., and the nightmare continued with each and every passing day.

Mid-January 1999: The Police Detective I was working with gets her pager number, pages her, and has a conversation with her. After she identifies herself as me when she returned the page, he tells her he knows that she really is Heddi Ille, and to turn herself in the next day. She agrees. Two subsequent times in the next week, she requests more time to turn herself in. Within the next week, the Detective issues a warrant out for her arrest and attaches required bond set at $750,000.

May 1999: Heddi is arrested in Texas for smuggling 3,000 pounds of marijuana, she identifies herself as me to the DEA and to a federal magistrate. The arrest is recorded in my name, "I" am subsequently named in the criminal complaint, and listed as the DEA's informant. She was somehow set free even though my name and Drivers' License number was flagged with fraud since January 1999. I know nothing of her criminal activities at this time.

June 1999: Through my landlord's property manager, I was told that they heard through one of Heddi's acquaintances that there was a warrant out for my arrest somewhere in Texas. Since I was going out of the country on vacation within 2 weeks, I asked the detective to write a letter explaining the circumstances and my innocence. I also had the police run my information in databases to tell what city/county the warrant was in, and tell me how to clear it prior to my vacation. No positive responses were found; I assumed it was a local county warrant—it was a federal felony warrant as I found out in July when she was arrested.

July 1999: Heddi called an acquaintance of hers while she was in a suicidal state, and they turned her in. She identified herself as me even still as the police came to her hotel door. She was found with drugs in her possession, credit cards that had been melded down and re-imprinted with my name, and her CDL in my name. She was brought in on 13 criminal counts.

September 1999: Returning from a trip to Cabo San Lucas, I was held at LAX's Customs and Immigration for an hour while I explained the circumstances of my erroneous link with her criminal record (after my passport was swiped in the computer). As I presented endless documentation of court records, police filings, etc., and explained my situation in a stream of tears, I knew then that I had become erroneously linked with Heddi's criminal record. The agents questioned my story and documentation, and treated me very suspiciously—like I was the criminal. After the Police Detective was called and vouched for me, I was allowed to leave. I feared being arrested or being taken into custody. I found out later that, even though Heddi had already been in police custody at a jail since July, the DEA posted a lookout for "me" in the system. They neglected to let me know that I might want to be prepared for this type of confusion at any time.

September 1999: Heddi is convicted of 3 felony counts (perjury, grand theft, and possession of stolen property) at the state level at 2 years each, which she is serving simultaneously. Note that the specific charge for identity theft/impersonation was not a charge that she was actually convicted of.

October/November 1999: Heddi is transferred to the Chicago Federal Prison and they book her as an inmate in my name. She even addressed outgoing letters from the Federal Prison using my name in the return address. Needless to say, I was furious. When I called the DA, they told me they would have this corrected. I was told subsequently that it was corrected; however, they could never provide me proof of this in writing as I requested.

June 2000: Heddi is sentenced to 73 months in federal prison for possession with intent to distribute 3,000 pounds of marijuana, with an enhanced sentence for lying

to a federal magistrate. She received a reduced sentence from the pre-determined 110 months because she provided assistance to the government. [I believe she was tied to a major drug smuggling ring. Even though my name was used, I was never privy to details of her crime; however, I was informed that there were several defendants in this case.]

Through the course of uncovering her trail and waiting for her to be caught, I honestly believed that the victimization would never end, that I would never become whole again as the true "Michelle Brown." My world had become a living nightmare. I personally was affected extremely: I was significantly distracted at a job that I had just started three weeks prior to the day of discovery, I suffered from a nearly non-existent appetite, very little sleep, and was consumed with the ferocious chore of restoring my name and attempting to quell any future abuse. I lost identification with the person I really was inside and shut myself out of social functions because of the negativity this caused on my life. I know that a very meaningful 3 year relationship with my then boyfriend suffered dearly because of the affect this traumatic chapter of my life had on me—the relationship ended about 4 months later.

No words will ever be strong enough to completely convince others what this period was like, filled with terror, aggravation, unceasing anger and frustration as I woke every day (since my discovery of the identity fraud in January 1999) with emotionally charged, livid angst. I unceasingly was forced to view life through a clouded reality, one seriously altered by a horrendous individual who committed a series of unforgivable acts in my name. The existence of Heddi has robbed me of the normal life I have strived for and entirely deserve. My life should be one in which I, and I only, should be the only one being held responsible and accountable for my personal credit history and what should be, a lack of a criminal history.

For me, the most personally frightening moment was dealing with LAX's Customs and fearing an erroneous arrest. Because of this situation, I purposely have NOT gone out of the country for fear of some mishap, confusion, language barrier, that may land me in prison for some unknown period of time. I do not deserve to be in this predicament and do not deserve to feel imprisoned by the U.S. Borders. I still fear what might happen as I cross the U.S. Border and I cannot get assurance from any governmental agency that this situation will never happen again.

Identity fraud (especially those cases escalated to a criminal level) leaves a very dark and filthy cloud around the victim. Although I am the free Michelle Brown, living what may on the surface seem to be a normal life with freedom on the streets, I have never deserved less than that: a normal life, one free of the ill effects of a heinous individual who deliberately and unabashedly used and abused my world that I had always been so careful to create and maintain. I am a law-abiding, good natured and caring individual, contributing through legitimate business and upstanding citizenship, who never deserved to be haunted with this naggingly irritating air Heddi has shadowed me with.

Clearly many preventive measures and protective procedures need to be enforced to prevent such a horrendous crime from being so easy and attractive for a perpetrator to facilitate. Below I've attached a list of items highlighting some of the weaknesses I see with the current system.

I thank you for your time and consideration and hope that my case can provide you with the awareness that this is truly a real crime, with real victims, and dire life-altering consequences attached.

ATTACHMENT 1

During the course of the restoration of my credit and my personal records, including criminal associations, I can identify the following faults in the current system:

There should be a better system to clearly verify the innocent's residency for the past.—Creditors and the credit reporting agencies require various statements to prove residency over the course of time (when services were actually established). The types of documents they require as proof(s) of residency were rarely consistent with each other. Additionally, most people do not keep old statements. How is one to prepare for the occasion that you would have to prove residency for any time period? I happen to keep all of my old credit card statements, some utility bills, and most phone bills which allowed me to provide sufficient documentation. I doubt the common citizen retains the same level of credit card statements, utility bills, etc.

There should be a standardized form that would suffice to send to all parties that were victims of extending credit, extending identification/documentation of identity (Department of Motor Vehicles for licenses, passport agencies), and reporting on these items (credit reporting agencies).—To clear fraudulent items, I was asked to fill out various forms from one creditor to the next, which is very time consuming.

Credit restoration (at the credit reporting agencies) is rarely timely, efficient, or effective.—Even though the fraudulent accounts were erased from my credit reports, some items mysteriously resurfaced months later. Also, several fraudulent inquiries still remain on my Trans Union report despite repetitive efforts with both the creditors and the credit reporting agency to clear these items.

Credit Monitoring Services should be provided free to victims of identity fraud for several years.—I still need to monitor my credit even though the perpetrator is in prison (she could use it again or could have sold it off, etc). I continually call to ensure that neither new inquiries nor accounts have been opened fraudulently. I also need to ensure that my fraud statement remains attached to each credit report. Many victims are re-victimized after the fraud alert expires on their credit reports. This will always be a necessity despite the appearance of a fraud alert tagged to each of the three credit reporting agencies' reports, especially in the event a merchant does not comply with the fraud instructions to contact the victim telephonically.

Identity fraud victims should always be able to speak to a live person at the credit reporting agencies.—As the attachment of a fraud alert if the first level of prevention once someone has learned of their victimization, it is a necessity to attach this as soon as possible. This was the first means of comfort to me that I could take this measure and discuss my situation with someone more familiar with the situation. However, in subsequent calls to the credit reporting agencies, I had discovered that often the call went straight to an automated call receipt system with inadequate options. It would have been quite unnerving if my first call to alert them of fraud had been funneled to an answering machine where you are asked to leave your name, number, social security number, etc., rather than speaking to a live individual who can better instruct you and understand your crisis.

Authorities are not always sensitive to this type of crime.—When I spoke to an LAPD, I was told blatantly not to file a report in their office because they didn't want such an enormous case on their hands. The DMV was also not sensitive to my case and was in fact accusatory: they suggested that I was lying about someone getting a duplicate CDL in my name, despite the fact that I had just spoken with another employee who verified this for me. I was guilty until proven innocent—like most identity fraud victims are treated time and time again.

In each Police Department, there should be an established Task Force to which calls of Identity Fraud nature should be referred, where expertise in this arena and sensitivity to the victim would be highly appreciated.—On filing my first police report, I was told to file a report in the county where the crime was committed. The first thing I was alerted to was the truck purchase, which took place somewhere over 100 miles away from me in San Diego. Additionally, the officer I initially spoke to in San Diego mistakenly thought that I should collect all of the necessary paperwork and bring it to the San Diego Police Department. Not only would this have been a major inconvenience, but legally, I did not even have access to this "proof:" the application for the $32,000 loan, copies of the perpetrators' drivers license, etc. My feeling is that Law Enforcement Officers are not trained to handle these types of calls and do not know the procedures.

The fraud alert posted on my driver's license in January 1999 obviously was not effective: either the various systems should be able to share this information across the state borders, or the DMV should be more careful about what they are telling victims.—What I understood created a false sense of security for me. Had this fraud alert worked, I would not be linked with: the perpetrator's arrest record, the criminal complaint, the warrant out for her arrest, nor would I have been detained at LAX's Customs and Immigration.

There are neither enough resources nor expertise dedicated to this crime in general, and government information sharing across state lines is poor.—I was highly frustrated by the length of time it took to finally catch Heddi; when she was finally taken into custody, it was not because of the diligence of the police, it was because she was turned in. Also, it amazes me that she was actually arrested in Texas in my name, taken into custody, and released even though California records were flagged to show that someone was using my name and to be on the look out. Clearly the current system and procedures failed horribly and are not adequate at this time.

There need to be clear cut procedures and evidence provided to the victim to break a victim free of an impersonator's crimes.—Authorities cannot provide assurance that I am now cleared of hassles with the law, Customs/Immigration, etc. In fact, I am told that I will always be linked with Heddi's criminal record because I'm her A.K.A, meaning that I will likely be questioned any time that my name and identifiers are run in government systems. This is an enormous, haunting burden on a victim, who has clearly already suffered enough. I believe the government does not have solid procedures on how to de-link a victim from its perpetrator, and they are

uncertain of the flow of information. I feel like I'm testing the system as if I'm walking through a minefield.

Finally, there should be severe consequences to the perpetrator of such crime.—Although my perpetrator is currently serving prison time, she was never convicted of the identity fraud felony count. Her other crimes carried more weight over the one most personally offensive and life altering to me. I would recommend to impose a $5,000 fine to anyone who steals another's identity, and require that this be paid to the victim within 2 years of conviction.

Additional recommendations, while not directly applicable to my case, would help prevent the extent of fraudulent activities:

Social security numbers should be treated as confidential information, and therefore should not be required to be part of passwords, medical identification numbers (this is usually clearly stated of medical cards which should be carried at all times by the insured), etc. Additionally, there are NO situations in which SSN's should be sold.

Credit issuers: all duplicate card requests should be verified by a mailer to the previous credit card address, or verified via telephone.

Credit issuers: change of address requests should be followed up with a level of verification. Possibly there could be a better communication system between the Postmaster, and credit reporting agencies and creditors, to verify that authentic address changes have been made.

Credit issuers: many unauthorized charges to a credit card holder are facilitated by shipping goods to an alternate address.—Any items billed to a credit card and shipped to another address should be subject to the same verification/authentication requirements as if the creditor were discussing private account information with the card holder. Further, as the shipment is requested, the credit card holder should be informed in writing of the shipment, including the address to which the item was billed.

Credit reports should be offered free to individuals at least once a year, at their request.

Unusual inquiry/account opening behavior should be flagged at the credit reporting agencies and further investigated.—The bureaus should take more responsibility for unusual activity as they are the first ones to be alerted of consolidated fraud on one individual's record.

Fraud alerts should be CLEARLY POSTED on the first page of victims' credit reports. Further there should be fines imposed to merchants who do not properly act on these statements and fail to verify the authenticity of an application.

Senator KYL. Beth Givens.

STATEMENT OF BETH GIVENS

Ms. GIVENS. Chairman Kyl, Senator Feinstein, thank you for the opportunity to testify today. I am Beth Givens, director of the Privacy Rights Clearinghouse, a non-profit consumer group in San Diego. We have been assisting victims since 1993 and we have witnessed the ravages of this crime on the victims and their families, and I commend you today for focusing on victims and on prevention.

In May, the Privacy Rights Clearinghouse and CALPIRG, another non-profit, released a survey on identity theft victims who had contacted us for help in the past, and here is what we learned.

On average, it took them 2 years to clean up their credit report and to regain their financial health. Many were still dealing with it after 4 years. Victims found that they spent an average of 175 hours to resolve the problem. That is the equivalent of 4 working weeks, and many were spending over 500 hours.

When victims are asked what would have prevented their identities from being stolen, most, including those we surveyed, said take the Social Security number out of circulation so it can't be obtained by criminals. It certainly should not be used as an ID for insurance companies, by universities and others, and it certainly should be not for sale on the Net. I am pleased that 2328 and 2699 have been

introduced because I think they address the prohibition of the sale of the Social Security number.

Victims also State that the credit issuers need to be more effective in weeding out fraudulent applications, especially in instant credit situations. Half of the victims in our survey told us that the fraud recurred after they put a fraud alert on their credit report, and I am also pleased that 2328 addresses that.

Victims have also stressed that early detection of fraud would have greatly shortened the time needed to regain their financial health. Our survey found that the average time it took them before they even learned they were a victim was 14 months after the fraud had begun.

What about victim assistance? It is now much improved since the Federal Trade Commission has opened its identity theft clearinghouse, thanks to the bill that was passed last year, your bill, Senator Kyl. But the credit bureaus and credit issuers must improve their victim assistance tremendously. This includes providing live staff members rather than voice mail and long waits, and also the industry must develop fool-proof methods to prevent fraud from recurring once a fraud alert has been established. The Associated Credit Bureaus' efforts, I think, are moving the industry in the right direction.

In closing, I want to bring to your attention to what I call the worst case scenario of identity theft, and that is when the imposter commits crimes using the victim's identity, like we heard from Michelle, giving that person a criminal record. These records are extraordinarily difficult to clear up. Victims may be unable to find work. They live with the constant fear of being arrested at any moment. Many of them have been jailed.

They must carry with them a document from either law enforcement or the courts, and they must carry it all times, that is if they are fortunate to even get such a document. This would be a letter of clearance. They face a lifetime of being burdened with someone else's criminal record.

Now, with that, I close. I do wish to present the committee with our identity theft survey, also with a documentary about some California identity theft victims that was made by a victim herself.

[The documentary will be retained in committee files.]

I thank you again for the opportunity to testify on behalf of consumers and on behalf of the identity theft victims.

Senator KYL. Thank you very much for your important work, and we will be very pleased to accept that material for the record of the hearing and try to promote its viewing by others as well.

[The prepared statement and information referred to of Ms. Givens follow:]

PREPARED STATEMENT OF BETH GIVENS

The Privacy Rights Clearinghouse is a nonprofit consumer information and advocacy program based in San Diego, California. The PRC was established in 1992. We have been assisting victims of identity theft since 1993, when we first started learning about this crime. Our guides for identity theft victims can be found on our web site at www.privacyrights.org. I estimate that I have assisted at least 4,000 victims of this crime, and that others on our staff have assisted many thousands more over the years.

I appreciate the ability to provide written and oral testimony on the skyrocketing crime of identity theft, its impact on victims, and possible solutions. And I commend

you and the Subcommittee members for addressing this issue. My written testimony is in four parts.

- Topic number one is the crime itself—what is identity theft, how much of it is going on, and why is it happening in epidemic proportions.
- Second, I will discuss the many ways in which identity thieves obtain the bits and pieces of information they need to impersonate others—mainly Social Security numbers (SSN) and credit card account numbers.
- Third, I will explain some of the impacts on victims.
- And fourth, I will recommend legislative and industry measures to prevent identity theft and to expedite the ability of victims to regain their financial health.

First, what is identity theft? There are numerous variations of this crime. Essentially, it occurs when someone uses bits and pieces of information about an individual—usually the Social Security number—to represent him or herself as that person for fraudulent purposes. Examples are obtaining credit cards and loans in someone else's name and then not paying the bills, opening utility accounts, renting an apartment, getting a cellular phone, purchasing a car or a home, and so on. Another type of identity theft—what I call the worst case scenario—is when the perpetrator commits crimes in the victim's name and gives that person a criminal record.

Victims are not liable for the bills accumulated up by the imposters, thanks to federal law. But they do have the anxiety and frustration of spending months, even years, regaining their financial health and restoring their good credit history.

How many victims of this crime are there? We don't have accurate statistics. But I estimate that there are 500,000 to 700,000 victims this year. A 1998 report by the U.S. General Accounting Office tracked identity theft statistics from 1992 to 1997, based on figures provided by the Trans Union credit reporting agency (CRA). A graph on page 40 shows a dramatic 16-fold increase in the volume of calls from individuals to Trans Union's Fraud Department during the six-year period from 1992 to 1997. Trans Union now receives well over 2,000 calls a day from victims of identity theft. [U.S. General Accounting Office, *www.gao.gov,* "Identity Fraud," Report No. GGD–98–100BR, 1998, p. 40]

Why are these figures significant? When individuals learn they are a victim of this crime, the first step they should take is to contact the three bureaus and place a fraud alert on their file. The CRA's are Trans Union, Equifax, and Experian (formerly TRW). Therefore, the number of calls received by the CRA's fraud departments is a good indicator of the volume of this crime.

Why is this crime so rampant today? It is very easy for the criminals to obtain the information needed—in particular, Social Security numbers. Non-Social Security Administration uses of the SSN have not been prohibited by law, at least not to date. As a result, SSN's are used as identification and account numbers by many entities—insurance companies, universities, cable television companies, military identification, banks, securities brokerage companies, and the like. In about a dozen states, the SSN is used as the driver's license number.

Identity thieves can obtain SSN's by stealing mail where those numbers are included. They sift through the trash outside of businesses and residences in hopes of finding unshredded documents containing SSN's and other data. Dishonest employees can obtain SSN's in the workplace by obtaining access to personnel files or accessing credit reporting data bases (commonly available in auto dealerships, realtors' offices, banks and other businesses that approve loans).

Another reason identity theft is rampant is because of credit industry practices. Credit grantors make it all too easy to obtain credit. Many credit issuers do not adequately check the identities of applicants before granting credit. Instant credit opportunities are especially popular with identity thieves for this reason. Credit grantors are all too eager, in their competitive zeal, to obtain new customers. It is not uncommon for households to receive several pre-approved offers of credit per week. In fact, a *Los Angeles Times* news story reported that credit issuers mailed 3.4 *billion* pre-approved offers of credit to consumers in 1998. ("Charges are flying over credit card pitches," by Edmund Sanders, *Los Angeles Times*, June 15, 1999, p. D–1. *www.latimes.com*).

Another reason identity theft is skyrocketing is that it does not yet get the attention of law enforcement that more violent crimes receive—like breaking and entering, mugging, robbery by gunpoint, and bank thefts. Many violent criminals and organized crime rings are moving to identity theft because they know that law enforcement resources are not yet sufficient to investigate the majority of such crimes. Identity thieves are rarely apprehended and sentenced. If they are, penalties are minimal and rarely include jail time. Community service and parole are the usual sentences.

My second topic is the methods used by identity thieves to obtain identifying information about their victims. Typically, they obtain the Social Security number and name. That's often all that is needed to apply for credit (called "application fraud"). They also might obtain credit card numbers and hijack existing accounts (called "account takeover). Other pieces of information useful to identity thieves are dates of birth, mother's maiden name, and driver's license numbers.

• One such method is the old fashioned way—by stealing a wallet or purse. The thief either uses the information obtained or provides the contents to a crime ring. Even if the individual does not carry the Social Security card in the wallet (and we recommend that they do not), he or she might have an insurance card or student ID with that number on it.

• Another strategy is to fish credit card slips and loan or credit applications from the trash. Unfortunately many businesses, banks, mortgage companies, and restaurants do not shred these documents.

• We are seeing an increase in the "inside job" in the workplace—dishonest employees with access to computer terminals connected to one of the credit reporting agencies. They might look for names similar to theirs, or just someone with good credit. Obviously what goes hand in hand with this type of access is the negligence of the company which is permitting such uses in an unmonitored environment.

"Insiders" have also used their access to personnel records to obtain Social Security numbers of identity theft victims. In a recent case in San Diego, a dishonest employee had unfettered access to a storage room where past payroll information was filed. She obtained SSN's of over 100 current and former employees and used them to obtain credit in their names.

We learned of a case where a member of a Nigerian crime ring was employed temporarily at a very large corporation. He downloaded the employee list containing SSN's and then one by one the employees' identities were used for fraudulent purchases. The employees didn't know about it until they started sharing stories and learned that many of them had been hit. It wasn't until much later that the human resources department confessed that they had known about the theft, but they didn't want to tell the employees and cause them to panic.

• Sadly, some identity theft is perpetrated by relatives or friends, roommates, household workers like health care givers, and spouses going through a divorce who have a grudge. These individuals obtain Social Security numbers, driver's license numbers, and credit card numbers by having access to their personal effects.

• Mail theft is another way of obtaining identifying information, as mentioned above. We urge people not to leave their paid bills out at the mailbox for the carrier to pick up. It's better to drop them off at the Post Office. There's also insider mail theft, where credit card mall is stolen from the mail processing areas by postal employees.

• Then there's the change of address routine. The thief fills out a change of address card so the victim's mail is diverted to the thief's drop box. The thief obtains bank statements and credit card bills, monthly investments reports, and preapproved offers of credit containing the information necessary to impersonate the victim. The Postal Service has recently initiated changes to make this more difficult.

• Application fraud is another method. The imposter fills out a credit application—perhaps a pre-approved offer of credit retrieved from the trash—with the victim's name and identifying information and has the credit card mailed to another address. The major credit card issuers say they are now more wary of changes of address, but their efforts are not foolproof.

• The Internet is becoming a more popular resource for identity thieves. Yes, there are web sites that sell individuals' Social Security numbers. Visit *www.infoseekers.com* and *www.fastbreakbail.com* for example. Social Security numbers can be purchased for as little as $20. They are found in records called "credit headers" that are sold by credit reporting agencies to information brokers. Credit headers include name and name variations, current and former addresses, telephone numbers (including unlisted numbers), year and month of birth, and SSN. At this time, there are no restrictions on the sale of credit headers to information brokers. Consumers have no way to "opt-out" of the sale of their credit header data. The information broker industry adopted a voluntary privacy policy in 1997, but it has been ineffective in restricting the sale of sensitive personal information to the general public. (See the Individual Reference Services Group guidelines at *www.irsg.org.*)

• There are many more schemes. Most victims with whom we have spoken haven't a clue as to how their identifying information was obtained by the imposter.

My third topic is what happens to the victims of these crimes? Even though each identity fraud case is different, what happens to the victims is, sadly, all too similar.

• They get little to no help from the authorities who issued the identifying information to them in the first place.

• Law enforcement doesn't investigate many such crimes. There's just too much identity fraud occurring for them to handle all such cases, although the financial fraud departments of many police departments are being expanded.

Many police and sheriff's departments refuse to issue a police report to the victims. They claim that the banks and credit card companies are the real victims because they suffer the financial losses. Many victims find they need the police report to prove their innocence to the credit card companies and the check guarantee services.

• Many victims report they do not get effective help from the credit grantors, banks, and the CRA's. They describe difficulty in reaching the credit reporting agencies, and tell how they are treated disbelievingly by some creditors. Victims also report that flagging their credit report for fraud doesn't always stop the imposter from obtaining more credit.

Victims must also deal with abusive collection agencies. They are threatened with law suits, garnished wages, and having their homes taken away from them.

• Another common experience of victims is that they must spend a great deal of time cleaning up the mess. I've talked to many who are taking the day or the week off work so they can make the necessary phone calls, write the letters, and get affidavits notarized. This costs them money as well. Many victims are saddled with this situation for years.

In a recent survey we conducted with CALPIRG, we found the average amount of time spent by victims to regain their financial health was 175 hours. And those cases had dragged on for an average of two years, with many cases taking more than four years to be resolved. ("Nowhere to Turn: Victims Speak Out on Identity Theft." May 2000. *www.privacyrights.org/ar/idtheft2000.htm).*

• Victims are often scarred emotionally. They feel violated and helpless—and very angry. I've heard people use the word "rape" to describe how they feel. I've talked to many who are crying or close to it because they cannot stop what is happening to them, and no one else will either. I've talked with elderly people who are terrified of losing their life savings and their homes.

It's little wonder that victims feel violated, helpless and angry. They are unable to rent an apartment, get a job, qualify for a mortgage, buy a car, all because someone else's bad credit history is recorded on their credit report. Essentially the entire burden of this crime is placed on the shoulders of the victims.

• The worst-case scenario is when the thief commits crimes in the victim's name. We learned of a case where the imposter was a major drug dealer, using the identity of a high-tech company president. This man travels out of the country often and has to carry a letter from law enforcement which explains he is not the drug dealer, because he gets pulled into secondary inspection every time he comes back to the U.S. Recently law enforcement from another state, who had not read the entry on the FBI's NCIC crime data base completely, entered his bedroom in the early morning hours and tried to arrest him at gunpoint. He was able to convince them they were seeking the wrong person.

Another case that came to our hotline was an Hispanic man, a U.S. citizen, who was visiting relatives in Tijuana, Mexico, across the border from San Diego. He was taken into secondary inspection by U.S. Customs on his return trip to San Diego. A search of his SSN showed he was wanted for a crime in the Bay Area. He was transported from San Diego to San Francisco and put in jail. It took him 10 days before one of the officers believed him, took his fingerprints as he had requested all along, and realized they had the wrong person.

• Another worst-case scenario is when the imposter is working under the victim's name and SSN, and the earnings show on the victim's Social Security Administration record. We learned of one such a case that had been going on for 10 years. The imposter obtained the victim's birth certificate, a public record in California. And even when the victim acquired a new SSN, the impersonator was able to obtain it shortly thereafter. Victims of employment fraud often must deal with the Internal Revenue Service because IRS records show they are under-reporting their wages.

• Finally, in order for victims to extricate themselves from the identity theft mess they find themselves in, they have to be fairly savvy consumers. They must be assertive with the credit card, banking and credit reporting industries. They must be assertive with all kinds of other officials as well. I have talked with many consumers who are not equipped to deal with the challenges that this crime brings to them—individuals whose first language is not English, or those whose English language skills are such that they cannot communicate at the level of complexity that this problem requires. Those who are semi-literate or illiterate cannot write the nec-

essary letters. Unfortunately, there are not enough consumer assistance offices to help these people.

My fourth and final topic is legislative and industry solutions to the crime of identity theft.

The awareness of identity theft among consumers has skyrocketed in the past year—primarily because of media coverage. I think consumers are becoming much more wary of disclosing personal information and having it given out without their consent, especially on the Internet. These outcries by members of the public have resulted in some legislative attention brought to the issue, both on the federal level and in the states.

In 1998 Congress passed and the President signed the Identity Theft and Assumption Deterrence Act (18 U.S.C. 1028). It makes identity theft a federal felony when someone knowingly uses the identification of another person with the intention to commit any unlawful activity under federal and state law. Violations of this Act are investigated by federal agencies like the U.S. Secret Service, the FBI, and the U.S. Postal Inspection Service. Such crimes are prosecuted by the U.S. Department of Justice.

This new law allows for restitution for victims. It established an identity theft clearinghouse within the Federal Trade Commission. The FTC now offers a toll-free number for consumers to call, 877–IDTHEFT, as well as a web site, *www.consumer.gov/idtheft.*

In recent years nearly 40 states have criminalized identity theft. Most of them have made it a felony. A list of those states can be found on the FTC's web site at *www.consumer.gov/idtheft/statelaw.htm*.

On the one hand, I'm pleased that this crime has been criminalized by these new laws. But I believe that in order to make a dent in identity theft, the practices of the credit industry must change dramatically. Until laws create incentives for the credit industry to change how they do business, the crime of identity theft will continue to climb at epidemic proportions.

I am encouraged by the introduction of Senate Bill 2328 by Senators Feinstein, Kyl, and Grassley, titled the "Identity Theft Prevention Act of 2000." It places the emphasis on prevention where it rightfully belongs. The points that follow include discussion of the key provisions of S. 2328 (*http://thomas.loc.gov).*

Here are some suggestions for making credit industry practices more fraud-proof:

• A change of address is often an indicator of fraud. Simple steps by both credit grantors and reporting agencies in verifying address changes would greatly reduce fraud incidents. S. 2328 requires that if the card issuer receives a change of address notification, it must send a confirmation notice to both the new and former addresses. Further, if a card issuer receives a request for an additional credit card within 30 days of receiving a change of address, it must also notify the cardholder at the old and new addresses. Credit reporting agencies must notify credit issuers when it becomes aware that a credit application bears an address for the consumer that is different from the address they have on file.

• A penalty should be assessed whenever a credit grantor extends credit to an imposter after the victim has placed a fraud alert on the credit file (a provision of S. 2328).

• All consumers should be able to receive one free copy of their credit report annually (a provision of S. 2328). With more consumers checking their credit reports frequently, identity theft will be detected earlier and the impact will be minimized. Six states have passed such laws: Colorado, Georgia, Massachusetts, Maryland, New Jersey, and Vermont.

• Consumers should be able to notify the credit bureaus to put a "freeze" on their credit report—to prevent their credit report from being furnished without specifically authorizing the release. A Vermont law requires that users of credit reports obtain permission from the consumer prior to obtaining the credit report (Title 9 sec. 2480e at *www.state.vt.us.* Click on "Statutes Online"). In California, state Senator Debra Bowen's SB 1767 would adopt the Vermont "opt-in" model.

• Another important piece of legislation that needs to be enacted is a provision that takes the Social Security number out of circulation. A separate bill introduced by Senator Dianne Feinstein would prohibit the commercial sale of SSN's (Social Security Privacy Act of 2000). This measure would also limit uses of the SSN by private sector entities. Government agencies could not display the SSN on mailing labels and documents available to the public.

In California, a bill introduced by state Senator Debra Bowen during the 2000 session would prohibit the use of the SSN as an account or member number by such entities as insurance companies and universities. (SB 1767 can be found at *www.leginfo.ca.gov.* Click on "Bill Information.")

• Credit grantors should be required to verify at least four pieces of information—name, address, date of birth, SSN, driver's license number, and place of employment—with information on the credit report. This is especially important in instant credit situations. If the consumer is applying in person, the credit grantor must inspect a photo ID.

• As discussed earlier in this testimony, we consider the worst-case scenario of identity theft to be when the victim is burdened with a wrongful criminal record because of the activities of the imposter. This usually occurs when the imposter is arrested and released, perhaps for a traffic violation or shoplifting, and then does not appear in court. This results in a warrant for the arrest of the identity theft victim.

Victims of criminal record identity theft can find it impossible to obtain employment. Many have been jailed. It is common for such victims to be detained by U.S. Customs when entering the country after traveling abroad. They must carry a letter with them from law enforcement or the courts at all times in order to prevent wrongful detention. Such victims are faced with having their identity associated with a criminal record for the rest of their lives.

It is critical that legislation address the plight of such identity theft victims. There must be a way for them to learn that they have a wrongful criminal record. S. 2328 includes an excellent provision enabling individuals to obtain the content of information about them that is compiled by an information broker, employment background check service, or individual reference service. If erroneous information is compiled in a background check for employment or other purposes, it is essential that the subjects of those investigations know the exact information that has been disclosed and the source from which the information was obtained.

Individuals who have wrongful criminal records must also be able to clear such records through an expedited process involving the law enforcement agency that made the arrest, the court system where the warrant was issued, and the official criminal records data bases at the state and federal levels. At present, there is no such process easily available to victims of criminal records identity theft. You might want to read about such a measure currently being considered in the California legislature, Assemblymember Susan Davis's AB 1897.

Victims of criminal record identity theft must also be able to locate all the information brokers that have obtained the erroneous information so they can have those records cleared as well. One solution would be to develop a national registry of individuals who are victims of criminal record identity theft and require all entities who conduct criminal records background checks to access that data base before reporting the criminal records information. In California, Assemblymember Tom Torlakson's AB 1862 would call for the development of such a data base within the California Department of Justice.

Legislation is not the entire answer to the vexing problem of identity theft. The credit granting and reporting industries must step up their efforts to assist consumers in preventing fraud altogether and in recovering from identity theft. The Associated Credit Bureaus announced an identity theft initiative in March 2000 that would streamline fraud-handling by the credit reporting industry (*www.acb-credit.com)*. The ultimate goal of this endeavor should be "one-stop shopping" for fraud victims—a single phone call to launch the fraud clean-up process.

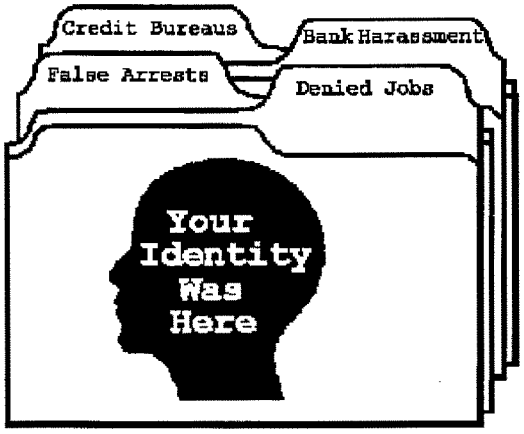
Both creditors and the CRA's should increase the use of artificial intelligence computer programs to identify patterns of fraud and to quickly notify consumers of suspected fraud activity. The May 2000 identity theft victims survey conducted by the Privacy Rights Clearinghouse and CALPIRG found that the average amount of time that had transpired before individuals learned they were victims of identity theft was 14 months. (*www.privacyrights.org/AR/idtheft2000.htm*). Yet, evidence of fraudulent activity can often be easy to detect—numerous inquiries on the credit report in a short period of time, changes of address, monthly credit account bills that are much higher than usual, many late payments when the individual had none previously, and so on.

Before closing, I want to briefly discuss the role of law enforcement in investigating identity theft crimes and assisting victims. Three-fourths (76 percent) of the respondents to the PRC/CALPIRG identity theft survey reported that the police whom they contacted were unhelpful. Detectives were assigned to their cases less than half of the time. And one-fourth of the victims were not able to obtain a police report.

It is clear that the crime of identity theft calls for some new approaches by law enforcement. One approach that is being explored in California is the development of a single unit within the police department that specialize in identity theft. The Los Angeles Sheriff's Department has established such a unit. Assemblymember Robert Hertzberg has introduced AB 1949 to fund three pilot projects in the state to establish such specialized units.

Additional suggestions for addressing the multi-faceted crime of identity theft can be found in the PRC/CALPIRG identity theft survey, a copy of which has been provided to the Subcommittee.

Thank you for the opportunity to testify about the crime of identity theft. Please feel free to contact the Privacy Rights Clearinghouse if you seek additional information or assistance.



Nowhere to Turn:

Victims Speak Out on Identity Theft

A Survey of Identity Theft Victims And Recommendations for Reform

CALPIRG

Privacy Rights Clearinghouse

May 2000

Nowhere to Turn: Victims Speak Out on Identity Theft
A CALPIRG/Privacy Rights Clearinghouse Report
May 2000

---

by

Janine Benner
Consumer Associate, CALPIRG

Beth Givens
Director, Privacy Rights Clearinghouse

Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Special Thanks To:

Dan Jacobson, Consumer Program Director of CALPIRG
Linda Foley, VOICES
Jodi Beebe, PRC
Elsie Strong, VOIT
Mari Frank, Esq.

And all of the victims of identity theft who took the time to share their experiences with us.

For additional copies of this report, please send $15.00 to

CALPIRG's Consumer Program
926 J Street #523
Sacramento, CA 95814

Please contact CALPIRG or VOIT
at: www.pirg.org/calpirg
(310) 397-3404

Contact information for Privacy Rights Clearinghouse:

Privacy Rights Clearinghouse
1717 Kettner Blvd., Suite 105
San Diego, CA 92101

Please contact PRC or VOICES
and access fact sheets on id theft at:
www.privacyrights.org
prc@privacyrights.org
(619) 298-3396

Nowhere to Turn: Victims Speak Out on Identity Theft

Table of Contents

I. Executive Summary

Identity theft is a growing crisis in the United States. As the crime becomes more visible, stories of victims' complex experiences permeate the media. Identity theft occurs when someone invades your life, taking pieces of your personal identifying information as his or her own, and ruins your financial reputation. In addition, victims of this crime face extreme difficulties attempting to clear the damaged credit, or even criminal record, caused by the thief.

The California Public Interest Research Group and the Privacy Rights Clearinghouse have been helping victims of identity theft for years through advocacy, free guides, hotlines, and monthly support group meetings. We have talked to thousands of victims over the phone, through letters and electronic mail, and in person, hearing new, unique and horrifying experiences every day. But so far there have been little in-depth data collected on the specific problems that victims face or on the specific gaps in law enforcement efforts and credit industry practices that make cleaning up a stolen identity such a time-consuming and seemingly impossible task.

This report follows up on CALPIRG's groundbreaking identity theft reports,[1] released in 1996 and 1997, and on the pioneering work of the Privacy Rights Clearinghouse in assisting victims and drawing attention to their plight. Both organizations have also worked with victims to find ways that they can help themselves, because until recently there was no government agency that made identity theft solutions its priority.[2]

This report summarizes the findings of a detailed survey of 66 recent identity theft complainants to our organizations, conducted in the spring of 2000. The findings may not be representative of the plight of all victims; but they should be viewed as preliminary and representative only of those victims who have contacted our organizations for further assistance (other victims may have had simpler cases resolved with only a few calls and felt no need to make further inquiries). On the other hand, we know of no other survey of victims conducted in as much depth as this. As much as is practical, we let the victims speak for themselves in this report.

Key findings illustrate the obstacles victims face when trying to resolve their identity theft cases. Less than half of the respondents felt that their cases had been fully resolved, and those with unsolved cases have been dealing with the problem for an average of four years. Victims estimated that they spent an average of 175 hours and $808 in additional out-of-pocket costs to fix the problems stemming from identity theft. The data pinpoint the failure of law enforcement, government, and the credit industry to address the root causes of identity theft. By not changing their procedures, these stakeholders have both helped perpetuate identity theft and have made it

[1] "Theft of Identity: The Consumer X-Files", CALPIRG and US PIRG, 1996
"Theft of Identity II: Return to the Consumer X-Files", CALPIRG and US PIRG, 1997

[2] In 1999 the Federal Trade Commission established a clearinghouse to assist victims of identity theft and document their cases in a database. This endeavor is a result of a new federal law, "The Identity Theft and Assumption Deterrence Act of 1998" (18 USC 1028), implemented in 1999. The FTC maintains a toll-free telephone number for victims, 877-IDTHEFT, as well as a web site, www.consumer.gov/idtheft.

difficult for victims to resolve their cases expeditiously. Although each identity theft case is different, we have been able to identify patterns and trends in the victims' responses. The survey data also verify that the stories in the news on identity theft are not extreme cases in which an unlucky victim has had an unusually bad experience. As one victim from California stated, "It was as terrible as all the books and articles say it is."

RECOMMENDATIONS:

This report includes detailed recommendations and updates the CALPIRG/Privacy Rights Clearinghouse "Platform On Identity Theft." Key recommendations are the following: 1. Require credit bureaus to provide free credit reports annually on request, as six states already do (CO, GA, MA, MD, NJ, VT). 2. Provide victims, as well as consumers, with the right to block access to their credit reports. 3. Require matching of at least four points of identity, such as exact name and exact address, date of birth, former address, and Social Security number between credit reports and credit applications. 5. Improve address-change verification. 6. Close the "credit header" loophole that allows Social Security numbers to be sold on the information marketplace, including over the Internet.

II. Findings and Highlights

- Forty-five (45%) of the victims consider their cases to be solved; and it took them an average of nearly two years, or 23 months, to resolve them. Victims (55%) in the survey whose cases were open, or unsolved, reported that their cases have already been open an average of 44 months, or almost 4 years.

- Three-fourths, or 76%, of respondents were victims of "true name fraud." Victims reported that thieves opened an average of six new fraudulent accounts; the number ranged from 1 to 30 new accounts.[3]

- 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 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 1500 hours on the problem.

- 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.

---

[3] "True name fraud" occurs when the imposter opens *new* credit accounts in the name of the victim. "Application fraud" or "account takeover fraud" occurs when the imposter uses a victim's *existing* credit accounts.

- 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%).

- 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.

- In one-third (32%) of the cases, victims had no idea how the identity theft had happened. Forty-four percent (44%) of all the victims had an idea how it could have happened, but did not know who the thief was. But in 17% of the cases, someone the victim knew -- either a relative, business associate, or other acquaintance -- stole his or her identity.

- Victims reported that all of the credit bureaus were difficult to reach, but the hardest one to get in touch with, and the one about which most negative comments were made, was Equifax. Over one-third of the respondents reported not being able to speak with a "live" representative at Equifax or Experian despite numerous attempts. 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.[4]

- All but one of the respondents contacted the police about their cases, and 76% of those felt that the police were unhelpful. Law enforcement agents issued a police report less than three-fourths of the time, and assigned a detective to the victims' cases less than half of the time. Despite the high rate of dissatisfaction with law enforcement assistance, 21% of the victims reported that their identity thieves had been arrested, often on unrelated charges.

- Thirty-nine percent (39%) of the victims reported contacting the postal inspector about their cases, and only 28% (7 out of 25) of those respondents found the post office helpful. Only four of the respondents reported that the postal inspector placed a statement of fraud on their name and address.

- Forty-five percent (45%) of the respondents reported that their cases involved their drivers' licenses. For example, the license had been stolen and used as identification, or the thief had obtained a license with his or her picture but containing the victim's information. Fifty-six percent (56%) of the respondents contacted the Department of Motor Vehicles, and only 35% of those found the DMV helpful.

---

[4] When a "fraud alert" is placed on a victim's credit file, the credit bureau reports to credit issuers that the subject of the report is a victim of fraud. The creditor is supposed to contact the victim at the phone number provided in the fraud alert in order to determine if it is an imposter or the rightful individual applying for credit. Obviously, if the credit bureau does not adequately report the presence of an alert, which often happens when only a credit score is reported, or if the credit grantor fails to detect the fraud alert, which is a common experience of victims, the imposter is able to obtain additional lines of credit in the victim's name.

- Forty-nine percent (49%) of the respondents contacted an attorney to help solve their cases. Forty-four percent (44%) of those people found their attorney to be somewhat helpful. Many consumers contacted attorneys at public interest law firms and received advice for free. Attorneys' fees ranged from $800 to $40,000.

- Respondents reported that the most common problem stemming from their identity theft was lost time (78% of consumers identified this problem). Forty-two percent (42%) of consumers reported long-term negative impacts on their credit reports, and 36% reported having been denied credit or a loan due to the fraud. Twelve percent (12%) of the respondents noted as a related problem that there was a criminal investigation of them or a warrant issued for their arrest due to the identity theft.

III. Analysis of Findings

- **Types of Identity Theft**

A majority (76%) of the victims surveyed reported that they had been victims of what is called "true name" fraud. This occurs when someone uses pieces of a consumer's personal identifying information, usually a Social Security number (SSN), to open *new* accounts in his or her name. Thieves can obtain this information in a variety of ways, from going through a consumer's garbage looking for financial receipts with account numbers and SSNs, to obtaining SSNs in the workplace, to hacking into computer Internet sites, or buying SSNs online.

The other type of identity theft, experienced by 38% of the respondents, is called "account takeover." In this type of fraud, the thief gains access to a person's *existing* accounts and makes fraudulent charges.

Although the fraud committed against the victims surveyed totaled as much as $200,000, the common themes were that stress, emotional trauma, time lost, and damaged credit reputation -- not the financial aspect of the fraud -- were the most difficult problems. One victim from Nevada explained, "(T)his is an extremely excruciating and violating experience, and clearly the most difficult obstacle I have ever dealt with."

Thieves committed various other types of fraud with the respondents' information, including renting apartments, establishing phone service, obtaining employment, failing to pay taxes, and subscribing to online porn sites. In 15% of the cases, the thief actually committed a crime and provided the victim's information when he or she was arrested. One victim from California relates a particularly involved case:

> "(The thief) smuggled 3,000 pounds of marijuana and gave the duplicate CA driver's license (my name and #) to the authorities; she convinced them that she was me and they were going to indict me on the charges. (She) received a duplicate California Driver's License from the DMV with my name and number; rented properties in my name, signed a year lease for one

> residence, attempted to get credit cards and timeshare financing, bought a brand new truck, had liposuction performed via a line of credit, set up various utilities and services in my name ... Worse even, they booked her under my name in the federal prison of Chicago."

Although most victims did not know how their identity had been stolen, many could point to a loan application requiring personal identification that had been carelessly handled by, say, a real estate agent, or employee records containing a Social Security number that had been used fraudulently by a co-worker or an employer. One victim from Maryland stated confidently, "My situation was directly caused by the policy of health insurance companies who use Social Security numbers and account numbers." Seventeen percent (17%) of the respondents believed that their information was first used to open up "instant credit" accounts, where the creditors do not conduct a thorough check to make sure the credit grantee is not a fraud. Only 2 of the 66 victims surveyed had reason to believe that the thief had obtained their information via the Internet.

- **Breaking the News**

Respondents discovered that they had become victims of identity thieves in a variety of ways. The most common was to be denied credit or a loan due to a negative credit report caused by the fraudulent accounts, which happened to 30% of the victims. People were also alerted to the problem after being contacted by a creditor or debt collection agency demanding payment. In many cases the victims said that they wished the creditor had contacted them to verify a change of address or suspicious application. They felt that if this warning had occurred, they could have stopped the problem more quickly.

Victims also reported hearing the news in more startling ways. One victim from California was stopped by the highway patrol and informed that her license had just been surrendered in Nevada. Another victim was shocked to find that her license had been suspended for a D.U.I. citation and a hit-and-run. Yet another victim learned his plight when the police attempted to arrest him for a crime he did not commit.

- **Cleaning up the Mess: The Nightmare Continues**

Respondents spent an average of 175 hours actively trying to resolve problems caused by the theft of their identity. The victims reported missing several days or weeks of work to put their lives back together, and two people even reported losing their jobs due to the time devoted to identity theft resolution. A victim from California felt that resolving her problem was "nearly a full-time job." Robin, a victim from Los Angeles, explains, "One bill -- just ONE BILL -- can take 6-8 hours to clear up after calling the 800 numbers, waiting on hold, and dealing with ignorant customer representatives." She concludes, "The current system is not created for actual assistance, it is created to perpetuate the illusion of assistance."

Of all of the problems that victims said had stemmed from their identity theft, the most common was the loss of time to solve the problem (78%). Other common problems were being denied credit and having a long-term negative impact on their credit report, which can lead to various other

financial difficulties in the future. Twelve percent of the victims said that there was a criminal investigation of them or warrant issued for their arrest because of crimes the thieves had committed.

Victims face these types of problems for years after their identities are actually stolen. Fraud alerts are not effective. Further, the majority of thieves are not caught and continue to use the victim's identity. Over half of the victims surveyed said that their cases had not been solved. One victim reported she had been dealing with the problem for 13 years. A victim from California reported that he had to file Chapter 7 bankruptcy because of his thief. He still cannot get a job due to his thief's criminal record.

- **Where Do They Go for Help?**

Respondents commonly indicated that when they first realized they had been victims of identity theft, there was nowhere for them to go for help. One victim stated, "Aside from the organizations like yours, no one seems to care about these criminals." Another expressed frustration at the lack of assistance to be had, and the necessity for her own resourcefulness: "I am my own expert. I was three steps ahead of every expert's advice."

All but one of the participants in the survey contacted the police about their cases. They reported a high rate of frustration. An elderly victim from California wrote, "Not even the patience of Job helps!" Due to the lack of funding and other resources available to law enforcement, as well as to the multi-jurisdictional nature of identity theft cases, it is often virtually impossible for the police to investigate financial crimes. One victim stated, "The greatest difficulty was having to file a police report in the precinct where the fraud occurred – 3,000 miles away." Many of the victims recognized the lack of resources as the reason law enforcement agencies were not able to assist them and apprehend the criminals. A respondent from California said, "Although the police were not helpful, I have to agree with them. Our legislative people need to give the police more funds and manpower whenever these laws are enacted."

Most of the respondents' written comments focused on the lack of police assistance. In many of the situations, the victims themselves took the investigation into their own hands. They had found the address, phone number, or other information about the thieves, but the police were unable to follow up. A victim from California reported, "They told me it was not their job." Although the percentage of cases in which the thief was arrested was fairly high (21%), respondents pointed out that the thief was often caught for a crime other than identity theft. Another victim from California, whose thief was finally caught, explained:

> "I, personally, found out who the thief was and the address where he lived - even his cell phone number. I reported this to the police at least twice. They did nothing...The thief was accidentally arrested for identity theft during a search of his apartment for a stolen computer. Police found a video that he had made of himself bragging about all the credit cards he had stolen and all of the money he had gotten within a few days' efforts. He had convicted himself."

In many of the responses, victims indicated that the police in their own jurisdictions did not know how to investigate the crime of identity theft. In some states, identity theft is not yet considered a crime against the victims; instead, the creditors are considered the victims because they bear the costs of the financial fraud. A victim from Nevada states, "The police department treated me as if I were the criminal." However, even in states where identity theft is a felony, such as California, respondents still had difficulties. Robin, of Los Angeles, complains:

> "They will lecture you, the victim, endlessly about how it's the fault of the credit card companies that you're in this position...that technically you're not the victim...that there aren't enough people on the police force to handle this...that if your info has only been used to commit $5,000 worth of fraud, how can they explain working on your case to someone whose info has been used to commit $50,000 worth of fraud."

Victims reported the same difficulties with other government agencies they dealt with. Many responded that the Postal Inspector and the Department of Motor Vehicles told them nothing could be done, even if the theft had involved the victim's mailbox or driver's license. One resident of Wisconsin was asked of the DMV, "Were they helpful?" and replied, "Sort of - my contacting the DMV in Texas triggered not an investigation of my thief, but an investigation of me." Robin wrote of the Post Office:

> "It is aggravating, debilitating and depressing beyond belief to meet with this kind of response at virtually every place one calls to get some assistance. One is advised to follow the proper channels, but the proper channels yield impotence at best, hostility toward the 'annoying' victim at worst. They are more like obstacles to tangible assistance."

Respondents said they ran into roadblocks trying to clear things up with their creditors and the three credit bureaus. According to one, "This only compounds the problem." About half the respondents reported that their banks or creditors had been moderately helpful, but many expressed frustration with rude representatives and fraudulent accounts that are still not cleared or that keep reappearing on the victim's credit report. Many reported using pressure or an attorney to force cooperation from creditors. They had the most difficulty with debt collection agents who treated them as if they were merely trying to avoid payment of their bills. A victim from Los Angeles states, "The current system serves the needs of the creditor but to the detriment of the consumer."

Even though victims were able to reach the credit bureaus and place a fraud alert on their accounts (so that they would be notified if a creditor had requested access to it), in almost half of the cases, fraud recurred. One victim from California stated, "It seems as if as soon as I have put out one fire another is lit. It seems as if there is no end to this infringement upon my civil liberties." Many victims felt that it was negligence on the part of the creditor or credit bureau that had caused their identity theft. They felt that the credit industry had perpetuated, rather than prevented, the problem.

One respondent's comment sums up the victims' feelings about identity theft well: "What a perfect crime this is for thieves – they get to abuse you over and over and over and nobody pursues them. Who says crime doesn't pay?"

- **Advice**

In the survey, victims were asked what advice they would give to future victims, and what laws or actions would have helped them resolve their problems more quickly and easily. The respondents offered many different pieces of advice, but three comments were mentioned most often.

1. Be careful with your personal information. Although most victims reported that they had never lost their wallets or been victims of burglary, they nevertheless warned future victims to closely guard all of their personal identifying information. In many cases victims advised people never to give out their Social Security numbers unless absolutely required by law. Victims also suggest monitoring one's credit report at least twice yearly. This is a way to make sure that there are no mistakes, and to catch the fraudulent accounts early.

2. Know your rights. Victims also suggested asking the police or another organization or agency for information on what to do and what their rights as victims are. A victim from Wisconsin explains, "Find out what your rights are and what you need to do first prior to contacting the credit bureaus and police and creditors. These three agencies tend to not tell you what your rights are, incorrectly inform you that you don't have any rights, or ignore you completely." Other respondents mentioned places that were particularly helpful, such as the Privacy Rights Clearinghouse website at www.privacyrights.org, the Public Interest Research Group's website at www.pirg.org, or www.identity theft.org the website of Mari Frank, Esq. Respondents also encouraged victims to join support groups. Currently there are two groups in California, Victims of Identity Theft Support Group (VOIT) in Los Angeles, and V.O.I.C.E.S. (Victims of Identity Crimes Extended Services) in San Diego. There are links to these groups on CALPIRG's and the PRC's websites.

3. Be persistent. Victims emphasized the necessity of perseverance in the fight to resolve their identity theft problems. Respondents realized that it was up to them to spend time and money to clear their names, because no one else was going to help them repair the damage caused by this crime. One victim offered inspiring words to future victims, "If you are a victim of this crime, don't give up. You have to be persistent, and dispute, dispute, dispute until the matter is resolved. It can get overwhelming, but you have to do it." Another stated, "Know that you are not alone."

IV. Need for Reform: Victims' Perspectives

Victims' recommendations for laws and credit industry actions follow:

1. Give law enforcement the resources and education to adequately investigate the crime. They should respect victims, write police reports, and take steps to pursue and arrest the perpetrator. The results from the survey show that when law enforcement did actually take steps to investigate the perpetrator, they were often successful. In many cases, a

victim will not feel that his or her case is completely solved until the thief is behind bars and cannot commit the crime again.

2. Make identity theft a crime against the true victim in states where it is not. In states where identity theft is a crime, criminals should face more severe punishment, and victims should have the right to sue those partly at fault for their stolen identity -- the creditors and credit bureaus. A few of the victims surveyed reported that their thieves had served short prison terms, between two months and three years, or that they were held on probation.

3. There needs to be a clearinghouse of information where victims can turn for advice. Establish an agency or office whose job it is to make phone calls on behalf of the victim to the credit bureaus, creditors, and collection agencies. This would help relieve the hundreds of hours that victims reported spending on their identity theft cases.
4. Make it harder for creditors to grant credit to an identity thief by creating fraud alerts that work and by requiring creditors to be more vigilant in their investigation into the person seeking credit. Most of the cases reported could have been prevented if the first creditor receiving the fraudulent application had looked more closely at the information on the application, or had attempted to contact the original person on file to check if the applicant was the same.

5. Creditors and credit bureaus should assist victims in both investigating the crime and repairing their damaged credit. Victims should be able to obtain the original application that was fraudulently completed by the thief with the victim's information. Many victims reported that they had been refused copies of the fraudulent application. They said it would have been easier to apprehend the perpetrator if this information had been available.

6. There should be laws prohibiting the sale of personal information and the release of a credit report without prior authorization and a password known only by the victim. The fact that almost half of the victims' fraud *recurred* on their credit report demonstrates that the current system of fraud alerts is not working.

V. CALPIRG/Privacy Rights Clearinghouse Identity Theft Platform

Additional Provisions Needed in State and Federal Laws, and in Industry Practices, to Protect Identity Theft Victims and Prevent Fraud

In 1998 Congress enacted legislation, the Identity Theft Assumption and Deterrence Act, criminalizing identity theft.[5] At least 22 states[6] have also criminalized this crime. By making

[5] Identity Theft Assumption and Deterrence Act of 1998, PL 105-318 (10/30/98), criminalized identity theft and established the Federal Trade Commission as a national identity theft clearinghouse. It was based on HR 4151 (Shadegg-R-AZ) and S. 512 (Kyl-R-AZ). The law is found in the U.S. Code at 18 USC 1028.

identity theft a specific crime, Congress and the states have taken an important first step toward fighting identity theft. In addition, the 1998 Act required the Federal Trade Commission to expand its role as an identity theft clearinghouse for both federal agencies and consumers.

Yet, much more needs to be done to stop identity theft. In particular, legislation must be enacted to require creditors and credit bureaus to improve their credit-granting and complaint-handling practices. Further, easy access to the bits of information that comprise a consumer's financial identity must be curtailed.

Sloppy credit-granting practices by banks, department stores, phone services, and other creditors make the crime all too easy to commit. Once the crime has occurred, creditor and credit bureau practices help perpetuate the problem by subjecting victims to a nightmarish system of clearing their names, making victims into repeat victims, or both.

Over the years, CALPIRG and the Privacy Rights Clearinghouse (PRC) have developed the following platform to prevent identity theft and ease the burden of victims. Important pieces of the platform have been included in bills currently before the California Legislature and the U.S. Congress. In addition, legislatures in other states are also considering parts of the platform.

The following platform pieces would greatly improve the accuracy and privacy of credit reports. Some provisions may overlap. And some could only be enacted by Congress due to preemption, and are so noted.

> *Note:* Many state and Congressional legislative measures are discussed in the platform. California legislative bills can be found at the website http://www.leginfo.ca.gov. Click on "Bill Information." Bills in the U.S. Congress can be found at http://thomas.loc.gov.

The following is a summary of PIRG/PRC's platform and recommendations:

- Give consumers free access to credit reports and improve consumer notification when reports are accessed.

- Prevent illegitimate access to credit reports.

---

[6] See chart "STATE IDENTITY THEFT LAWS" [from New York Senate Majority Task Force On Privacy, March 2000, <http://www.senate.state.ny.us/Docs/nyspriv00.pdf>] Arizona Ariz. Rev. Stat. Sect. 13-2708, Arkansas Ark. Code Ann. Sect. 5-37-227, California Cal. Penal code Sect. 530.5, Connecticut 1999 Conn. Acts 99, Georgia Ga. Code Ann. Sect. 121, Idaho Idaho Code Sect. 28-3126, Illinois 720 ILCS 5/16/G, Iowa Iowa Code Sect. 715A8, Kansas Kan. State Ann. Sect. 21-4108, Maryland Md. Ann. Code art. 27 sect. 231, Massachusetts Mass. Gen. Laws ch. 266 Sect.37B, Mississippi Miss. Code Ann. Sect. 97-19-85, Missouri Mo. Rev. State Sect. Sect. 570.223, New Jersey N.J. State Ann. Sect. 2C:21-17, North Dakota N.D.C.C. Sect. 12.1-23-11, Ohio Ohio Rev. Code Ann. 2913, Oklahoma Okla. Stat. Tit. 21, Sect. 1533.1, Tennessee Tenn. Code Ann. Sect. 39-14-150, Texas Tex. Penal Code Sect. 32-51, Washington Wash. Rev. Code Sect. 9.35, West Virginia W. Va. Code Sect. 61-3-54, Wisconsin Wis. Stat. Sect. 943.201
Source: ID Theft: When Bad Things Happen To Your Good Name. FTC, February 2000.

- Ensure accuracy of the report and authenticity of the report recipient.
- Tighten DMV procedures to prevent imposters from obtaining fraudulent deriver's licenses and to assist identity theft victims.
- Help victims regain their financial health
- Improve accuracy and accountability of the credit granting process
- Seek solutions to the critical problems faced by criminal identity theft victims.

Here is a detailed discussion of these platform measures:

1. **Give Consumers Free Access to Credit Reports. Improve Consumer Notification when Reports Are Accessed.**

(a) Credit bureaus should provide a free report annually on request to detect identity theft early and improve accuracy: Six states (CO, GA, MA, MD, NJ, VT) grant consumers the right to a free credit report annually on request from each of the Big Three credit bureaus – Equifax, Experian and Trans Union. Colorado's law laudably also requires an annual notice from the Big Three national credit bureaus (also known as credit reporting agencies, or CRAs) to all credit-active consumers describing their rights under the law, including their right to a free report annually on request. Georgia allows consumers to obtain two free reports per year.

All consumers should have the ability to request a copy of their credit report from the CRAs at least once a year to check for fraud and for other inaccuracies. This right is especially important since federal law allows credit reports to be sold for credit, insurance and other "permissible purposes" to any business without a consumer's consent, except in Vermont, where oral consent is required. U.S. Senator Dianne Feinstein (D-CA) recently introduced an identity theft prevention measure, S.2328, in Congress in April 2000. This bill includes a provision for free credit reports, as do bills by Rep. Roybal-Allard (D-CA) HR 1015, and Rep. Hooley (D-OR) HR 4311.

Under the Fair Credit Reporting Act (FCRA, 15 USC 1681), employers must get the individual's consent before obtaining an individual's credit report. The FCRA, as amended in 1996, only enables consumers who have recently been denied credit, are unemployed, indigent, or believe themselves victims of identity theft to obtain a free copy of their credit report. Federal law otherwise allows credit reporting agencies to charge $8.50 for a credit report. A few states limit the charge to a lower amount.

(b) Credit bureaus should notify the consumer following business requests for their report in order to detect illegitimate access and fraud: Require that consumers receive an automatic *notice* that their report was accessed at their current address, with a phone number and address for any requestor, following any new (not from an existing creditor) request for it. And, any time credit

is extended within 60 days of the credit bureau updating an address, the consumer should be notified at both the new and old address. The name and phone number of the business that granted credit should also be provided.

(c) Provide credit scores: Give consumers access to credit scores and provide explanations as part of their credit reports. Instant credit offers are a primary precursor to identity theft. Yet neither the FTC nor the credit industry will explain the credit scoring systems derived from credit reports that make instant credit possible. Federal legislation proposed by Rep. Chris Cannon (R-UT), HR 2856, would make credit scores part of credit reports. California State Senator Liz Figueroa's (D-Fremont) SB 1607 would require that consumers obtain their credit score and an explanation of the score in home mortgage situations.

(d) Give notice of inquiries and subscriber names: CRAs should be required to improve disclosure of inquiries and subscriber codes by providing an explanation of how to interpret information on the credit report. They should also be required to provide all consumers, not only fraud victims, with the name and toll-free telephone number of a contact for all trade lines and inquiries appearing on a consumer's credit report.

While 1996 federal FCRA amendments do require better disclosure of persons that obtain the consumer's credit report, a credit reporting agency is only required to provide an address or phone number of the person or company procuring the credit report if the consumer requests it. Many consumers may not know that they can request the address and phone numbers to be included on a copy of their credit report. Time is of the essence for victims of identity theft who need to contact creditors with whom their names have been used fraudulently in order to minimize the damage done by their imposter. The Associated Credit Bureaus, in cooperation with the Big Three bureaus, implemented an identity theft initiative in March 2000 that addresses some of these disclosure problems. (See http://www.acb-credit.com)

2. Prevent Illegitimate Access to Credit Reports.

(a) Allow consumers the right to block access: California State Senator Debra Bowen (D-Marina Del Rey) introduced SB 1767, a broad identity theft prevention bill, that includes a provision enabling individuals to "freeze" their credit report. It is important that any such blocking provision also apply to the release of a credit score on a consumer, since most instant credit (favored by identity thieves) is issued by businesses requesting credit scores, not the full credit reports. Further, blocking must not remove a consumer from the credit system. A consumer who elects blocking should not be prevented from applying for and obtaining credit and loans when they do provide their express written authorization to the credit grantor to obtain information from credit reporting agencies.

(b) Close credit header loophole: As part of a 1994 consent decree with TRW (now Experian) that properly prohibited target marketing[7] from credit reports, the FTC made a serious mistake. It

defined certain sensitive personal information contained in credit reports as exempt from the definition of credit report. Under this loophole, the credit bureaus now traffic widely in "credit headers," which include the demographic information found in a credit report that is not associated with a specific credit trade line or public record.

Credit headers may include names, addresses, dates of birth, previous addresses, telephone numbers and Social Security numbers. Credit header databases are re-sold by the Big Three credit bureaus in bulk and used for a variety of products. Many information brokers operate websites that sell credit headers, along with public records information. Such products often include Social Security numbers, which can be obtained by identity thieves.

In 1997, the credit bureaus and other firms that traffic in credit headers formed a so-called "self-regulatory" association known as the Individual References Services Group. The organization says its "principles impose significant restrictions on the access and distribution of non-public information, such as non-financial identifying information in a credit report. For example, Social Security numbers obtained from non-public sources may not be displayed to the general public on the Internet by IRSG companies." [8]

Despite this assertion, PIRG and PRC have found that SSNs can still be purchased from websites. We strongly support closing the credit header loophole because, even if the IRSG's voluntary rules were effective in halting the sale of SSNs to the general public, it is easy to use a "pretext" to obtain SSNs from one of the many sites on the Internet that purports to *only* sell it to qualified requestors. Several federal proposals would close the credit header loophole. U.S. Senators Dianne Feinstein (D-CA), Charles Grassley (R-IA) and Jon Kyl (R-AZ) have proposed S.2328. Similar companion legislation, HR 4311, has been proposed by Rep. Darlene Hooley (D-OR). Rep. Jerry Kleczka (D-WI) has a broader proposal, HR 1450, to close the credit header loophole and further restrict the use of Social Security numbers.

(c) Mandate consumer consent: Until full blocking is enacted, states or the federal government should enact legislation to require all prospective users to ask a consumer's permission to access a credit report. Under current laws, only Vermont requires the subject's (oral) permission to access a credit report. Federal law requires employment users to ask a consumer's permission. Requiring consumer authorization will not slow down legitimate inquiries by creditors -- most ask already -- but will discourage illegal access by information brokers and identity thieves, and will require credit bureaus to improve auditing procedures.

---

[7] At the time, Equifax voluntarily agreed to stop target marketing from credit reports. Trans Union, on the other hand, refused, and has since led the FTC through eight years of litigation, while it continues to use credit reports to generate target marketing lists in defiance of the FTC. Most recently, on 1 March 2000, the FTC again ordered Trans Union to stop, although it then (30 March 2000) agreed to stay the ruling while Trans Union appeals yet again. <http://www.ftc.gov/opa/2000/03/transunion.htm>
The Act should also be clarified to ban target marketing explicitly to end Trans Union's lawsuit.

[8] See http://www.irsg.org

(d) Establish unique identifiers: Congress should require creditors and CRAs to replace the use of the Social Security number as the key identifier with a more accurate, less accessible code.

(e) Pre-screening "opt-outs" should be "opt-ins" to prevent mail interception: Each year, banks mail at least 3 billion "pre-approved" (pre-screened) credit card solicitations.[9] Many experts contend that intercepted mail is a major factor in identity theft. Yet, federal law allows credit reports to be used for the marketing of both insurance and credit cards unless consumers provide an opt-out by calling a toll-free number (888-5OPTOUT) or sending a written request. HR 1450 (Kleczka) would change that to an opt-in.

At a minimum, consumers who opt-out of pre-screening by telephone should not be required to also mail in a "Signed notice of election" to extend their opt-out beyond two years. Also, credit issuers should be required to post the opt-out telephone number prominently on all pre-approved offers of credit. The latter provision is included in California State Senator Bowen's SB 1767.

(f) The fraud-flag process should be improved: The generation of credit scores should be blocked on any report containing a fraud flag (or even an error dispute), unless additional verification is made that the report is accurate and that the credit request is from the actual consumer. An alternative would be for the credit grantors to deliver the credit score with an indication that the report contains a fraud alert. When complete credit reports are delivered to the customer, the fraud flag should be posted prominently at the top of the report. The Associated Credit Bureaus launched an identity theft initiative in March 2000 that includes improved security alert reporting.

Credit grantors who issue credit to imposters *after* the victim has established a fraud alert should be penalized. California State Senator Bowen's SB 1767 contains this provision, as does U.S. Senator Feinstein's S.2328.

3. Ensure Accuracy of the Report and Authenticity of the Report Recipient.

(a) Match points of correspondence: Currently operative consent decrees allow the CRAs to ship a credit report that matches the credit application in only any two or three points of correspondence, which is inadequate to prevent either theft of identity or credit denial due to inaccuracy. We recommend that at least four points be matched.

Such inadequate credit application verification procedures leave victims with numerous fraudulent credit accounts that contain completely false information except for their name and only one or two other correct identifiers. Secondary identifiers which may be used to determine a match could include, but not be limited to, driver's license number, current employer, and phone number. In 1997, then-Assemblymember Kevin Murray of California (D-Los Angeles) (now a State Senator) gained passage of AB 156 which, among other things, requires that credit grantors match a

[9] Edmund Sanders, "Charges Are Flying Over Card Pitches," *Los Angeles Times* (June 15, 1999) p. C1.

minimum of *three* identification elements. It is not yet known if this measure has been instrumental in preventing fraud. We recommend that the effectiveness of this provision be studied.

(b) Improve address confirmation for new and existing credit accounts: Credit bureaus should be required to disclose to the creditor that an address on the application for new credit does not match the address listed for that consumer on the credit bureau's file. This practice would alert the creditor that it is a potential fraudulent application. Currently, when information from a credit or loan application is furnished to a credit reporting agency with an address different from the address on the credit report, the credit reporting agency may simply replace the old address with the new address. Creditors should be required to send confirmation notices to all addresses listed on the named applicant's credit report.

In addition, banks and other creditors should be required by law to send a confirmation to consumers whenever an address change is requested on the existing account. In addition, a confirmation should be required for all address changes within 45 days of a request for an additional card on a new account.

Identity thieves use victims' personal information to commit "account takeover" of existing accounts. They contact existing creditors and request new credit cards to be sent to a different address. While some creditors have procedures to verify whether the person requesting the new card is in fact the true cardholder, many banks and other creditors do not. Commendably, the U.S. Postal Service implemented an address-change notification protocol in response to some highly publicized identity theft cases where victims' personal financial information was obtained from mail diverted to the thief through a fraudulent change-of-address form filed with the Post Office.

In 1999 the California Legislature approved an address verification measure, Senator Teresa Hughes' (D-Inglewood) SB 930. When an application is returned to the creditor with a different return address than on the creditor's solicitation, it must verify the address. Verification is also required if a change of address is reported with a request for a duplicate or replacement credit card. In the 2000 session, California State Senator Debra Bowen's SB 1767 contains an additional address verification provision, as does U.S. Senator Dianne Feinstein's S.2328.

4. Tighten DMV Procedures to Prevent Imposters from Obtaining Fraudulent Driver's Licenses and to Assist Identity Theft Victims.

Many victims surveyed for this report indicated that the imposter used a fraudulent driver's license to legitimize credit transactions. California Department of Motor Vehicles identification verification procedures for duplicate and replacement licenses need to be strengthened. Assemblymember Lynne Leach's (R-Walnut Creek)AB 2382 would require the DMV to compare the photograph on the original driver's license record with the likeness of the individual who is requesting the replacement license in-person. Such requests could no longer be ordered over the phone.

The DMV should also institute other procedures to streamline and systematize its fraud-handling protocols. For example, a centralized lost-and-stolen license reporting function should be

implemented in California. A proposal has been introduced by the Santa Clara County Identity Theft Task Force to develop a uniform process among all criminal justice system stakeholders in the county that handle identity theft cases, including criminal impersonation.[10] Their recommendations hold promise for such practices to be implemented in other jurisdictions.

California Assemblymember Roderick Wright (D-So. Central Los Angeles) has introduced AB 2462 that would simplify many victims' credit bureau fraud reporting tasks vis-à-vis DMV records. In 1997, AB 156 provided that when the victim presents a copy of the *police* report to the credit bureau, the bureau must then remove the fraudulent account(s) from the information it provides to creditors. Wright's AB 2462 would extend that process to the *DMV investigative reports* that have been filed by identity theft victims. The credit bureaus would be required to remove fraudulent records based on a DMV report, the same as it currently does for police reports.

5. Help Victims Regain Their Financial Health.

(a) Streamline fraud notification: Credit bureaus and creditors should be required to develop a fraud notification system that eliminates the current burden on victims to make dozens of phone calls and obtain numerous notarized statements at great cost. In March 2000, the Associated Credit Bureaus (ACB) announced an initiative by the credit reporting industry to streamline fraud reporting for victims. We recommend that the ultimate goal for this endeavor be "one-stop-shopping" for fraud victims, a single phone call to launch the fraud clean-up process.

(b) Take advantage of artificial intelligence: Creditors should increase the use of artificial intelligence programs to identify patterns of fraudulent use and notify consumers of suspected fraud activity. Most of the victims' cases reported in our survey could have been prevented if the credit bureaus and creditors had detected the imposter's unusual activity.

(c) Provide victims with adequate information: Fraud victims who contact the credit bureaus should receive "fraud kits," describing the steps required to recover from identity theft. The ACB's identity theft initiative includes this recommendation for the three bureaus. Because credit issuers are often the ones to inform victims of suspected fraudulent activity, they too should provide consumers with such "fraud kits."

(d) Streamline law enforcement information and investigation functions. A common theme of the victims who were surveyed was their inability to obtain assistance from law enforcement in their own jurisdiction and in the jurisdictions where the identity thief was active. California Assemblymember Robert Hertzberg's (D-Van Nuys) AB 1949 addresses several of the complaints raised by victims. The California Department of Justice would establish pilot programs in the police departments of at least three counties. Special units devoted solely to identity theft would be developed, thereby centralizing the identity theft efforts of that police department. These units

[10] Participants in the Santa Clara County Identity Theft Task Force are: DMV Investigations Unit, Santa Clara County District Attorney's Office, San Jose Police Department, Santa Clara County Sheriff, California Highway Patrol, and Santa Clara County Courts.

would (1) create a public awareness campaign about how to avoid becoming a victim, (2) act as a regional clearinghouse for law enforcement, industry, and victims, (3) serve as a liaison with other local, state, and federal government agencies, and (4) investigate and prosecute identity theft suspects.

(e) Help victims deal with debt collectors. Many victims complain that they are "hounded" by debt collectors who are attempting to obtain payment for the imposter's bills, or who purport to have a claim for money or interest in property against the victim. California Assemblymember Roderick Wright's AB 2462 enables victims to obtain a judgment that declares the victim is not obligated on these claims and that provides for an injunction restraining attempts to collect.

6. Improve Accuracy and Accountability of the Credit Reporting and Granting Processes.

(a) Expand subscriber duties: One method by which identity thieves obtain information about their victims is by accessing credit reporting terminals in their workplace (such as auto dealerships, realtors, banks). Credit bureaus should be required to establish, by contract, the names of individuals with access to subscriber terminals. Require all access to be by unique individual password to maintain audit trails of violations. Require credit bureaus and re-sellers to verify identification and purposes of subscription applicants, to keep adequate records of report requestors, and to conduct ongoing audits of existing customers.

While the 1996 federal FCRA amendments require additional duties for resellers of information to verify the identity and purposes for which their subscribers will use their information, there remains the problem of people who illegally access credit report databases from authorized subscriber terminals.

(b) Delete inquiries related to fraudulent accounts: All credit reporting agencies should be required to delete fraudulent inquiries related to accounts they have determined to be fraudulent. Further, credit bureaus should be required to investigate a consumer's dispute and delete inquiries that were not from companies with whom the consumer initiated a business transaction nor from a company that extended a firm offer of credit to the consumer.

A frequent reason given by creditors for refusing new accounts is that the consumer has "too many inquiries" on his or her credit report. Every time anyone obtains a copy of a consumer's credit report for determining whether or not they should extend credit, regardless of whether they actually do extend credit, that company is listed as an inquiry on the consumer's report. Identity theft victims often have dozens of inquiries listed on their credit report. Some result in fraudulent accounts being opened and others represent failed attempts by an identity thief to open accounts.

(c) Implement truncation on account numbers and Social Security numbers. Take Social Security numbers out of circulation: Expand actions by financial regulators and credit bureaus to truncate key identification numbers, such as account number on ATM receipts, credit card transaction slips, and credit reports, as well as SSN truncation on credit reports. This simple measure limits access by identity thieves to full account numbers. In the 1999 California

Legislative session, Senator Teresa Hughes gained passage of SB 930 that requires account number truncation on transaction slips starting in 2004. We recommend that the timetable for implementation be accelerated.

Many victims complained that easy access to their Social Security numbers made it easy for identity thieves to impersonate them. California State Senator Bowen's SB 1767 would prohibit the use of SSNs for identification purposes except for Social Security administration, tax, credit, or law enforcement purposes. This bill also states that individuals should not be required to provide the SSN except for the latter stated purposes.

(d) Businesses must properly dispose of documents containing sensitive personal information. A common means by which identity thieves obtain Social Security numbers, account numbers, and the other information that they need to impersonate their victims is "dumpster diving." Despite the increased attention that identity theft has received in media stories in recent years, many organizations – businesses, healthcare facilities, government offices, work places of all kinds -- continue to dispose of documents without properly destroying them. This applies to paper documents as well as files on computer disks and hard drives.

California Assemblymember Howard Wayne (D-San Diego) introduced AB 2246, a bill requiring that records containing personally identifiable information be destroyed properly. Any individuals who are harmed as a result of a company's failure to practice responsible information-handling would be entitled to recover damages.

(e) Make credit activation verification more rigorous: All credit cards and ATM/debit cards should be mailed "unactivated" and only activated after adequate verification of the recipient's identity. Verification should not be limited to a match of the SSN because imposters usually have that information. Additional information should be included in the verification process. We are aware of one bank that asks for a copy of a recent utility bill.

(f) Establish $1,000 minimum damages per violation: The federal FCRA does not provide for minimum statutory damages to consumers for violation of the FCRA by credit bureaus or furnishers. Consumers should not have to tediously prove actual damages in each complaint. CRAs count on the difficulty of establishing actual damages when they refuse to settle disputes with consumers.

7. Seek Solutions to the Critical Problems Faced by Criminal Identity Theft Victims.

Although this report has focused on credit-related identity theft, several survey respondents (15%) reported that in addition to having to clean up their credit reports, they have also found that they must deal with wrongful criminal records. Victims of criminal impersonation find that it is virtually impossible to clear up the criminal record. Even if they succeed in having the slate wiped clean by the law enforcement agency, the court system, and/or state or federal criminal records authorities, there is no way for victims to know if the many information brokers who once obtained erroneous records continue to report them to employment background checkers and other investigators.

It is beyond the scope of this report to comprehensively address the complex and vexing problem of criminal identity theft. But we feel it is noteworthy to report on encouraging developments in the current session of the California Legislature.

- Assemblymember Susan Davis's (D-San Diego) AB 1897 would establish a process whereby individuals who have wrongfully been given criminal records can petition the court to obtain a determination of factual innocence and to seal or expunge the erroneous or fraudulent information.

- Assemblymember Tom Torlakson (D-Antioch) has introduced AB 1862. This bill would establish a database within the California Department of Justice to record information concerning victims of criminal identity theft. Victims as well as their authorized representatives, such as employment background checkers, would access the database to prove that the victims are not the actual perpetrators of the crimes ascribed to them in court and other records.

VI. Information about CALPIRG and the Privacy Rights Clearinghouse

- **CALPIRG**

The California Public Interest Research Group (CALPIRG), is a statewide, non-profit public interest advocacy group that works on environmental, consumer, and good-government issues. Since 1972, CALPIRG has been one of the state's leading public interest groups, with 70,000 student and citizen members across the state. The consumer program works to protect consumers from financial rip-offs, unsafe products, and invasions of privacy. U.S. PIRG serves for the national lobbying office of CALPIRG and the other state PIRGs.

In recent years, CALPIRG's consumer program has been focused on assisting and advocating on behalf of victims of identity theft in California and around the country. In 1995, CALPIRG worked with victims, attorneys, and law enforcement to create V.O.I.T., the Victims of Identity Theft Support Group. The group, which meets monthly, provides victims a place to share their stories and hear from those who have been successful in resolving their cases. The group also hears from guest speakers, such as law enforcement agents or attorneys. It also allows victims to discuss positive solutions to the problem of identity theft and make recommendations to decision-makers.

- **Privacy Rights Clearinghouse**

The Privacy Rights Clearinghouse (PRC) is a nonprofit advocacy, research and consumer education program located in San Diego, California. It was established in 1992 with funding from the California Public Utilities Commission's Telecommunications Education Trust. It is a project of the Utility Consumers' Action Network, a nonprofit organization which advocates for consumers' interests regarding telecommunications, energy and the Internet. The PRC sponsors the identity theft support group VOICES, Victims of Identity Theft Extended Services. This groups assists victims, increases public/corporate awareness, and works to decrease the potential victim population.

The PRC maintains a complaint/information hotline on informational privacy issues. Although it was originally established to serve California consumers, it is increasingly being contacted by consumers from throughout the U.S. The Clearinghouse publishes a series of consumer guides on a variety of informational privacy topics including identity theft, credit reporting, telemarketing, "junk" mail, Internet privacy, medical records, and workplace issues, among others. These publications, along with speeches and testimony, are available on its website, www.privacyrights.org.

The PRC participates in numerous public policy proceedings to bring consumer privacy issues to the attention of decision-makers. It has contributed testimony and formal comments to the California Legislature, the California Public Utilities Commission, the Federal Trade Commission, the National Telecommunications and Information Administration, the U.S. Comptroller of the Currency, and the U.S. Department of Health and Human Services.

Senator KYL. Steve Emmert.

STATEMENT OF STEVEN M. EMMERT

Mr. EMMERT. Thank you, Chairman Kyl, Senator Feinstein. I appreciate the opportunity to testify before the subcommittee today about the information practices of our company, LEXIS–NEXIS, and the industry's leadership efforts to balance privacy protections with legitimate, socially beneficial information needs.

Among the services that LEXIS–NEXIS offers are people-finder or individual reference services that customers use to locate individuals and to verify identities. Individual reference service products contain only basic identifying information, such as name and address, not financial information.

LEXIS–NEXIS is a founding member of the IRSG, which represents leading information industry companies, including the three major credit reporting agencies. We provide commercial information services to help verify the identity of or to locate individuals. Customers use individual reference services for a variety of purposes, including finding witnesses, heirs, pension beneficiaries, and hidden assets. In fact, there are a number of Federal regulations that require the use of location services for these very purposes. They are also used to track down missing and exploited children; locate deadbeat dads, parents; to locate bone, blood and organ donors; and to verify identities of contributors to political campaigns.

Each of the companies who belong to the IRSG has adopted self-regulatory principles governing the dissemination and use of personal data. The IRSG developed these principles in 1997 in conjunction with the Federal Trade Commission.

As part of these principles, companies commit, among other things, to restrict their distribution of non-public information through appropriate safeguards. One such safeguard prohibits the display of Social Security numbers and dates of birth in individual reference service products distributed to the general public, the types of websites that Senator Feinstein referred to at the beginning of the hearing; also, for products distributed to professional and commercial users, a prohibition on the display of such information in a less truncated and appropriate manner.

The example of that would be to mask the last four digits of the number so that you can use the initial numbers to identify the place of issuance and the year of issuance. This principle has helped reduce the availability of Social Security numbers for sale on the Internet. I have summarized in my written testimony the other key safeguards contained in the IRSG principles.

Given the subcommittee's focus on identity theft today, I know you are interested in the substantial use that is made of these services in the fight against identity theft where verifying an individual's identity is crucial. Banks, credit card companies, and other types of credit institutions, as well as gas, electric and telephone utility companies and government entities, distributing public entitlement programs are all becoming increasingly plagued by frauds who use existing persons' identity to illegally extract products, services and money.

Individual reference service products are also an important tool for other types of fraud prevention efforts by businesses. The insurance industry, for example, relies on individual reference service products to investigate fraudulent claims. Credit card companies and department stores use them to detect and limit credit card fraud. Banks use them to detect and report credit card fraud, insider abuse, and money laundering. Many businesses use them to minimize the risk of financial fraud when they receive an unusual order for the delivery of merchandise.

Since the victims of identity theft are not only the businesses that lose billions to various forms of identity theft per year, but also the consumers whose credit is often ruined by this insidious act, everybody directly benefits by this application of personal identifying information provided by individual reference services. My point is that the availability of individual reference services helps to reduce identity theft.

Although some have alleged that the availability of identifying information from individual reference services contributes to identity theft, two Federal agencies, the Federal Reserve Board and the Federal Trade Commission, have studied this question, and neither agency was able to find any support for this proposition.

With respect to S. 2328, our concern is that if enacted in its current form, it would jeopardize the usefulness of such services. Specifically, we believe it goes too far in sections 7 and 8. Section 7 would have the effect of cutting off identifying information that we use to index and organize disparate information, distinguishing between John Smiths that live in the same town.

I actually checked this morning. Currently, there are 34,516 entries for "John Smith" on a nationwide basis. Trying to determine which John Smith you are looking for is a little bit of a trick sometimes. When we have the availability of prior addresses, age, and Social Security information, we can make those distinctions. These indexing and verification uses are critical to ensure that the products that we and other IRSG members offer to professional and government agencies contain accurate and complete information.

Section 8 would mandate that individual reference service companies enter a very different market than they ever sought to enter, the consumer market for public record information, as a condition of selling public record information to lawyers, law enforcement officials, journalists, and other professionals.

We do not object to providing an individual with non-public information contained in an individual reference service product that specifically identifies him or her. The IRSG principles already require this. Nor do we object to advising an individual about the nature of public record information that an individual reference service makes available in its products, if reasonably available, where you can obtain a correction and where a correction request can be directed. The IRSG principles also require this.

We do object, however, to having to undertake the enormous burden associated with retrieving potentially relevant information from a large number of data bases of public records and verifying that it pertains to the individual making the request. In addition to being burdensome, it would be ineffective for the consumer.

To be effective, any correction of errors must be made with the government entities where the sources of the information originate. The task of individual reference services in this regard is to reflect reliably the data made available by the originating public record source.

Again, I would like to thank you for the opportunity to testify this morning and welcome any questions you may have.

[The prepared statement of Mr. Emmert follows:]

PREPARED STATEMENT OF STEVEN M. EMMERT

I. INTRODUCTION

I am the Director of Government and Industry Affairs for Reed Elsevier Inc. and LEXIS–NEXIS, a wholly owned division of Reed Elsevier. On behalf of both LEXIS–NEXIS and the Individual Reference Services Group, I very much appreciate the opportunity to testify before your Committee about the information practices of my company, our efforts in the area of acquisition, security, and use of personally identifiable information from non-public sources, and industry's leadership efforts to balance privacy protections with legitimate, socially beneficial information needs.

LEXIS–NEXIS leads the information industry with the largest one-stop, dial-up information service, the LEXIS–NEXIS service for legal, business, and government professionals. The LEXIS–NEXIS service contains more than 2.2 trillion characters and approximately 2.5 billion documents in more than 10,200 data bases. It adds 14.7 million documents each week.

Today, two million professionals worldwide—lawyers, accountants, financial analysts, journalists, law enforcement officials, and information specialists—subscribe to the LEXIS–NEXIS services. They perform more than 400,000 searches per day. The combined services contain more than 24,800 sources: 18,800 news and business sources and 6,000 legal sources.

The NEXIS service is the largest news and business online information service, with not only news, but company, country, financial, and demographic information, as well as market research and industry reports. The NEXIS service is unmatched in depth and breadth of information. In fact, 120,000 new articles are added each day from worldwide newspapers, magazines, news wires and trade journals.

Although the overwhelming majority of the information sources on the LEXIS and NEXIS services are public in nature, all of which are available to the general public through their public libraries, the local news stand or bookstore, or from government offices, a handful of the data sources that contribute to our services are not available to the general public. These data sources include consumer credit reporting files but contain only basic identifying information (e.g, name, address) that is used by customers of LEXIS and NEXIS to locate specific individuals.

LEXIS–NEXIS also is a founding member of the Individual Reference Services Group (IRSG), which represents leading information industry companies, including the three major credit reporting agencies, that provide commercial information services to help verify the identity of or locate individuals. Each of the member companies has adopted self-regulatory principles governing the dissemination and use of personal data, principles which the IRSG developed in 1997 in conjunction with the Federal Trade Commission. While I will concentrate on LEXIS–NEXIS' practices, we believe that these are typical of the practices of members of the IRSG.

Our company and the other members of the IRSG are committed to the responsible acquisition and use of personally identifiable information, and share the Subcommittee's concern about the potential misuse of data for identity theft and other harmful purposes. Indeed, in the fight against identity theft, where verifying an individual's identity is crucial, individual reference service products are absolutely essential.

My remarks today will focus on three areas. First, because most people know relatively little about our industry and may confuse the sort of services that are the topic of this hearing with the mainstream of the industry, I will explain the customer base and socially beneficial uses for individual reference information. For example, law enforcement agencies and fraud investigators are major users of these services, and at a 1997 FTC workshop on data base privacy the Secret Service, the Treasury Department's Financial Crimes Enforcement Network ("FINCEN"), American Bankers Association, and National Retail Federation all testified to the importance of these services for their work preventing and pursuing fraud.

Second, I will provide some background about the IRSG principles and their enforcement mechanisms. I also will illustrate some of the IRSG principles by explaining how LEXIS–NEXIS implements them.

Finally, I will make some observations about the impact of sections 7 and 8 of S. 2328 upon LEXIS–NEXIS and other individual reference services.

II. USES OF INDIVIDUAL REFERENCE SERVICE INFORMATION

Individual reference services are companies that furnish timely and reliable information to identify and locate individuals. The information is used by governmental, private sector, and non-profit entities for a wide range of beneficial purposes.

Individual reference services, such as those provided by LEXIS–NEXIS, are often the only way that individuals with limited resources, through the assistance of a professional who has access to these services, can obtain critical information. LEXIS–NEXIS' customers are professionals, primarily in the fields of law, business, journalism, and law enforcement.

For example, law enforcement agencies use these services to locate criminals and witnesses to crimes, and to confirm identities. In fact, individual reference services play an important role in combating the very sorts of fraud that flow from personal financial information falling into the wrong hands. At the June 1997 FTC workshop examining reference services, witnesses from both FINCEN and the Financial Crimes Section of the U.S. Secret Service testified to the value and importance of these services for their work.

In the fight against identity theft, where verifying an individual's identity is crucial, individual reference service products are absolutely essential. Banks, credit card companies, and other types of credit institutions, as well as gas, electric, and telephone companies and governmental entities distributing public entitlement programs, are all becoming increasingly plagued by fraudsters who use an existing person's identity to illegally obtain products, services and money. The best, and perhaps only, means of preventing this type of fraud is to crosscheck through the use of personal identifying data, often provided by individual reference services. Since the victims of identity theft are not only the businesses that lose billions to various forms of identity theft per year, but also the consumers whose credit is often ruined by this insidious act, everyone directly benefits by this application of the personal identifying information provided by individual reference services.

Individual reference service products also are an important tool for other types of fraud prevention efforts by businesses. The insurance industry, for example, relies on individual reference service products to investigate fraudulent claims. Credit card companies and department stores use them to detect and limit credit card fraud. Banks use them to detect and report credit card fraud, insider abuse, and money laundering. Many businesses use them to minimize the risk of financial fraud when they receive an unusual order for delivery of merchandise. Other businesses use them when performing due diligence before engaging in a business venture with a little-known corporation in the increasingly mobile world economy. The Insurance Information Institute reports that special investigation units save their companies about $10 for every dollar invested in them.

Reference services help people in many other ways. One of the most compelling is child support enforcement. Whereas government-compiled child support data bases have encountered difficulties in some instances, individual reference services have proven to be invaluable in tracking down parents who are delinquent in these obligations. In this way, these services advance personal responsibility, give much-needed income to divorced parents and their children, help free families from welfare dependency, and provide an additional source of revenue to state welfare programs. Individual reference services can locate non-custodial parents—quickly and inexpensively, even in circumstances where they move to a different state or begin using a different name. The Association for Children for Enforcement of Support ("ACES"), the leading child support advocacy organization, uses LEXIS–NEXIS' P–TRAK service to assist families—approximately 80 percent of whom are on welfare—in locating parents who have failed to meet legal child support obligations. ACES has reported tremendous success with the service, locating more than 75 percent of the "deadbeat" parents they sought, and helping families receive much-needed support.

Among the many other important uses of individual reference services are:

- finding long-lost family members,
- locating heirs to estates who have moved or changed their names through marriage,
- locating pension fund beneficiaries who have left a company,
- locating victims of fraud schemes or environmental hazards,

• protecting consumers from unlicensed professionals and sham businesses,
• locating blood, organ and bone marrow donors,
• promoting the transparency of the political process by providing easy-to-search information on individuals' campaign donations,
• locating witnesses, and
• providing citizens with efficient, ready access to Federal, state, and local government information.

From these examples, I hope the Subcommittee will appreciate the value of individual reference services.

III. THE IRSG APPROACH

Privacy Protection

Rapid advances in technology, a highly mobile society, the need to prevent fraud, and other market demands for information have spurred increased reliance upon information services provided by companies like LEXIS–NEXIS. These changes in society and technology also have resulted in a heightened interest in the privacy considerations implicated by such services. At LEXIS–NEXIS we are attuned to these issues and have strongly committed to taking a leadership role in effectively addressing them.

Privacy protection in the United States has evolved in a way that offers individuals effective protections while, at the same time, not limiting the benefits of technological advances. The ability to preserve both of these important interests results from a network of different policies. These policies are tailored to provide protections in specific circumstances in order to prevent actual or potential abuses of personal information. This sectoral approach is preferable to an omnibus or "one-size-fits-all" privacy policy that would govern all industries. Addressing privacy issues within specific industry sectors has proven very effective in evolving and responding to changes in industry and society.

The IRSG Principles

The importance of defining privacy practices tailored to specific types of information is demonstrated in the IRSG principles.

In September 1996, in the closing hours of the 104th Congress, the Federal Trade Commission proposed a broad prohibition on the use of credit header information—non-financial identifying information obtained from a consumer reporting agency's data base. Members of the individual reference service industry and those who rely on credit header information alerted Congress that such a prohibition would severely limit important uses of this information. As a result of arguments made by industry, regulatory efforts were postponed until a further study of the issues could be conducted.

This gave LEXIS–NEXIS the opportunity to join together with 13 other companies in the individual reference services industry to form the IRSG. The companies that comprise the IRSG are the leaders in providing information and assisting users in identifying and locating individuals. In close consultation with the Federal Trade Commission, the IRSG developed a comprehensive set of self-regulatory principles backed by third-party assessments and government enforcement that these companies follow.

These principles focus on non-public information, that is, information about an individual that is of a private nature and neither available to the general public nor obtained from a public record. For example, the principles govern information obtained from credit headers, such as social security numbers and addresses and telephone numbers.

Companies that sign on to the IRSG principles commit—among other things—to:

• acquire individually identifiable information only from sources known as reputable,
• restrict their distribution of non-public information through appropriate safeguards,
• educate the public about their data base services, and
• furnish individuals with a copy of the information contained in services and products that specifically identifies them, unless the information is publicly available.

One of the safeguards on the distribution of non-public information is a prohibition on the display of social security numbers and dates of birth in individual reference service products distributed to the general public and, for products distributed to professional or commercial users, a prohibition on the display of such information unless truncated in an appropriate manner (*e.g.*, masking of the last four

or more digits of social security numbers). This IRSG principle has helped reduce the availability of social security numbers for sale on the Internet.

Self-Regulation with "Teeth"

Third-party assessments backed by government enforcement provide real "teeth" for enforcing these principles. Enforcement rests on the following three pillars:

- Legal sanctions—Any company that holds itself out to the public as following the principles may be responsible under existing Federal and state law if the company fails to live up to them. Both the Federal Trade Commission and state attorneys general can bring charges under Section 5 of the Federal Trade Commission Act and similar state laws against member companies that fail to adhere the principles.
- Cut-off of data supply—Signatories to these principles require by contract that all companies buying non-public data from them for resale abide by the principles. Non-complying companies risk losing access to the data they need for their products or services. This is particularly significant in that it is estimated that IRSG signatories control 90 percent of all non-public information obtained from credit headers.
- Independent assurance reviews—Every IRSG company must undergo a third-party assessment to verify compliance with the principles. I will describe this in more detail below.

Information Practices

In the spirit of openness, the principles require individual reference services to have an information practices policy statement available to the public upon request. These statements describe:

- the types of information included,
- the types of sources from which that information is obtained,
- the nature of how the information is collected,
- the type of entities to whom the information may be disclosed, and
- the type of uses to which the information may be put.

This openness enables individuals to understand the reference service's use of the information it possesses. Individual reference services also inform individuals, upon request, of the choices available to limit access to or use of information about them contained in a company's products and services. Further, the principles require an individual reference service to provide information about the nature of public record and publicly available information that it makes available in its products and services and the sources of such information.

Third-Party Assessments

To help ensure that member companies do not make unsubstantiated assertions of compliance, the IRSG principles require that independent professional services conduct annual third-party assessments of their compliance. These independent professional services can be accounting firms, law firms, or security consultants who use the criteria developed by PriceWaterhouseCoopers for the IRSG.

When the principles were adopted in December 1997, these companies agreed that the assurance reviews would be completed within 15 months. I am pleased to report that this is the second consecutive year in which the companies that offer products that fall within the scope of the IRSG principles and subscribe to the principles have successfully undergone these assessments. As this milestone attests, the IRSG has made great strides through self-regulation to secure the benefits of information service resources and ensure effective protection of consumer privacy.

IV. LEXIS–NEXIS' PRACTICES: THE IRSG PRINCIPLES AT WORK

In addition to the IRSG principles, LEXIS–NEXIS maintains its own code of fair information practices. While these practices are based upon LEXIS–NEXIS' policies, they also provide an example of how the IRSG principles are implemented.

A. LEXIS–NEXIS Acquires Information Only From Reputable Sources

Section II of the IRSG principles requires that information be acquired "from only sources known as reputable in the government and private sectors." IRSG members are specifically required "to understand an information source's data collection practices and policies before accepting information from that source."

The majority of the information contained in LEXIS–NEXIS data bases is public record information. Moreover, a significant portion of the information we provide comes from publicly available information such as news reports. A few of our many data bases contain some information from non-public sources, such as credit header information (the non-financial, individual identifying information derived from the top of a credit report).

At present, we do not provide individually identifiable financial information from non-public sources. However, as discussed above, the IRSG principles are sufficiently broad to encompass, and would apply to, any member company's provision of this sort of non-public information.

Because most of our services offer public records, in many cases LEXIS–NEXIS obtains information directly from the government entity that originated it. In addition to governmental sources, the information gathered for our data bases is collected from a wide variety of other sources, some of which are large, well-known companies and smaller, lesser-known businesses. Regardless of the size of the source, in our acquisition of information, we must be confident that all of the information we obtain is owned by the sources and possessed in a legal manner. We review the data collection practices and policies of our sources before accepting information from them to determine whether the data they propose to furnish to us was compiled in a lawful and ethical manner. Furthermore, in order to continue to ensure the accuracy and acceptable origin of information in our data bases, we also engage in occasional site visits to evaluate directly the information practices of the source.

In addition, Section III of the IRSG principles requires that "[r]easonable steps be taken to help assure the accuracy of information in individual reference services." LEXIS–NEXIS has embraced this as one of our core policies for many years and through the IRSG we have reaffirmed our commitment to this important principle. LEXIS–NEXIS strives to obtain or create exact reproductions of the machine-readable versions of public records as copied and maintained by the official custodian of the records. We enter into written contracts with all of our sources that contain provisions attesting to the accuracy of the information the source provides LEXIS–NEXIS. These provisions instill confidence that our information is accurate by providing both a deterrent against providing us with inaccurate information, as well as recourse against sources that may violate these provisions.

LEXIS–NEXIS' commitment to accuracy, however, does not end with the contractual commitment from the source. We also engage in original source checks to verify that the source is in compliance with our agreement. From time to time LEXIS–NEXIS will go to the original jurisdiction where information is generated and compare samples of information obtained from the jurisdiction with the information provided to LEXIS by its source. This procedure allows us to measure the level of accuracy of our suppliers.

B. Security

Section VI of the IRSG principles requires signatories to maintain facilities and systems to protect information from unauthorized access and from persons who may exceed their authorization. LEXIS–NEXIS employs a wide array of measures to protect at all times the security of our products and the information obtained from our suppliers. Our security measures are deployed both within our computer systems and within our physical plant.

To establish security within our data base system, we employ the most effective security programming available. We constantly evaluate our system looking for weaknesses in order to eliminate them and upgrade security.

Our physical plant also uses the most effective security available, including state-of-the-art surveillance systems. Access to the various sections of our facilities is limited to authorized employees. This is done through the use of a "swipe-in"/"swipe-out" card system that allows us to account for individuals who are working in certain areas and the times that they are in these areas. Security guards, surveillance cameras, and other surveillance techniques also are employed. Our security system provides the highest level of accountability, and has proved extremely successful in eliminating unauthorized use of information. Additionally, all LEXIS–NEXIS employees are required to sign a non-disclosure agreement stating that they will not disclose confidential information to which they have access as part of their job responsibilities.

C. Selective and Limited Distribution

Section V of the IRSG principles addresses distribution of non-public information. Section V.A requires that individual reference services distribute non-public information only to qualified subscribers and sets out a lengthy set of conditions that determine these qualifications, as well as recordkeeping requirements concerning subscribers.

All of our subscribers enter into formal agreements with LEXIS–NEXIS that define the limits and appropriate uses of information obtained from our data bases. For example, in its customer agreements, LEXIS–NEXIS requires customers to agree contractually not to use information obtained from the data bases for purposes

that would violate the Fair Credit Reporting Act. In addition, a warning about FCRA restrictions is prominently visible to LEXIS–NEXIS customers before they access many of the data bases contained in the public record library, as well as files containing non-public information. This warning states:

> The Fair Credit Reporting Act (15 U.S.C. § 1681) prohibits use of information from this file to determine a consumer's eligibility for credit or insurance for personal, family or household purposes, employment or a government license or benefit.

To become a LEXIS–NEXIS subscriber, the prospective customer must furnish information including company/organization name, address, contact person and telephone number. We do not respond to anonymous requests for information, and we thus would be able to assist authorities in the event that subscribers were ever to misuse information.

V. ADVERSE IMPACT OF SECTIONS 7 AND 8 OF S. 2328

S. 2328 would directly affect individual reference services in two ways. First, section 7 would cut off the supply of the type of identifying information we obtain from consumer reporting agencies and use to help ensure accuracy in indexing and compiling disparate information. Second, section 8 would mandate that individual reference service companies enter a very different market than they ever sought to enter—the consumer market for public record information—as a condition of selling public record information to lawyers, law enforcement officials, journalists, and other professionals. These proposals are, at best, burdensome and unnecessary and, at worst, unconstitutional and harmful to consumers.

Section 7—Cutting Off the Supply of Identifying Information

In prohibiting consumer reporting agencies from supplying anything other than a consumer's name and current address without a "permissible purpose," as defined by the Fair Credit Reporting Act, section 7 would have the effect of cutting off identifying information that we use to index and organize disparate information. Distinguishing between "John Smiths" who live in the same town is far more effective when we have available to us prior addresses, age, and social security number information. These indexing and verification uses are critical to ensuring that the products we, and other IRSG members, offer to professional and government agencies contain accurate and complete information.

The use of social security number information for indexing and verification purposes is different than the display of such information in individual reference service products. As noted earlier, the IRSG principles prohibit the display of social security numbers and dates of birth in individual reference service products distributed to the general public and, for products distributed to professional or commercial users, prohibit the display of such information unless truncated in an appropriate manner.[1]

Cutting off the availability of social security numbers and similar identifying information for indexing and verification purposes is particularly ironic in light of the requirement in section 8, discussed below, that individual reference service companies provide consumers with copies of "their files," who in turn will probably review the information for accuracy and completeness.

Section 8—Consumer Review of Public Record Information in their "Files"

Requiring individual reference service providers, upon request, to disclose to a consumer "the nature, content, and substance of all information in the file maintained by the provider," is unnecessary, burdensome, and unwise.

Section 8's requirement is unnecessary insofar as the IRSG's access principle already requires an individual reference service to provide an individual with "nonpublic information contained in" its look-up products that specifically identifies him or her. (Two types of information are exempted from this requirement: information obtained on a limited use basis from a governmental agency and information whose disclosure is limited by law or legally recognized privilege.)

For public record information (and publicly available information) contained in an individual reference service's products, the IRSG principles require a company, upon request, to advise an individual about the nature of such information that it makes available in its products and the sources of such information. Public record informa-

[1] This IRSG principle has helped reduce the availability of social security numbers for sale on the Internet. The most common sources of such information today are Web sites operated by private investigators and Web sites selling "stale" information they obtained prior to the implementation of the IRSG principles.

tion is information about or related to an individual that has been obtained originally from the records of a Federal, state, or local government entity that are open for public inspection. Examples of public records include titles to real property, real property tax assessor records, bankruptcies, judgments, liens, state professional licenses, and death records.

When contacted by an individual concerning an alleged inaccuracy about that individual in its public record information, the IRSG principles further require an individual reference service company to inform the individual of the source of the information and, if reasonably available, where a request for correction may be directed. To be effective, any correction of errors must be made with the government entities that are the sources of this information. The task of individual reference services in this regard is to reflect reliably the data made available by the originating public record source.

Moreover, neither inaccuracies nor consumer harm are a significant issue in connection with individual reference services. Technological developments and quality assurance measures yield information that reliably mirrors the original public records. Furthermore, the FTC acknowledged in its 1997 Report to Congress on Individual Reference Services that "neither workshop participants nor commentators identified concrete evidence of harm linked directly to inaccurate records offered by look-up services." Nor has any evidence to the contrary emerged since 1997. In addition, statutory safeguards do exist for individuals in the vast majority of circumstances in which the distribution of inaccurate public record information might cause them real harm. For example, the Fair Credit Reporting Act already regulates extensively the use of public record information in connection with decisions about a consumer's eligibility for employment, credit, or insurance.

Weighed against this dearth of evidence of inaccuracies or consumer harm is the enormous potential burden associated with retrieving potentially relevant information from the large number of data bases of public records and verifying that it pertains to the individual making the request. This is necessary because many individual reference services, unlike consumer reporting agencies, do not maintain "files" in connection with specific individuals. For example, individual reference services leave to their customers the tasks of formulating their search inquiries, of personally reviewing the search results to determine whether the search might have been under-inclusive and, where the search inquiry is over-inclusive, of personally reviewing the search results to determine what records may be relevant. To meet the bill's demands, however, individual reference services would need to hire teams of customer service representatives, train them, and assume the risk of error in formulating search inquiries and making associated decisions. In short, it would force individual reference services to assume risks they long ago shifted to their customers.

Finally, section 8 would require that, as a condition of selling public record information to lawyers, law enforcement officials, journalists, and other professionals, individual reference services enter the consumer market for public record information. This is a very different market than most individual reference services ever sought to enter. Moreover, imposing this condition would run afoul of the First Amendment because it would unduly burden the publication of information already in the public domain. See, e.g., *The Florida Star* v. *B.J.F.*, 491 U.S. 524 (1989) (striking down statute that imposed civil liability upon a newspaper for publishing the name of a rape victim which it had obtained from a publicly released police report); *Smith* v. *Daily Mail Publishing Co.*, 443 U.S. 97 (1979) (finding unconstitutional the indictment of two newspapers for violating a state statute forbidding newspapers to publish the name of any youth charged as a juvenile offender).

VI. CONCLUSION

Our company and the IRSG are committed to the responsible acquisition and use of personally identifiable information, and share the Subcommittee's concern about the potential misuse of data for identity theft and other harmful purposes. Nevertheless, individual reference service products are absolutely essential in the fight against identity theft, and the Congress should not take any steps that would jeopardize the usefulness of such services.

Senator KYL. Thank you.

Mr. Pratt.

STATEMENT OF STUART K. PRATT

Mr. PRATT. Chairman Kyl and Senator Feinstein, let me join with the others who have testified already and thank you very

much for holding this hearing. It is important to us, as the Associated Credit Bureaus, because we represent 500 or so companies out in the marketplace who, in fact, are the information companies who ultimately have their data bases polluted by the crime of identity theft.

Mr. Chairman, in particular, we thank you for your thoughtful leadership on the enactment of the Identity Theft Assumption and Deterrence Act of 1998. It was the right step, it was the right time. In fact, at several hearings that I have attended—and one of the reasons we go to these hearings is that it isn't just a matter of telling you what we think. It is a matter of hearing what else is said.

Each time I hear a victim, it gives me a chance to go back to our own industry and make it more real to our chief executives, to encourage them to be more efficient, to make sure that they understand that we all have personal lives. I have two children and they go to swim team and they do other things, and if I am spending most of my time unraveling a problem, I am not spending my time on what I guess I would think of as higher priorities in our personal lives.

In fact, that is really what drove the Associated Credit Bureaus to establish an identity theft task force that consisted of the chief executive officers. It was a longitudinal process. We actually hired a former attorney general to work with us and we have launched our first series of initiatives. They were announced March 14 and were a part of the identity theft summit that was hosted by the Department of the Treasury earlier this year.

We are not finished in terms of our work. I think it is time for industry to be progressive. It is time for industry to look at what we can do. I remember Jim Bauer a number of years ago testifying, in fact, to a Senate Banking Committee subcommittee encouraging industry to step forward and take its responsibility seriously in terms of how this crime affects consumers. It is invasive, it is longitudinal. There is a snarl of problems that result from this, and I think each one of us has our role in trying to solve that problem. We are unhappy, again, with that data that is in our file that is inaccurate that causes a legitimate consumer to not have access to the benefits and the services that they would like to have in this society today.

So with that, let me just focus a few comments on the types of initiatives that we have undertaken so far, at least some of which are consistent with some of the ideas we have heard discussed already.

We think it is very important that we do what we can to improve both the use of and the effectiveness of the security alerts that we add to the credit files. You have heard testimony today saying are these effective. We want them to be effective, obviously. So, in fact, just this past month we have decided to standardize both the literal statement as well as the coding of what goes into a security alert to ensure that our customers across any technology platform can look for and identify that security alert to make sure that they can then take the actions that they feel are appropriate.

We also think that consumers, when they are calling three different consumer reporting agencies for credit fraud, for example, need an even experience. We interviewed victims who said, you

know, it is hard for me if you are asking for this data, but you are asking for this data; you ask me to jump through this hoop, but you ask me to jump through this hoop. So can we harmonize, can we standardize some of that experience?

We are moving to standardize the advice we give consumers. We are moving to standardize the communications that we give to consumers. We are moving, in fact, to standardize what steps we take first in the process for consumers.

Another step was, in fact, even on a weekend where a consumer would get an automated voice attendant potentially rather than get live personnel. One of the keys is to assure that consumers have confidence in what is being done. I think I heard testimony today, and I have heard this before: I am still not sure I feel good, I am not sure I am safe.

We want to create a safer world, and so in our case we will add a security alert automatically even if you just leave a message—no verification, no authentication, no hoops. So, that is going to be a change that we are making this year.

We will also take you out of all pre-screened offers of credit automatically, no verification, no efforts to check further, but just do it. And we will also issue your file within 3 business days and get that out into the mail so that you can look at that file, and then you will have access to an 800 number and live personnel where you can continue the process of working through this.

We will escalate communications to credit grantors even where we do not yet see credit on the file. This is a change in our practices, so that we will communicate electronically through a network that we have established and funded through the 1990's which allows us to communicate with a majority of our data furnishers so that even where there is just what we call an inquiry on the file, and if a consumer says I don't recognize doing business with that bank, and we don't see an account yet on the file, but we wonder what is happening, is there something in the pipeline, that is part of the longitudinal effect. You see what is on the file. It is a snapshot, but there may be more that is cycling in, and this is the experience that consumers have. It seems to go on and on and on.

One of the most important steps I think we have taken is that we are going to build new software technologies that will be available within 7 months of that announcement we made earlier this year. We are going to monitor the file, and I think this is going to help solve one of the problems.

One of the problems is that consumer says, "You know, it is on my shoulders to check the file, and to check it again and check again and make sure I am still OK." Well, we are going to trigger communications to consumers where we see unusual file activity. We are actually going to mail or communicate with that consumer and say we have seen something happen to your file that doesn't look right, can you call us again on the 800 number, free of charge, and escalate our linkage with the consumer who has been victimized.

Again, I think it makes good business sense, by the way, to keep the file clean once we have gotten it cleaned back up again. But we can't be confident that all of the credit problems out there have

been cleaned up as well. So we have to try to keep it clean by staying in touch with that consumer.

So, that is a sampling of the efforts that we are undertaking, and we have more on the way, actually. I have a conference call next week with another segment of our industry to further refine and take some additional steps to try and build these efficiencies into the system.

So I am happy to be here today. We are happy to answer your questions and we appreciate the opportunity you are taking to learn and get the big picture of what is happening on this issue of identity theft.

[The prepared statement of Mr. Pratt follows:]

PREPARED STATEMENT OF STUART K. PRATT

Mr. Chairman and Members of the Subcommittee, my name is Stuart Pratt and I am vice president of government relations for the Associated Credit Bureaus, headquartered here in Washington, D.C. ACB, as we are commonly known, is the international trade association representing over 500 consumer information companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services, and collection services to hundreds of thousands of customers across the United States and the globe.

Our members are the information infrastructure that contributes to the safety and soundness of our banking and retail credit systems; which:

- allows for the efficiencies of a secondary mortgage securities marketplace that saves consumers an average of 2 percentage points on the cost of a mortgage.
- helps e-commerce and bricks-and-mortar businesses authenticate applicant data, thus reducing the incidence of fraud.
- gives child support enforcement agencies the information tools necessary to accomplish their mission.
- allows states to reduce the incidence of many forms of entitlement fraud.

On behalf of ACB, I want to commend you for holding this hearing on the issue of identity theft and for your efforts in the previous Congress, leading to the enactment of the Identity Theft Assumption and Deterrence Act of 1998. Identity theft is an equal-opportunity crime that can affect any of us in this hearing at any time. It is a particularly invasive form of fraud where consumers, consumer reporting agencies and creditors must untangle the snarl of fraudulent accounts and information resulting from a criminal's actions. This task is often frustrating and time-consuming for all concerned.

Before I specifically address how our industry has responded to the needs of creditors and victims of identity theft, I have found it helpful to provide a short review of what a consumer reporting agency is, what is contained in a consumer report, and the law that governs our industry.

CONSUMER REPORTING AGENCIES AND CONSUMER REPORTS

Consumer reporting agencies maintain information on individual consumer payment patterns associated with various types of credit obligations.[1] The data compiled by these agencies is used by creditors and others permitted under the strict prescription of the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) to review the consumer's file.

Consumer credit histories are derived from, among other sources, the voluntary provision of information about consumer payments on various types of credit accounts or other debts by thousands of data furnishers such as credit grantors, student loan guarantee and child support enforcement agencies. A consumer's file may also include public record items such as a bankruptcy filing, judgment or lien. Note that these types of data sources often contain SSN's as well.

For purposes of data accuracy and proper identification, generally our members maintain information such as a consumer's full name, current and previous addresses, Social Security Number (when voluntarily provided by consumers), date of birth

[1] Our members estimate that there are approximately 180 million credit active consumers. Since our members operate in competition with each other, these consumers are likely to have more than one credit history maintained.

or age, and sometimes places of employment. This data is loaded into the system on a regular basis to enhance the completeness and accuracy of data.[2]

It is important to note that the vast majority of data in our members' systems simply confirms what you would expect: that most consumers pay their bills on time and are responsible, good credit risks. This contrasts with the majority of systems maintained in other countries, such as Japan, Australia, or Italy, which store only negative data and do not give consumers recognition for the responsible management of their finances.

As important as knowing what we have in our files is also knowing what types of information our members *do not* maintain in files used to produce consumer reports. Our members do *not* know *what* consumers have purchased using credit (e.g., a refrigerator, clothing, etc.) or *where* they used a particular bank card (e.g., which stores a consumer frequents). They also do not have a record of *when* consumers have been declined for credit or other benefit based on the use of a consumer report. Medical treatment data is not a part of the data bases, and no bank account balance information is available in a consumer report.

THE FAIR CREDIT REPORTING ACT (FCRA)

In addition to our general discussion of the industry, we believe it is important for your Subcommittee to have a baseline understanding of the law that regulates our industry. Enacted in 1970, the Fair Credit Reporting Act was significantly amended in the 104th Congress with the passage of the Credit Reporting Reform Act.[3]

Congress, our Association's members, creditors and consumer groups spent over 6 years working to modernize what was the first privacy law enacted in this country (1970). This amendatory process resulted in a complete, current and forward-looking statute. The FCRA serves as an example of successfully balancing the rights of the individual with the economic benefits of maintaining a competitive consumer reporting system so necessary to the efficient operation and growth of a market-oriented economy.

The FCRA is an effective privacy statute, protecting the consumer by narrowly limiting the appropriate uses of a consumer report (often we call this a credit report) under Section 604 (15 U.S.C. 1681b), entitled "Permissible Purposes of Reports."

Some of the more common uses of a consumer's file are in the issuance of credit, subsequent account review and collection processes. Reports are also, for example, permitted to be used by child support enforcement agencies when establishing levels of support.

Beyond protecting the privacy of the information contained in consumer reports, the FCRA also provides consumers with certain rights such as the right of access; the right to dispute any inaccurate information and have it corrected or removed; and the right to prosecute any person who accesses their information for an impermissible purpose. The law also includes a shared liability for data accuracy between consumer reporting agencies and furnishers of information to the system.

FRAUD PREVENTION AND IDENTITY THEFT

Let me now turn to our industry's efforts with regard to fraud. Our industry has a history of bringing forward initiatives to address fraud. These efforts focus on use of new technologies, better procedures and education.

Consider the following efforts undertaken during this past decade:

- ACB formed a Fraud and Security Task Force in 1993.
- A "membership alert form" was developed for use in notifying other ACB credit bureau members of customers who were committing fraud through the misuse of data. Implemented in 1994.
- A "Universal Fraud Information Form" was developed for use by creditors when communicating the incidence of fraud to national consumer reporting systems.
- The credit reporting industry developed a comprehensive presentation on ACB fraud and security initiatives for delivery to customer segments during 1995.
- Minimum standards for data access equipment and software were announced to industry suppliers in March 1995.

---

[2] Note that there are in fact a number of major credit reporting systems in this country. Within ACB's membership the three most often recognized systems are Equifax, Atlanta, GA; Experian, Orange, CA; and Trans Union, Chicago, IL. These systems not only manage their own data but also provide data processing services for the over 400 local, independently-owned, automated credit bureaus in the Association's membership.

[3] Public Law 104–208, Subtitle D, Chapter 1.

• ACB members have implemented company-specific limitations on the availability of account numbers, and truncation of Social Security Numbers on consumer reports sold to certain customer segments.
• Experian, Equifax and Trans Union voluntarily formed special fraud units with toll-free number service and consumer relations personnel specially trained to work with fraud victims.
• A hardware and software certification program has been created by the industry and administered by a third-party certification authority for those access products, which have implemented industry security standards.
• Over 150,000 copies of a new customer educational brochure entitled "We Need Everyone's Help to Protect Consumer Privacy and Reduce Fraud" have been distributed since its first printing in 4th Q. 1997. An education program was also developed for use by ACB members in presenting the information found in the brochure. 2nd Q. 1998.
• On March 14, 2000, the ACB announced new voluntary initiatives to assist consumers who have been victimized by identity theft. Following is a description of each initiative and also attached is our press release.
• Advocate the use and improve the effectiveness of security alerts through the use of codes transmitted to creditors. These alerts and codes can help creditors avoid opening additional fraudulent accounts.
• Implement victim-assistance best practices to provide a more uniform experience for victims when working with personnel from multiple fraud units.
• Assist identity theft victims by sending a notice to creditors and other report users when the victim does not recognize a recent inquiry on the victim's file.
• Execute a three-step uniform response for victims who call automated telephone systems: automatically adding security alerts to files, opting the victim out of prescreened credit offers, and sending a copy of his or her file within three business days.
• Launch new software systems that will monitor the victim's corrected file for 3 months, notify the consumer of any activity, and provide fraud unit contact information.
• Fund, through ACB, the development of a series of consumer education initiatives through ACB to help consumers understand how to prevent identity theft and also what steps to take if they are victims.

CONCLUSION

In conclusion, you can see by our actions that our members have a history of combating fraud of all types including identity theft. We were the first industry trade association to form a task force to consider how best to address the plight of victims who through no fault of their own are left with, as we said at the beginning of this testimony, a snarl of fraudulent accounts to deal with.

Along with our progress, there are a few cautionary thoughts that I would like to leave with each of you. It is difficult for laws to prescribe procedures and practices that actually prevent crime. Crime is a moving target and, thus, our fraud prevention strategies must be as agile as the tactics of the criminals.

Information is a key economic growth factor in this country. Laws that limit legitimate and beneficial information use are most likely to take fraud prevention tools out of the hands of legitimate industry. Ironically, to prevent fraud, we must be able to crosscheck information. Absent this ability to authenticate identifying information, we will be less able to prevent the very crime we are discussing here today.

I think the initiatives I have discussed here today provide ample evidence that our industry is serious about doing its part in reducing the crime of identity theft and fraud and in helping consumers restore their good name and an accurate credit file. Just as it is to consumers, the integrity, accuracy and reliability of the credit files our members maintain is vitally important.

Thank you for this opportunity to testify.

NEWS RELEASE

[Norm Magnuson]

CREDIT REPORTING INDUSTRY ANNOUNCES IDENTITY THEFT INITIATIVES

Associated Credit Bureaus, the international trade association for the consumer reporting industry, announced today a commitment on behalf of the nation's leading

credit reporting agencies to voluntarily implement a comprehensive series of initiatives to assist victims of identity theft in a more timely and effective manner.

> "While there is no evidence to show that the credit report is a source for identity theft, our industry has always taken an active role in assisting consumers who are fraud victims. Our members have taken this responsibility seriously, and we're very proud of these initiatives that help consumers who are victims of identity theft or fraud," noted D. Barry Connelly, president of Associated Credit Bureaus. "Designing and implementing these initiatives is a significant milestone in the ongoing efforts of our industry to help address the problem of identity theft. As long as there are criminals who prey on innocent consumers, we will continue to seek even better ways to serve consumers and work with law enforcement and our industry's customers to address this threat."

Connelly outlined the industry's six-point program to improve identity theft victim assistance:

- Advocate the use and improve the effectiveness of security alerts through the use of codes transmitted to creditors. These alerts and codes can help creditors avoid opening additional fraudulent accounts.
- Implement victim-assistance best practices to provide a more uniform experience for victims when working with personnel from multiple fraud units.
- Assist identity theft victims by sending a notice to creditors and other report users when the victim does not recognize a recent inquiry on the victim's file.
- Execute a three-step uniform response for victims who call automated telephone systems: automatically adding security alerts to files, opting the victim out of prescreened credit offers, and sending a copy of his or her file within three business days.
- Launch new software systems that will monitor the victim's corrected file for three months, notify the consumer of any activity, and provide fraud unit contact information.
- Fund, through ACB, the development of a series of consumer education initiatives through ACB to help consumers understand how to prevent identity theft and also what steps to take if they are victims.

ACB's initiatives, to be fully implemented within seven months of this announcement, resulted from a task force comprising senior executives from the ACB Board of Directors and former State Attorney General, M. Jerome Diamond. Diamond interviewed consumer victims and law enforcement officials, made onsite visits to credit reporting agency fraud units, and obtained input from privacy advocates. His counsel was an integral part of the decisionmaking process and influenced the final content of the initiatives.

Connelly said: "Identity theft is a crime that is deeply unsettling for the victims. Our initiatives will make it easier for victims to put their financial lives back together." Connelly stressed, though, that the crime extends beyond individuals to creditors and ACB members and added, "We must all work together in the areas of prevention and victim assistance. We supported the enactment of the Identity Theft Assumption and Deterrence Act of 1998 and have worked with more than half of the State legislatures on similar laws. We urge law enforcement to vigorously investigate and prosecute the criminals."

Associated Credit Bureaus, Inc. is an international trade association representing 500 consumer information companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services, and collection services.

Senator KYL. Thanks very much, and thanks to all of you.

Let me ask Senator Feinstein to begin. I will have to step out for just a moment and be right back.

Senator FEINSTEIN. Thanks, Mr. Chairman.

Mr. Pratt, I was very heartened by your testimony. Let me just thank you for making changes in your system. One of the problems that we have had is that identity theft victims report that they have difficulties getting in touch with a person, as opposed to a recording, when they call a credit bureau to report an incident. And they are frustrated at having to call each of the major main credit bureaus to report identity theft.

Is what you are saying that you will have this systematized so that one call will be able to reflect through all credit bureaus?

Mr. PRATT. It is a discussion item. I can't tell you yet that that is where we will end up, but I will tell you that what we want to be able to do is make sure that a consumer who calls knows what is going to happen and has confidence in what will happen so that they aren't frustrated, even if it is Sunday night that they are learning about the problem and they are making that phone call on a Sunday. Whether they are calling and getting live personnel or not, either way we want to make sure that experience is fairly standardized.

We have other data bases out there, Senator Feinstein, and we are looking at how we can make sure that across a larger spectrum of data bases consumers don't end up making more and more phone calls down the road to help with that efficiency.

Senator FEINSTEIN. How many credit bureaus are there?

Mr. PRATT. Well, there are three major credit reporting systems that I think we commonly think of. There is a total of 500 members in the Associated Credit Bureaus, some of whom produce mortgage reports, some of whom produce employment screening reports or tenant screening reports of various types. There are check services data bases. One million two hundred thousand fraudulent checks are written a day in this country.

Senator FEINSTEIN. Well, let me ask you, if Michelle, for example, wanted to call a credit bureau to say, "Look, I have got a problem," how many calls would she have to make now?

Mr. PRATT. I think today she would make three main calls, and with those major calls we would be able to take those steps, making sure that a security alert works, but take those steps that a security alert works and is effective, take the steps that she wants us to take, and so on; three main calls.

Senator FEINSTEIN. It would really be helpful, I think, if an individual could make one call, and as a product of that call the word could go out and they wouldn't have to do the rest of it.

Mr. PRATT. I think that is an idea that goes far back, and let me just say that, of course, Jodie Bernstein has been a real thought leader and her division has been a real thought leader in the area of identity theft, even as far back as some of the workshops. We still have some of those ideas plugged into the decisionmaking process to take the right steps in the right order.

Senator FEINSTEIN. Do you know how much business is actually generated by the sale of marketing lists with Social Security numbers?

Mr. PRATT. I really don't.

Senator FEINSTEIN. Mr. Emmert, the FTC has made some recommendations to my staff for the improvement of 2328, particularly sections 7 and 8 that you spoke about. I would like to ask that you talk with Tom Oscherwitz of my staff and go over these and see if they satisfy your concerns.

I was reading the bill while you were speaking, and I really didn't quite understand what the heart of your concern was. Can you repeat that again?

Mr. EMMERT. Sure. Thank you, Senator, and we would be very happy to work with you and with Tom on the language.

One of the issues that we have is the same comment that Inspector General Huse made, which is you should prohibit the sale of

Social Security numbers. I think you should prohibit the sale in the consumer marketplace of Social Security numbers, but there are sales that happen in a more restrictive environment that we believe need to happen that will, in fact, be counterproductive if you stop them. When we obtain a list of names, addresses and Social Security numbers from the credit bureaus, that is a sale.

Senator FEINSTEIN. Go over what those are, those instances.

Mr. EMMERT. Yes. What we will do is we will acquire data in a large set and then we will, in turn, sell it on a limited basis to a very finite group of customers that include government law enforcement agencies, fraud investigation groups within insurance——

Senator FEINSTEIN. Well, now, there is an exception for that in the bill. Keep going.

Mr. EMMERT. OK. We also need an exception for us so that we can obtain it to begin with.

Senator FEINSTEIN. Right.

Mr. EMMERT. You have insurance companies who have fraud investigations units, many of which are established as mandated by State law. The insurance companies are very big on this. I believe the statistics show that they save $10 for every $1 they spend on fraud investigation. So they are very big on it, but it is private sector-type law enforcement activity.

You have similar issues with the securities industry and with the banking industry. We have child support enforcement work. We have work with groups that locate missing children. These are activities that we think that arguably we should support and that we would like to continue to be able to support.

We don't try to defend the use of Social Security numbers for marketing or solicitation. It seems unnecessary. I don't need to be able to get my neighbor's Social Security number just because I am curious, and so a website that would make that information available to the general public—I don't want to defend that practice. I think it is reprehensible, and it is a huge feeder for the types of persons who would commit fraud. So, that is not what we are trying to defend. It is the notion of "no sale" that is the problem because there are behind-the-scenes types of transactions that need to continue.

Senator FEINSTEIN. I think we are prepared to make specific technical exceptions. As you said, the Social Security number is one thing and other data is other things. If you would work with our staffs, perhaps we can work this out. One bill is just the Social Security number. Another one that I am looking at is also the driver's license, personal financial data, and personal health data.

Mr. EMMERT. All of those are areas that have slightly different issues. The driver's license issues are slightly different from the health data and the financial data. We are not in the market of distributing health or financial data. We don't want to be in that market. We don't want to be disseminating people's medical records or their personal financial records. Again, I would agree there are reasons why you don't want that in the general marketplace, in the public.

Driver's license records are an interesting category because, first, they are public records. And, second, they can be used to help with a number of functions. Again, the Drivers Privacy Protection Act

has helped to restrict those uses considerably, and I will point out that even under the most restrictive interpretations that have come through on the recent amendments, 96 percent of our current customer base qualifies under the most restrictive amendments because, again, we don't sell for marketing or commercial solicitations or to members of the general public who have curiosity.

We are selling to law enforcement, we are selling to the courts, we are selling to attorneys who are working on litigation, things of that nature. And so our concern is that we can protect those uses which we believe are socially beneficial. But we would be more than happy to work with you and your staff on this.

Senator FEINSTEIN. Great. I am a big fan of NEXIS–LEXIS.

Mr. EMMERT. Thank you, Senator.

Senator FEINSTEIN. On this personal financial data, I have been told that there are places where I could purchase every mortgage you have ever had, who gives the mortgage, what you have owing on the mortgage, any delay in payment you may have made, where the houses or house or property or whatever it might be is, so that by buying this information, I could actually develop a very good financial profile of you, any weaknesses you might have, any strengths you might have. I find that very dangerous to have out there in the public marketplace.

Mr. EMMERT. A couple of comments on that. First, my friend Stuart here may, in fact, have that information, but we do not. What we do have is we do have information about real estate titles. As you know, lawyers do title searches. They help you when you go to purchase a house or when you go to sell a house. What we make available are the public records themselves that you get from the county recorder's office.

So for a particular parcel of land, we can show who the owner of the record is, where the parcel is situated, and a legal description of the parcel. If there are liens currently in existence against the parcel, the liens would show on the title. That is so when you go to buy a house, you don't pay $200,000 for a house, only to find out that there is also a $150,000 tax lien that you personally are now liable for because nobody found it when you made the purchase and it wasn't settled. And so that basic information is available. Also, you may find things like the assessed tax value of the property. What are the property taxes on the property? What is the assessed value for tax purposes?

In terms of the mortgages, I believe the initial mortgage amount is stated on some of the deeds. These are records that we don't create. We don't necessarily dictate what is in these records. We simply report them as they are recorded in the county recorder's office. It would not show the amount of the payment. It would not show the current balance of the mortgage, it would not show prior mortgages, but it may show a second mortgage which would be filed as a matter of record against the property as a lien.

Senator FEINSTEIN. Can anyone get this information if they are on some kind of a fishing expedition to find a good victim?

Mr. EMMERT. Well, anyone can get this information at the county recorder's office today in any county in the country. It has been a public record for as long as we have had land records in this country. So in that sense, the answer is yes.

Senator FEINSTEIN. But it is difficult to get.

Mr. EMMERT. Well, it is, but again you look at the distributions. Certainly, for our company we have a fairly limited distribution. We have a lot of users, but the users tend to be in professional categories in the law enforcement community, in major law firms, and in large corporations. It is not something that we make generally available to the populace at large over the Internet.

Legally, that can be done because those records are public. Even if you can't afford a lawyer, even if you are not with a law enforcement agency, you are entitled to go down to the county recorder's office to find out when that tax bill comes in whether your next-door neighbor's property has been assessed at the same basic level as yours is.

I just went through that. I bought a new house. I had been in the house less than 6 months and the assessed property value was significantly above what I paid for the property. Well, I am entitled under the law to go over and see how did they assess the other properties on the street. Am I being treated fairly with respect to my neighbors? That is one of the reasons that those records are available to the public. I don't have to hire a lawyer to do it. I can do it myself.

So there are some touchy issues here in a free society because we want to protect persons from fraud, from theft, certainly from any scenario of that nature. But it is kind of a fine line between protecting people and allowing people to sort of protect themselves as well in other contexts.

Senator FEINSTEIN. Thank you very much. Mr. Pratt, did you have something you wanted to add at one point?

Mr. PRATT. I think Steve really covered some of the basic points. We would have mortgage information in a consumer file that might show payment information, but that would be controlled by the Fair Credit Reporting Act. So in that case, a privacy statute is in place which limits distribution.

Obviously, that is a great challenge you have going forward, and I know Tom and you and others on your staff are working through that, about what does Graham-Leach-Bliley cover, what does it not cover, what does Fair Credit cover and what does it not, and so on and so forth. So this is the policy issue that we are in today, how to parse through the laws that currently exist and to look for, I guess, the element which might lead to injury somewhere down the road.

Certainly, another context for mortgage information being available is the efficiencies for a mortgage lending system today, the fact that we securitize an enormous amount of primary market loans into secondary markets. And in those large automated underwriting contexts, the ability to draw from electronic data bases which create the efficiency—that is, a business-to-business transaction—allows them to do very inexpensive assessments of values of property which allows them, in fact, to approve up to 70, 75 percent of the loans without all of the normal expensive closing costs processes that we have seen in the past. So there are those issues to think about when you are thinking about this larger context of public record and the availability of it, and what are the basic tenets of why it was there in the first place.

I have lived in other countries. Land ownership in this country is kind of taken for granted in a lot of ways. We live in a very stable society, comparatively. In a lot of countries, people don't know who owns the land. They don't know why it is being owned. They don't know who controls large swaths of property.

That was one of the fundamental tenets behind the idea of making ownership available. Environmental groups today use ownership records of that sort to track down who, in fact, really controls land, who, in fact, controls wetlands, who can build on it, who cannot, that sort of thing. So are these other societal benefits that just have to be weighed in context. Unfortunately, I guess that is the job of U.S. Senators, to try to divine the truth in all of that.

Senator FEINSTEIN. Thank you. Thank you, Mr. Chairman.

Senator KYL. The old saying "knowledge is power" is really the fundamental of this hearing. That knowledge can be very powerful in a very positive way. That is primarily what has permitted the Internet and this kind of technology to benefit our society in such a significant way.

But as we point out in this hearing, it can also be used in a very powerful negative way, and the trick here is to find the proper balance to protect people from the kind of extraordinarily harmful activity that can occur, while not unnecessarily interfering in the free flow of information for positive purposes.

I was struck, Senator Feinstein, by the fact that if we could have these four witnesses sit down with us, we could probably craft a very, very good bill, with all of the information that is represented at this table.

Incidentally, we may have a vote any minute here, and when that vote is called, we will have about 7 or 8 minutes to conclude the hearing and then we will have to finish, but that perhaps will be enough.

Ms. Brown, I was going to ask you what assisted you the most in your efforts to clear your name, and then, second, to what extent did you receive assistance from the FTC. You have given us in writing a lot of great recommendations, some of which are being pursued, some we need to pursue. And if you would like to add anything else there orally, that would be fine, too.

Ms. BROWN. I would say that the first resource that I found actually was the Privacy Rights Clearinghouse. And I did searches on the Internet for identity fraud that assisted me in certain steps to take to not only report the crime, but also to try to prevent further misuse of my name.

Senator KYL. By the way, did you find that on the Internet?

Ms. BROWN. On the Internet, yes, rapid information. That is exactly why I went there. I didn't know where else really to turn. If I didn't have access to the Internet, I am sure that it would be a very, very lengthy process to figure out what steps logically—where to go, to call the DMV, to call the Social Security agency.

I looked onto, say, FBI sites and Secret Service sites, but generally at that point the initial thing that I knew about was the car loan. That was only $32,000, and to get into something of the FBI and Secret Service, my case did not apply yet. I think maybe down the line, it could have.

So I think that those resources from the FTC websites and the Privacy Rights Clearinghouse give great information of how to go about clearing the process. But I didn't receive any further assistance from anybody. It was all just my own diligence and my own persistence in calling the police departments, and so forth. And like I said, there were many times that authorities were not sensitive to my plight.

I actually called one time to the LAPD when I found out that something had occurred in the L.A. County, basically, and that is where I was to file a police report. I was told blatantly not to bring the case there because, as the guy was laughing, you know, he did not want a burdensome case like that. So, often, there weren't resources and it was just my persistence in going forward. And from there, it was just logical. When you make a fraud report, they send you documentation, they send you forms to fill out, and you just continue to do that at every step of the way.

Senator KYL. And, of course, one of the things you suggested is much more uniformity in that.

Ms. BROWN. Absolutely.

Senator KYL. And we have heard here that that is a step that is at least to be pursued.

Ms. BROWN. Absolutely.

Senator KYL. Did you talk to anybody at the FTC ever, and did they provide any specific help?

Ms. BROWN. Off the top of my head, I don't recall, but I have extensive notes of every single phone call that I made.

Senator KYL. Did you ever get a letter, a document that you could carry with you, the kind of thing that Ms. Givens talked about?

Ms. BROWN. When I found out that there was a warrant out for my arrest, then I specifically requested from the police detective that was working on my case—I filed a police report in January 1999. This is June 1999 when I found out I had a warrant out for my arrest. Up until that point, even though I filed a police report, I didn't have anything in my hand, really, aside from a statement that I did file with my local police, because I actually feared for my life and if something happened to me, I wanted some record of that.

From that, I had a 1-page sheet that said that I had reported identity theft, basically. But up until that point, no, I had not received anything in my hand to show my innocence. And because I was leaving the country and there was a warrant out, I specifically requested this. But in most cases, I don't think that victims would really be allowed that information. Sometimes, you don't know that there is a clear perpetrator. I knew blatantly because she went to the DMV, and from their records, after they pulled that information, it was clear someone had impersonated me.

Senator KYL. So did you eventually get some kind of a document that you could carry with you?

Ms. BROWN. From the courts, yes, after she was tried.

Senator KYL. So that was late in the process?

Ms. BROWN. September 1999.

Senator KYL. And just describe that document briefly.

Ms. BROWN. Initially, I received a letter from the probation officer saying that she was going to be convicted on such-and-such date; you are allowed to put in a victim statement, and so forth.

Senator KYL. Excuse me. But when you try to come in the country from Mexico, that wouldn't——

Ms. BROWN. Exactly. When I came back from Mexico, that is what I had in hand. I also had a letter from the detective. Those were the only things I had in hand—well, not necessarily. I also have certain statements and documentation of filing disputes with credit agencies, and so forth. But the real document came from her conviction in the San Diego court in September 1999, and I specifically requested this out of the court that I wanted them to say this person of such-and-such description, and to provide my description——

Senator KYL. Alias your name.

Ms. BROWN. Used my name to perform all of these acts, you know, burglary and what not.

Senator KYL. Let me ask Ms. Givens, you talked about a specific document. And this is one of the things I had in mind when we introduced our original bill and it didn't come out exactly the way I sort of had thought about, but there was at least some reference to it.

What would you recommend, understanding that there are different kinds of cases and there are different times in the process here, but to try to respond to the precise problem Ms. Brown had? What kind of document or series of documents could we provide for? And I would think that this could be done, by the way, perhaps without legislation. It doesn't necessarily have to be a Federal law.

Ms. GIVENS. Well, we are working on two bills in California that you might want to look to as models. One would be an expedited court process where you would get a document from the court in the jurisdiction where the arrest or the conviction happened. And, by the way, you have to deal with both arrests and convictions. Michelle's case is horrible, but the one good thing is that the perpetrator was convicted and is in prison. That is a rarity.

Most of the time, you are dealing with a nefarious unknown, and you have an arrest warrant and you don't know where they are or what they are doing. So you need to be able to address both arrests and convictions. But perhaps something that you go through your local law enforcement that goes to that court, an official document from the court, but the document must be accepted by U.S. Customs, by the FBI.

We have the case of a man who has a document for bad check-writing that he carries with him. He came back into the country and was jailed. U.S. Customs did not accept that document even though it was from the courts in Missouri, and he lives in New York City. And that was for bad check-writing. So there has to be something that is standardized, that is official, that is acceptable to all levels of law enforcement.

Senator KYL. And it seems to me also something that pre-dates an actual conviction like this or arrest. You may have nothing more than the beginning of learning of the event, two or three bad things that you find out about. You report it to, say, the credit bureaus. You are starting the process of clearing your name, but I mean at

that point it seems to me there is so much about your life that is now going to be implicated in this that it would be useful to have something from the FTC or somebody that says this person has at least been reporting some really bad anomalies. There would have to be some kind of verification—and we can verify that at least the first one reported was, in fact, an anomaly, and so listen to this person. When she tells you there is something wrong, listen to her.

Senator FEINSTEIN. I think we might look at a statement or a letter signed by the chief law enforcement officer of the jurisdiction that she has at least filed a case and that an investigation is going on, and that he or she may well be the unwitting victim of identity theft. The problem is you don't want guilty people to go and get this document as well.

Senator KYL. No.

Senator FEINSTEIN. Therefore, it has to be something that has some personal attention given to it. It would seem to me the local law enforcement agency would be the best source because they know whether the complaint, A, is valid or not; B, whether there are really suspicious grounds for it and could give you a clearance on those two bases without waiting for a conviction or an arrest.

Senator KYL. One thing that I need to say here for anybody who might be watching is that by virtue of our legislation a couple of years ago, we made this a crime against the individual as well as the financial institutions and others that might have been defrauded. Up until then, the individual didn't really have standing to force this kind of information and force this kind of action. So we have done that much.

We clearly have to try to refine the various bills and amendments that Senator Feinstein has filed and that we have been collaborating with here, and I think we will do that and would like to be able to consult with all of you. And I would suggest, Mr. Pratt, in particular, and Mr. Emmert with the association that you represent, and so on, you ought to hire people like Ms. Brown.

I mean, I don't know what she does for a living here, and you don't need to tell us here on the record, but the point is people with real experience like that, as well as, of course, people like Ms. Givens who have a wide survey approach to this based upon their extensive work in the area, to understand each of the kinds of problems that a victim goes through. I think bringing someone like Ms. Brown to some of your meetings and saying, "All right, listen to all of the different things that have gone on here"—surely, can't we in the marketplace devise ways of dealing with this and not have to rely upon the U.S. Congress to pass some kind of law.

For example, I have been reluctant to force the credit reporting agencies to provide a free report. You know, it is an expense. I did want to ask you, are you at the point where you think you can do that, if it is a reasonable kind of requirement, without being too much of a financial burden on the companies, Mr. Pratt?

Mr. PRATT. Senator, we really did deal with that question in the many, many years of dialog about the Fair Credit Reporting Act that took place in the decade of the 1990's. By 1996, we had new amendments which were, I think, extensive and material, and changed remarkably the privacy statute originally enacted in 1970.

In fact, we agreed at that time there were populations of consumers that needed to have a free report. One of those populations is a consumer who even just thinks they have been a victim of fraud. They don't have to walk in with a police report. So, in fact, we felt that that was a population that deserved access. I lost my wallet, I want a free report. So we agreed with that at the time. We also agreed for welfare recipients, for those who are unemployed seeking employment, any consumer who has ever been denied a benefit. So we provide an enormous volume of free reports per year.

We do ask, I guess, for some equity, just as if you want in and got a deed from the local courthouse, you might pay a fee. As long as we can keep that fee reasonable so it doesn't deny access merely by the cost, you give us a chance in those cases to just handle it in the same way. Currently, the law caps that fee at $8 plus the CPI.

Senator KYL. Well, we will continue to work with you on that, too.

Because we have this vote, I think we will have to bring the hearing to a close, but I can't thank each of you enough. I mean, you have all provided very important information for us, and I am serious about relying upon your expertise as we move forward with this legislation. Please understand we may be back in touch with you. Thank you all very, very much.

Senator FEINSTEIN. May I say ditto. Thank you.

Senator KYL. This hearing will now adjourn.

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

○