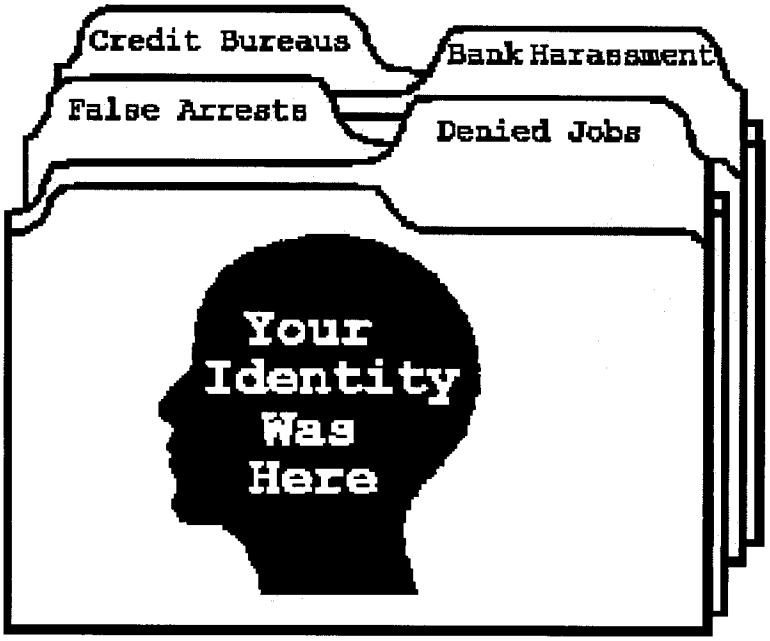

Nowhere to Turn:

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/PRC Report – May 2000

Janine Benner
Consumer Associate, CALPIRG

Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Beth Givens
Director, Privacy Rights Clearinghouse

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

or

The Privacy Rights Clearinghouse
1717 Kettner Blvd., Suite 105
theft at:
San Diego, CA 92101

Please contact PRC or VOICES and access fact sheets on id

www.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 difficult for victims to resolve their cases expeditiously. Although each identity theft case is different,

---

[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.

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.

- 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

---

[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.

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 identity theft a specific crime, Congress and the states have taken an important first step toward fighting

---

[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.

[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.

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.
- 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

---

[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.

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.

(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

---

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

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

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 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.

---

[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.

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 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.