Testimony of

Ms. Linda Foley

March 20, 2002

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

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

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

My written testimony will be divided into three parts:
× The crime: What is identity theft, its prevalence, why it is so popular among criminals
× Senate Bill 1742: Why ITRC supports this bill and believes it will assist victim, law enforcement and businesses
× Senate Bill 1399: Why ITRC supports this proactive identity theft protection act and believes it will prevent additional crime

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

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

× Criminal identity theft occurs when a criminal gives another person's personal identifying information in place of his or her own to law enforcement. For example, Susan is stopped by the police for running a red light. She says she does not have her license with her and gives her

sister's information in place of her own. This information is placed on the citation. When Susan fails to appear in court, a warrant is issued for her sister (the name on the ticket).

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

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

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

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

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

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

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

www.idtheftcenter.org"MACROBUTTONHtmlResAnchorwww.idtheftcenter.org under Speeches)

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

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

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

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

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

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

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

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

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

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

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

Testimony in Support of S 1742 (Cantwell):

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

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

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

When I became a victim of identity theft (Sept. 1997), I was fortunate in that the first credit card company I called shared the application information with me. I was able to immediately identify my imposter. It was my employer and she used her business address, which I recognized, as the mailing address for the account. The second credit card company provided me with a copy of the application which I turned over to the police. Armed with evidence, the detective could then get a search warrant that led to her conviction.

Unfortunately, even the companies that helped me have now adopted policies that make it next to impossible for victims to gain access to information on accounts opened in their names. I was told that there was legal issue involved. Credit card fraud investigators told me that once I said it

was not my account, they feared that they would be in violation of the Fair Credit Reporting Act by disclosing information to a "third party," someone who is not the account holder. They wanted to provide the information but their legal departments were unsure of what to do. The reality is that once this account has been established as fraudulent and that a crime has occurred, all rights to privacy for the person who opened the account should be suspended. Access to the information regarding the account should be freely given to the victim and law enforcement investigating the crime. Based on the reaction in California and Washington, both states with a law similar to this one, I believe you will see a positive reaction from business because this law will clarify their legal status in giving out information.

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

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

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

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

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

Sec. 6. Amendments to the Fair Credit Reporting Act
This section deals with two issues: the ability to block fraudulent accounts on an individual's credit report and extension of the statue of limitations from moment of occurrence to the moment of discovery.

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

This section will enable victims to more quickly expedite their recovery. This is vital especially since many victims hear about the crime when applying for credit. They may be purchasing a house or a car. Even a delay in a few weeks could affect the cost and availability of the purchase item. One of ITRC's regional coordinators (from San Francisco, CA) found out about her situation when trying to purchase a house. It took 1 ½ years to finally clear her credit report to the point that she could qualify for a mortgage again. Of course, housing costs had significantly increased and the mortgage broker asked for a higher interest rate.

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

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

Statute of Limitations: Identity theft is an unusual crime. Most victims of other types of crime are involved from the moment the crime began. If your car is stolen, your house is robbed or you are mugged and your purse taken, you know about the crime almost immediately. This is not true in identity theft. In three studies (FTC, Florida Grand Jury, Privacy Rights Clearinghouse -- all cited in footnotes below), the average victim didn't find out until 13-16 months after the crime

first began. By law the clock started when the crime began, giving identity theft victims only a few months to investigate, assess the damage and find out how the crime may have begun. Many victims take a year or more to get to this point.

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

Sec. 7. Commission Study of Coordination between Federal, State, And Local Authorities in Enforcing Identity Theft Laws.
One of the biggest problems facing both law enforcement and victims is that identity theft is a multi-jurisdictional crime. I live in San Diego but the imposter may be opening accounts in Los Angeles, New York and Dallas. The perpetrator may make purchases in various areas in one county. The Los Angeles area has 46 different law enforcement agencies in that one county alone. That does not include federal law enforcement, DMV, military, post office, immigration, IRS or Inspector General's Office of the Social Security Administration.

There are many questions that still need to be addressed.
× Who should investigate the crime? Most often it falls to local law enforcement to solve the crime. But which one? Is it the agency where the consumer lives? Is it in the jurisdiction where the biggest commercial victim is, assuming that they filed a crime report which many do not? If the crime is occurring in multiple areas, can one local agency afford to investigate a crime that may cross the nation? Rarely.
× Does this conflict contribute to the low arrest rate? Probably. It definitely contributes to victim frustration as they get passed from one agency to the next. In terms of prosecution, we find the same confusion and eagerness to pass the case to another location.
× Why are businesses reluctant to report this crime to law enforcement? Is there a way to encourage more active reporting?
× Is there a way to ease communications between jurisdictions?
× Where are these crimes going to be prosecuted? Is it in the jurisdiction where the consumer lives or where the largest economic loss to a commercial victim is located? Will the crimes be combined or is this person going to be tried repeatedly, once in each location?

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

Testimony in Support of S. 1399:

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

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

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

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

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

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

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

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

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

Fraud Alerts

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

A 1999 Lou Harris-IBM Consumer Privacy Survey reports that 94% of Americans think personal information is vulnerable to misuse. I believe that number has remained the same or even increased. We have all heard media reports that explain that our information is handled by far too many people on a daily basis. In an advertisement recommending traveler's checks, American Express stated that a wallet is lost or stolen every 10 minutes.

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

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

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

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

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

It is impossible to state loudly or clearly enough how important this section of S 1399 is to consumers and in turn to the nation's economy. If this bill is passed, the potential savings to

credit issuers, financial institutions and merchants could be in the billions of dollars.

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

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

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

Concluding Statements
Identity theft is a national crisis and the system allows, in fact encourages, criminals to take advantage of sloppy and thoughtless business practices. Media and community groups I speak with often asked why the increase in this crime. The answer is simple - this crime is almost irresistible. It has become ridiculously easy to commit this crime. Criminals know victims will get bounced from one jurisdiction to the other, often failing to find someone to investigate the crime. They also know that most businesses will not file charges against them. They count on the fact that in today's tight competitive market a company's greed may overcome caution and that fraud alerts will be ignored.

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

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

restocking time and costs, and in improved customer relations which draws people to their front doors.

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

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

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

Linda Foley
Executive Director
Identity Theft Resource Center

Addendum from ITRC'5
Many victims compare identity theft to rape, others to a cancer invading their lives. Many of the symptoms and reactions to identity theft victimization parallel those of violent crime. The following information is for understanding and, perhaps, to reassure victims that what they are experiencing is not abnormal. The reaction to identity theft can run the full spectrum from mild to severe. Clearly, the complexity of the crime itself will also define the severity of the impact, as will any other traumatic events that may occur around that same time frame.

Impact: The moment of discovery.
× Can last from 2 hours to several days.
× Reactions include shock, disbelief, denial, inappropriate laughter, feeling defiled or dirty, shame or embarrassment.

Recoil:
× Can last for several weeks or months, especially as other instances of theft are uncovered.
× Physical and psychological symptoms may include: heart palpitations, chest discomfort, breathing difficulties, shortness of breath, hyperventilation, dizziness, clumsiness, sweating, hot and cold flashes, elevated blood pressure, feeling jumpy or jittery, shaking, diarrhea, easily fatigued, muscle aches, dry mouth, lump in throat, pallor, heightened sensory awareness, headaches, skin rashes, nausea, sexual dysfunction, sleep disturbance.
× It is not uncommon for victims to frequently search through events trying to pinpoint what they did to contribute to this crime.
× Anger, rage, tearfulness, overwhelming sadness, loss of sense of humor, an inability to

concentrate, hyper-protectiveness, and a deep need withdraw are all part of the psychological reactions to identity theft.
× You may misplace anger on others, especially loved ones causing family discord. Those who tend to lean on unhealthy habits such as under or overeating, smoking, alcohol or drugs may be drawn to those additions for comfort.
× During Recoil, victims may experience a sensation of grief. They may grieve the loss of: financial security, sense of fairness, trust in the media, trust in people/humankind and society, trust in law enforcement and criminal justice systems, trust in employer (especially in workplace ID theft), trust in caregivers and loved ones, faith, family equilibrium, sense of invulnerability and sense of safety, hopes/dream and aspirations for the future.
× At one point or another, almost all victims will also grieve a loss of innocence, sense of control, sense of empowerment, sense of self and identity, and sense of self worth.

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

IDENTITY THEFT RESOURCE CENTER
2001 MILESTONES AND ACHIEVEMENTS

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

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

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

Our volunteer staff, who give so graciously of their time, has also increased. Our regional network has expanded and now includes coordinators in San Francisco, Wine Country/No. Calif., Dallas TX, New Hampshire, Maryland, Olympia WA, Atlanta GA, Seattle WA, Bridgeport CT,

Southcentral/East Michigan, Chicago, Akron OH, Milwaukee WI, Los Angeles and San Diego CA.

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

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

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

Finally, ITRC is proud to announce that our director, Linda Foley, has received several citations for her exemplary work and is the recipient of the Channel 10Leadership of San Diego "Individual Leader of the Year" Award for 2001, awarded by KGTV, the San Diego ABC affiliate.