U.S. Senate Banking and Finance Committee

Hearing on FCRA and Identity Theft

June 19, 2003

Written Testimony
of the Identity Theft Resource Center (ITRC):
Linda Foley, Executive Director
Jay Foley, Co-Executive Director

PO Box 26833, San Diego CA 92196
www.idtheftcenter.org
email: itrc@idtheftcenter.org
858-693-7935

"IDENTITY THEFT – VICTIMIZATION AND CRIME PREVENTION"

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.

The Identity Theft Resource Center (ITRC) is passionate about combating identity theft, empowering consumers and victims, assisting law enforcement, reducing business loss due to this crime and helping victims. We are honored by your invitation and will continue to make our opinions available upon request to your representatives over the next few months as you grapple with this complex crime and the FCRA sunsetting.

ABOUT ITRC:
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, Linda Foley founded this San Diego-based nonprofit program after becoming a victim of identity theft. In her case, the perpetrator was her employer. ITRC's work with thousands of victims (by email and by phone), credit granters, representatives from the CRAs, law enforcement officers, governmental agencies and business has taught us much.

Jay Foley, ITRC co-executive director and co-writer of this testimony has spent hundreds of hours speaking with victims while assisting in their recovery, listening as they discuss their revictimization by "a system that doesn't care, understand or listen." As one of the few groups that deal with a victim throughout recovery process, we have a unique perspective on the crime. Our information is not just moment of discovery statistics. Our information comes at the cost of minutes, hours, days, weeks, months and years of a victim's life.

Through our testimony we will introduce you to some of the victims who have helped us to understand the changes that must be made in the areas of prevention and recovery. We hope their stories illuminate the issues as clearly for you as they have for us. To protect their privacy, they will be referred to as an initial only.

The ITRC has worked for a number of years to make changes in laws, policies, business practices and trends to combat this crime. As a result we have composed a list of recommendations that we feel will make a difference both in crime prevention (keeping the information from the hands of criminals and the issuance of credit) and in victim recovery.

OUR TESTIMONY: ITRC has been asked to address the following points:

- The crime: Who are these criminals and what is identity theft
- The Victim: What are some of the crimes we hear about
- Crime expansion: crime trends, numbers, stats, anecdotes and articles
- Victim Recovery: What steps must victims take
- Recommendations about areas that need change
- Provide your perspective as to the value of state involvement.
- Our opinion of the FCRA battle

IDENTITY THEFT:

The Crime: There are four recognized main categories 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, 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. In relation to your committee and

focus- this type of crime might occur in relationship to checking account fraud. Many states do prosecute on bad checks or opening accounts fraudulently.

Case history: One of our recent cases involved a woman who lives in Pittsburgh. Her imposter had several warrants in Kentucky for opening a fraudulent checking account and writing bad checks on it. The victim was 8 months pregnant at the time of the crime, restricted by her doctor to bed (in Pittsburgh), and clearly incapable of committing this crime. The bank finally cleared her but forgot to tell the DA to cancel the warrant. She has incurred legal expenses as well as other expenses in clearing her name and rectifying the inaccurate records from various databases.

- Identity cloning is the third category. This imposter uses the victim's information to establish a new life. He or she actually lives and works as you. This crime may also involve financial and criminal identity theft as well. Types of people who may try this fraud include undocumented immigrants, 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."

- Commercial identity theft is similar to financial identity theft and cloning except the victim in this type of case is a commercial entity. Criminals open checking and credit accounts as that company, order product and may even try to conduct business as that entity. Unfortunately, there is a yet to be explored topic and good answers for these victims are few.

The Victims: Identity theft is a dual crime and no one is immune, from birth to beyond death. Who are these victims? It could be you, unknown at this very moment. Let us introduce you to some of our clients/victims who have turned to us for assistance. Some of these cases are cut/paste of emails we have received from victims. We present them to you so that you can see what we work with on a daily basis.

Case 1: Child ID theft
Victim owes about $65,000, $4,700 in child arrears and has 3 DUI warrants in his name. One problem. Jose is only 6 years old now and those arrears are to himself. The perpetrator is his father, now divorced from Jose's mother, an illegal immigrant and subject to deportation when found.

Case 2: Identity theft of the deceased
Perhaps one of the most poignant stories we have heard (NJ Star Ledger reported it) is the theft of a man's identity who died in the World Trade Center attack on Sept. 11th. His widow was notified about 10 months after the event to discuss her husband's recent auto accident. She went through hours of turmoil only to discover that an illegal immigrant had created a false driver's license and was living and working as her deceased husband. Unfortunately this is only one of more than several dozen cases that we have worked on involving the deceased. In some cases the imposter has purchased the information, in others the perp is a family member or even a caregiver. Some may ask what is the harm in using the SSN of the deceased. Not only can this affect the estate but the survivors steal dealing with the grief of losing a loved one. In one other

case, a mother has had to fight collectors trying to collect money from accounts opened in her daughter's name, a daughter who died several years ago. Each new call opens up the wound again.

Case 3: Information breach, workplace id theft
T's identity was stolen by her doctor's receptionist. She found out when applying for her first home loan, her dream home. Months later, after clearing her records, spending her own time to research how her thief got her information and used it, and seeing another family move into her home, she was able to convince authorities to prosecute her offender. The result- the thief is now living in a halfway house, driving the car she bought with T's identity and working for another doctor as a staff member. T was finally able to buy a house almost 2 years later, at a higher purchase cost, with a higher interest rate due to the multiple accounts that had been opened in her name after the placement of a fraud alert.

Case 4: Victim recovery issue
Victim owns her own business. For the past 3 years, she has been in a fight with her bank. They repeatedly open new accounts and grant access to her existing accounts, even generating dual credit cards sending them to the imposters as well as herself. At one point she went to the local branch of her bank to once again put to rights the transfer of her account information. With multiple pieces of identification in her possession she was devastated by the bank officers who would not acknowledge her right to discuss the accounts in question or accept her identifying documents including passport, driver's license, utility bills, business license and SS card. To date she still has problems with her bank and her accounts. She is currently talking to an attorney and plans to sue the multiple companies who continue to torment her and refuse to correct their errors. She believes that lawsuits are her only option left.

Case 5: Financial id theft turns into criminal case
Two nights ago, I was arrested as part of a four year on going theft of my identity. The arrest was over bad checks written in Lincoln, NE near where I reside.

The issue, other than the arrest and all that goes with it, is the fact that J P M was able to open fraudulent accounts because the Nebraska DMV issued her a license with her picture and my information. I don't know what documentation she provided them, but we clearly do not have the same physical features. This should have sent up a red flag to the DMV. As a result, J P M illegally used my identity to spend almost $40, 000, with new credit cards and with fraudulent checks.

I am doing the best I can to be compensated for the money spent on bail, loss of work time, personal stress, which all occurred while I was finishing my undergraduate degree and throughout my master's degree. Needless to say, this has interfered with my performance in school because of the time it takes to free myself as a citizen and as a consumer. The arrest was the last straw, and I've been told that the statute of limitations to sue the woman who stole my identity has expired. I am looking for help.

Case 6: SSN used as DL #

Victim had car broken just prior to a move from HI to DE. A file with all ID and information was stolen in HI including her DL which used her SSN as the identity number. Since then a fraudulent cell phone account was setup with Voicestream generating a bill for $10,000.00. The victim has made some payments during the course of the account dispute due to the bullying action of collectors threatening to attach to possessions. Because of that Voicestream refuses to acknowledge the account is fraudulent.

Case 7: Security breach
Victim was referred to ITRC by the FBI Victim/Witness Coordinator. The victim is a 72 yr. Retired Air Force Major. His dentist told him his ID was stolen. The dentist had befriended a man who saw the victim's dental records. This man then copied and used all of victim's info. The dentist found out when he saw files out of place. This befriended man/handyman was the only person who had access. The imposter purchased a condo, a BMW, and used the victims HMO for medical services. The victims HMO paid for this. Upon arrest it was discovered that the imposter had a prior record of fraud. The imposter is now in jail on non-related charges.

Case 8: Cloning
Victim lives in San Diego on disability. The imposter is living and working in IL. Fraud is impacting her disability. IRS and SSA have been contacted. Victim is fearful of losing housing and being unable to cover living expenses due to the lengthy time of recovering her good name and clearing the records.

Case 9: Workplace ID theft
The victim recently found out of the identity theft. In 1999 a co-worker stole her credit card. The victim went through all the necessary procedures with her credit card company to remove the charges including filing a police report. In January 2002, the victim applied for a loan with a small finance company. The victim was told her social security number had already been used to apply for a loan with this company. The victim retrieved the application and found it was used back in 1999 by the same lady who stole her credit card. The victim had never been contacted by this company. The company's reply: we denied the application. Unfortunately in doing so, they did not indicate that it was denial due to fraud but due to not enough income.

I did go to the company with this, I even spoke with the Vice President in South Carolina and she was useless. I still have not received a copy of my Credit report so I am not sure if she has not done any real damage or not. I am sure she used my social security number and I am not sure how else I can file a report if the police are not helpful. Thank you again.

Case 10: Extreme case
Victim's id stolen by co-worker 10 years ago. She knows who the perp is and he has been questioned but released by police (refusal to take action due to "extenuating family circumstances"). In the meantime the victim has been unable to stop the perp from opening credit and checking accounts, fraudulently applying for welfare, etc. She has had to change her SSN, DL# and name, essentially recreating herself in order to separate and protect her from the actions of the perp.

Case 11: Reoccurrence

My wife was a victim of identity theft in 1999. After many letters, a police report and an affidavit of forgery we thought everything was settling. We were reassured that the loan and credit that was taken out in our name was removed from our reports and that our credit restored. We asked several times for correspondence that this was taken care of but no one returned a letter. As time passed and we received no bills, we forgot about it. That is until we received an Equifax on 6-2-02 showing it still on the report. I tried to contact the office that I communicated with before but no one would return my call.
The date reported was after we had notified them of the dispute. Are they in violation of the (FCRA)? Please advise or direct.

Case 12: Family ID theft
Victim's relative used victim's identity to clear out victim's bank accounts. This relative has victim's SSN and stole checks. Victim has filed police report and in contact with the managers at her bank. LEA not investing a great deal of time on case, usually claiming that this is a family dispute. Family identity theft is one of the most difficult crimes we work on, in part due to lack of police action and in part due to the emotional impact of this crime. How does one turn one's own mother in to the police? Unfortunately we receive about 3-5 of these types of cases each week.

Case 13: Domestic abuse, harassment
The victim was divorced in 1987, she now lives in Florida. The ex-husband is operating here in San Diego. Due to the actions of her ex, the victim is having IRS, SSA problems and is dealing with 3 accounts under her name. Unfortunately ID theft is the perfect tool to harass another person and to perpetuate domestic abuse after a divorce or separation.

Case 14: Stolen wallet
I live in TX. On June 2, 2002 my wallet was stolen in New York City. On June 6, 2002 a woman began using my identity from the wallet including drivers license, social security number from a medical insurance card, place of employment and stolen cards to establish instant credit at 9 different stores in 3 different states. I have placed a credit alert fraud with the three credit reporting agencies but there has already been theft totaling in excess of $16,000 dollars. I am now having difficulty getting anyone to follow through with a report and also changing my drivers license number. Because the theft occurred out of my home state I am having to follow up on the phone and not getting much response or help.

Case 15: Military spouse
I have had the frustrating and humiliating experience of somebody taking my maiden name and social security number in order to open numerous fraudulent utility accounts leaving my credit reports a mess. I am also a military wife who is required to show my social security number on my id card, which is used for everything.

Case 16: Enable credit granting behavior
I was a victim of credit fraud/ID theft beginning in November of 2001, and continuing until approximately April of 2002. All of the many fraudulent credit applications using my name and identifying information were done in the Los Angeles area. Somehow, my personal identifying information (SS #, name, birth date, etc) were obtained and used to apply for instant store credit

at Radio Shack, Gateway Computers, and approximately a dozen other merchants. Additionally my personal credit card was "taken over" by these criminals. By calling Visa and posing as me, they changed my billing address, and claimed that they had lost the credit card. They then received my new Visa card in the mail at the fraudulent address. They applied for many credit cards under my name and were even successful at getting a few, then charging the cards up to the maximum very quickly

Case 17: Mail theft by an acquaintance
I just found out on June 14, 2002 that I am the victim of identity theft by my housekeeper/ babysitter. Since she had access to my mail it was easy. She opened the first account in April 2001. She has charged over 10,000.00 that I am aware of and I have jewelry etc. missing from my home.

This is so recent that I don't even know what I'm up against yet- what I do know is that this has hurt my eleven year old daughter very badly. My daughter sang in the housekeeper's wedding last May, I wonder now if the wedding was all charged to me!

I would be happy to talk to anyone about this. I live in a small town of 12,000 people right now I know 4 people personally that this has happened to including the president of one of the banks here in town. Something must be done!! She is having trouble getting creditors off her back.

Case 18: Domestic abuse, insurance fraud.
My ex-husband and his employer used my Social Security number to file medical claims on my health insurance. My ex has not been covered on my insurance since 1999, and I have changed employers and insurance carriers since that time. However, claims for February 2002 through May 2002 have been filed on my current insurance. He has obtained the information without my knowledge. I found out about the claims after receiving Explanation of Benefit forms from my insurance provider. The claims have been denied, so the insurance provider states that they are doing their job. The insurer will not file a report with the police.

Case 19: IRS complications
I have had my ID stolen. Someone has gotten hold of my social security number and from that cause me to have false credit bureau claims and warming from the IRS that I had underreported my income. Creditors have harassed me and required me to go to extraordinary lengths to prove that I could not have incurred the debt in question. The IRS has required extensive documentation as well. Right now the activity has settled down, but anytime the next shoe could fall.

Even though there is a certain person I suspect of engaging in this identity theft, law enforcement authorities turn a deaf ear. I really don't blame them, it's not a high priority crime to them. To me it is a major theft and close akin to rape.

This whole situation has been aided by the use of computers and the overuse of the social security number. I understand that the original law establishing the issuance of social security numbers stated that that number should only be used for social security, but indeed that has not been the case.

Case 20: Victim frustration- complex case
I became a victim of identity theft in March 2001. I found out when the person who had my social security number tried to open a credit card with a bank that I already had a card with. The woman was not able to give my correct birthday. They contacted me but they gave me a hard time saying that it was my daughter. They suggested that I contact the credit agencies about a fraud alert. That is when I found out that the person had many credit cards and a cell phone and they even bought a computer from Dell. Since I found out early I was able to stop almost everything before it was way out of hand. I filed a report with the Dallas police department and talk to a detective all the time. Only to find out they would do nothing. They had the address the cards and computer was sent to but they would not go there. They even had another address where the person used a credit card in my name to buy a pizza. I found a lot of information on the Internet and started writing letters and sending them certified return receipt. I also made a file that I have with everything I did and all the copies. It took many months to clear everything up and I still have the fraud alert on my report for seven years. This is a crime that is to easy for someone to do and they get away with it because our Laws are too easy and the officers are not trained on this type of crime. I feel I am luckier then most because I found out early and was able to clear up the damage within a year.

While you know my story, that only tells part of the picture. What I discovered disturbed me greatly:

1. Fraud alerts only help a little. Most places do not even honor them. So I'm not sure they help very much.
2. After I put the fraud alert on, they still opened a few more credit cards. All of the accounts they opened were done on the Internet.
3. I found that the credit card companies did not care much, they just closed the accounts. But before they will close the accounts you have to prove to them it was not you who opened the account.
4. They also made you wait on the phone a long time and you are transferred to many people before you found one that could help you. Most of the people I talked with acted like they were not educated enough on the subject.
5. They treat you like it was your fault and most of them need more training on this issue.
6. The police are no help at all.
7. The credit agencies take forever to remove the fraud accounts from your file.
8. The victim spends hundreds of hours writing letters and phone calls trying to remove the damage the thief caused while they are free to go to the next victim.
9. The Laws should help the victims, but you are alone when it comes to identify theft.

VICTIM IMPACT: THE GOOD, THE BAD AND THE UGLY
While victims are not usually held liable for the bills accumulated by the imposters, many do suffer significant financial and emotional harm from this crime. According to studies done by the Privacy Rights Clearinghouse (PRC)/CALPIRG in 2000 and Federal Trade Commission (FTC), the average victim spends about 175 hours and $1,100 in out-of-pocket expenses. These expenses include notarizing, postage, telephone, travel, photocopying, costs involved in getting police reports and fingerprints, and resource materials.

ITRC is in the process of completing an updated study. We believe that the numbers will be significantly higher due to the complexity of the crimes committed.

In many situations this does not cover time lost from work, loss in productivity while working or loss of personal or vacation time. Some victims never truly regain their financial health and find credit issuers and even employers are reluctant to deal with someone with "baggage."

To have someone use your good name, a reputation in which you have invested much time, energy and money, is a deeply felt violation – financially, emotionally and on that has the power to affect your decisions, relationships and financial/criminal history from that point forward in your life.

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.

Victims face many challenges in cleaning up the mess left by the thief.
In the best case scenario:

1. Law enforcement takes a report and provides a copy to the victim.
2. The victim discovers the case early enough to prevent it from being sold to a collection agency.
3. The initial contact with the creditor is not misleading nor ignored.
4. The creditor freezes the account based on telephone contact and closes it completely when presented with a police report identifying the account as fraudulent.
5. The victim is provided with information that when provided to law enforcement makes the case and supports the arrest and prosecution of the thief.
6. The victim is given a letter of clearance and the entries and inquiries are removed from the credit report.
7. The creditor works with the victim and the police to complete the case.

In the Bad version the victim.

1. Victim fights with police to get a report taken.
2. Has to deal with the creditor and one or more collection agency.
3. The creditor's staff is unhelpful. They provide inaccurate information
4. Creditors refuse to make account and transaction information available to the victim claiming privacy concerns of the account holder/criminal. The victim is burdened with proving innocence without the benefit of knowing where the charges were made, how the account was opened, dates of purchases, etc.
5. Too often victims are told to have the police request this information but when requests are made by law enforcement they are denied access as well without a stack of paperwork at best.
6. They make statements to the victim that the account is cleared up but do not take the actions necessary to close or clear the account.
7. Accounts are resold after the victim has provided proof of the fraudulent nature of the account.

8. Victims are told that they are still responsible for the account when a family member did it fraudulently.
9. Accounts are not removed from the credit report by the creditor when proven to be fraudulent.
10. Victim is mislead to believe that the CRA will respond to their requests to have information removed or corrected on the credit report. The CRA passes the fact that a dispute over the validity of an account exists to the creditor but does not present any of the evidence submitted by the victim.

In the Ugly Version the victim.

1. Faces all of the problems from the bad version plus.
2. The victim is sued by the creditor without the victim's knowledge and a judgment rendered against the account holder – the victim. (The imposter is served)
3. The victim is arrested for the crimes of the thief.
4. Property is seized by court order leaving the victim to attempt to have the court reverse the order.
5. Homeless people and minors face many unique problems getting copies of their credit reports.
6. Despite all efforts, the victim is unable to stop the thief from using his/her SSN, name and other information. In these cases the ultimate solution is to change one's identifying information – name, SSN, DL#, etc. The problem: This solution creates more problems then it solves. You are now a person without a credit, work, college or life history. You are nothing more than a blank slate.

IDENTITY THEFT'S NEGATIVE ECONOMIC RIPPLE EFFECT:

In terms of economic impact, a recent Florida Grand Jury 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 www.idtheftcenter.org under Speeches)

The Privacy Rights Clearinghouse 2000 report found the average economic loss per victim to be $18,000, ranging from $250 to in excess of $200,000 (footnote 1). While the FTC study so far shows a different number, their numbers are based primarily on moment of discovery. In identity theft, it sometimes takes months before the total damage can be assessed

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.

ITRC 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 trafficking, etc) funded with the money made by imposters or information brokers who sell the documents used by some imposters and those wishing to Identity Clone.

IDENTITY THEFT TRENDS:
There are clear indications that identity theft is not only a crime that is committed by your garden-variety type of thief but is also used by organized crime groups. ITRC's new study will help to show the complexity of the crimes that are committed, the impact financially and emotionally and to help us track this crime even more effectively.

Dumpster diving: Digging through trash is not glamorous but can be very profitable especially when that dumpster sits behind a mortgage broker, dentist's office, rental office, insurance company or even a market or governmental agency. The papers there are a wealth of information including account number, SSN, names and unlisted phone numbers and even mother's maiden name. The value of these dumpsters is that the thief doesn't leave with one document but with dozens at a time.

Scams: Creative writing teachers would be proud with the types of both telephone and Internet scripts that have been written to separate you from your information. Some, including that apparently come from governmental agencies or from credit providers even seem to fool experts. ITRC receives at least a dozen requests each week from people asking us to verify a "legitimate" looking scam. One DMV Director even forwarded an urban legend to us that contained only partially correct information. He received it "from a reliable source."

Mail theft: In a recent conversation with a Postal Inspector in California, we were told that a good portion of identity theft cases involves the post office. Not only is it a way to move information, receive "stolen" good and cards but also the mail is a rich source of sensitive information. Preapproved credit offers are but one of the problem areas. Convenience checks (that come with credit statements- ready to use by anyone), any bank/credit/financial statement with an entire account number imprinted on the bill, health benefit statement, payroll stubs and statements, literally hundreds of sheets that make their way to your home could be intercepted and used for identity theft. And the problem is that the post office is not the only location to steal this mail. It could be intercepted in a variety of locations – print shop, mail room (either outgoing or incoming if returned to sender), postal office and then finally your own either locked or unlocked mailbox. Your own roommate, friend, caregiver or family member could look at the mail, steal it or just use the information.

Checking Account Takeover: Checking account takeover is a heinous crime in that it can be accomplished in many ways. Your account can be accessed electronically, checks that you issue can be reused, and checks can be computer generated using your information on the top but a different bank routing and account number on the bottom. To date, the financial community and consumer groups have yet to find a good solution to this issue.

Identity theft and other illegal activities: The reality is that identity theft is a way to make a lot of money quickly. This automatically draws the attention of narcotic dealers, manufacturers and junkies, gamblers, alcoholics, those who compulsively spend money and those who sell

information (like selling drugs) to make large quantities of money to live the lifestyle they wish to enjoy.

Gang behavior, information trafficking and identity theft: Several law enforcement groups have now shared that their large cities have given rise to organized identity theft rings. These groups control the information selling, teach others how to commit identity theft and find the "targets" that will become their mules or information gatherers. They may have a division that helps to sell "stolen" merchandise or traffic merchandise on the black market.

These groups are also setting themselves up as businesses, allowing them access to information from groups like the CRAs and datahouses like ChoicePoint. They are finding ways to target groups of people based on a variety of fields- address, economic status, last name, ethnicity- so that they can customize the information for sell.

Level of sophistication: Just when we think we've heard the very worst-case scenario, another person contacts our office with an even more difficult case. Gangs are working smart and even teach each other about our law enforcement and business weak links. There is a reason that some companies are regularly hit and others are rarely hit. Instead of opening 5 new credit cards, they open 30. In fact, skimmers may be found with more than 10,000 "new" credit cards ready to sell or use. These criminals have become bold and brazen. Why- why not, especially when so few are caught and the crime is so profitable?

Three other areas of concern:

1. **Non-English language victims:** Identity theft is an equal opportunity crime. It can strike anyone with a SSN. According to the latest census, in California 1/3 of our population in non-English speaking. However, even the simpliest task of ordering your credit report is difficult. In both of the CRAs that use automated systems, neither provide an option for even Spanish. Should the victim have another person call in for their report on their behalf (trusting their SSN to yet another stranger/friend), the information sheets which include consumer rights, how to understand the report or what to do come in one language only- English. These same victims face similar situations in contacting credit issuers and collection agencies. ITRC has worked with some of these victims- in part through a translator and partly in the victim's native tongue. The frustration level is high and their dissatisfaction with the system even higher. Some have given up and just paid the bills, fearful of the consequences and not understanding their rights.

2. **Deployed Active Duty Military**: It is difficult enough to clear up a problem of identity theft if you have the time and ability to do so. But you cannot deal with a case in a timely manner while deployed – either into a battle zone or in an overseas duty station. We know- at this time we are working with about 20 military personnel.

   ITRC has proposed a plan for a Military Victim Support Program to several legislators, asking the DoD to consider creating a trained body of JAG aides/victim liaison officers who will work with these members, almost as a one-stop shop. This program will save money, help to highlight security issues and assist deployed military members as they

serve our country, sometimes at great physical risk. ITRC will make that plan available to any committee member who will help us to move this program forward.

3. **Identity theft and dominance/domestic abuse:** Identity theft is the perfect tool to dominate, abuse and harass another individual. More and more we are seeing cases that like this.

RECOMMENDATIONS FOR LAWS:

It is our goal in the next section to illuminate problems reported by victims and law enforcement and to provide recommendations for consideration. ITRC has always been known as a problem solver and not a finger-pointer.

The Finding section of each recommendation is based on ITRC's research, studies widely available and input by victims, law enforcement and businesses. For text recommendations, please contact the ITRC national office. A * denotes areas of highest priority.

A final comment: Many of these ideas are common sense, and ITRC hopes that the involved entities voluntarily absorb these concepts as standard practices. Legislative solutions should be a last resort. In fact, voluntary acceptance can be used to an advantage as illustrated in the following anecdote:

Three weeks ago we bought our cell phones from Cingular. Both of us have fraud alerts on our reports. We explained to the salesperson at Best Buys that he might encounter a delay. He never had heard of fraud alerts through he specializes in one of the items that thieves are more likely to buy. Indeed, Cingular did notice the alert, my husband went home to answer the telephone call to approve the transaction, and with no more than a 15-minute delay we had our phones. Cingular voluntarily did the right thing and has a loyal customer due to that.

Police Reports
Finding: One of the biggest victim complaints is that law enforcement refuses to take a crime report in identity theft cases. "You are not the victim, the business is." A secondary problem is jurisdiction, since many of these crimes cross lines both geographically and by agency. The victim's mail may have been stolen in Houston, but credit purchases are being made in Virginia and in Oklahoma. Who handles this case? The Post Office fraud investigation team, the Houston police or the sheriff in Virginia?

The other problem facing victims is that without a police report, credit issuers simply do not believe you. Bank fraud investigators have stated at legislative hearings and at conferences that a main determining factor in separating victims from those avoiding paying a bill is a crime report. The belief is that a "deadbeat" will not file a false police report and take the chance that they will be arrested for that action.

Recommendation: Legislation declaring that a person who has learned or reasonably suspects that another has unlawfully used his or her personal identifying information may initiate a law

enforcement investigation in his or her own local jurisdiction and shall receive a copy of said report. For recommended text, see California P.C. 530.6 **(www.leginfo.ca.gov)**

2. Victim Access to Records on Accounts Opened in His/Her Name
Finding: The burden of proving one's innocence lies on the shoulders of the victim. In a sense, you must prove a negative- that you did not open the account or make the purchases. This requires knowing the application and transaction information. If purchases were made in person in New York and you were working in Houston that day, you have a chance at being taken seriously. In some cases, victims recognize the handwriting on an application or know who made the purchase because they personally know the perpetrator.

Recommendation: Legislation that allows the victim of identity theft and the investigating law enforcement agency to receive application and transaction information on fraudulent accounts opened in his or her name. Language recommendations: Calif. PC 530.8 or S 1742 (federal bill-author Sen. Cantwell).

3.Declaration of Innocence – Criminal Identity Theft
Finding: Cases of criminal identity theft are especially difficult because even after proving you were not the person who committed the crime (or got the tickets), your name remains the "alias" on record. Every time a police officer stops you, when a potential employer does a criminal background check or you go out of the country on vacation, you wonder if you will be accused of the imposter's crime yet again.

Recommendation: Legislation and/or policies to allow a person to petition the court for a "factual declaration of innocence." We recommend that the victim not only be issued an official record of that declaration, but also for the state to establish a database that would keep these records. If the person loses the paper (most carry copies for life), this database would contain the order and a copy of the true person's fingerprint(s) for comparison in the case of another instance of mistaken identity.

4. Statute of Limitations for Lawsuits Involving Identity Theft
Finding: 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), the average victim didn't find out until 12-16 months after the crime first began. By federal law, the clock starts 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**.**

Recommendation: Legislation to allow victims of identity theft and financial fraud at least a 2-year window to initiate a lawsuit against involved parties, starting from time of discovery and not time of when the crime(s) occurred.

5. Confirmation of Change of Address – Account Takeover

Finding: Account takeover has been a problem for many years. It is fairly easy to find out the credit card number of an individual: via mail interception, shoulder surfing, skimming, register receipts and 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.

Recommendation: Legislation mandating that a company must notify the cardholder when a change of address is submitted. This change of address notification should be mailed by postal mail (not postcards) to the current address on the account, as well as the new address. The notice should inform the account holder of the request and give a toll-free number to call if the account holder had not submitted the change.

6. Mandatory Observation of Fraud Alerts

Finding: 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. While California is also experimenting with a credit freeze, ITRC believes that the mandatory observation of fraud/security alerts is the ultimate credit monitoring service.

The only measure of control over the establishment of new credit lines is through a fraud or security 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 or please contact me at the following email address: ___" – is advisory in nature only. Language for this bill has been already written by Senator Feinstein.

Recommendation: Legislation that would require all credit reporting agencies to indicate to credit issuers that there is a fraud/security alert and the entire text of that alert, whether a credit score, summary or full report is requested. AND that all credit issuers must check for and observe security alert request as written on credit reports. This legislation should include penalties and civil remedies for failure to comply.

7. Truncation of Credit Card Account Numbers on Credit Card Receipts

Finding: Many merchants print your entire credit card number on merchandise receipts. Unfortunately, this is an excellent way for thieves to gather information and enjoy a shopping spree at your expense. The scenario: It's a busy time, perhaps a white sale or during the holidays. As Mary wanders from store to store, she doesn't notice the gray-haired woman walking behind her. She also doesn't notice the woman slipping her hand into Mary's purchase bag and pulling out the receipt for the sweater she bought a few minutes ago. By the time Mary gets home a few hours later, this woman (minus the gray haired wig) has hit two nearby shopping centers and charged about $3,000 in merchandise to Mary's account.

Recommendation: Legislation that states that a person or entity that accepts credit cards for the transaction of business may not print more than the last 5 digits of the credit card account number or the expiration date upon any receipt provided to consumers. A 2-year phase out deadline can be included to allow stores to adjust programs as they replace or alter machines and software programs.

8**. Free Annual Credit Reports upon Request**
Finding: Credit Reporting Agencies (CRAs) collect credit information provided by credit issuers, merchants and others and then resell it to their customers – credit issuers, merchants and employers. That information is not verified for accuracy, and may even reflect addresses used by imposters or misread by clerks. The irony is that if this information is not accurate, not only does the consumer suffer, but the businesses that purchase this information and use it to determine whether to extend credit lines can also be harmed. Information distributed by the CRAs seems to take on a life of its own. These reports are replicated and distributed by resellers (i.e., real estate industry). Errors in reports spread like a malignant growth throughout the system, affecting a person's ability to get credit, buy a house or car, obtain a job and secure rental housing.

The only way to confirm the database information is to allow the consumer to check it over on a regular basis. Currently, the credit reporting agencies charge a fee to look at one's credit report, arguing that they shouldn't be forced to give anything away for free. Yet, the only person who can authenticate information is the consumer. Why should they be forced to pay to verify information they didn't provide to the CRA in the first place?

Recommendation: We recommend following the lead of several other states (Colorado, Georgia, Massachusetts, Maryland, New Jersey and Vermont) in allowing each consumer one free copy of all three credit reports per year, upon request and expand upon it to also follow California's lead in allowing multiple credit reports for victims of identity theft within the first TWO years after the discovery of the crime (perhaps one every three months). This bill is smart business, good for consumers and good for a state's economy.

9. Victim's Right Act
Finding: Victims of financial fraud must be given full rights under the law. These include the right to reasonable and timely notice of any public proceeding involving the crime and of any release or escape of the accused; the rights not to be excluded from such public proceeding and reasonably to be heard at public release, plea, sentencing, reprieve, and pardon proceedings; and the right to adjudicative decisions that duly consider the victim's safety, interest in avoiding unreasonable delay, and just and timely claims to restitution from the offender.

Recommendation: Legislation that would require the victim to be notified of all steps of the criminal process including the trial date and the release of the perpetrator from custody. Provisions should be made to allow for victim input prior to sentencing and for restitution when appropriate. Victims of white-collar crime should be afforded the same rights as those of violent crimes.

10. Information Trafficking

Finding: As identity theft has grown, suspects have become actively engaged in the collection of personal profiles for purposes of identity theft. These suspects often steal mail and trash in search of new identities to use. They compile lists of victims' names, birth dates, Social Security numbers, maiden names, addresses and other pieces of information that can be used to open fraudulent accounts or take over existing legitimate accounts. These profiles have become commodities that can be sold or traded for drugs or cash. Often the person compiling the profile is not directly involved in the actual use of the identifiers, thereby avoiding prosecution as an "identity thief." In some cases, suspects have retained victim profiles for years, knowing they can be used again and again**.**

Recommendation: Legislation making the action of information trafficking illegal and punishable as a felony or felony/misdemeanor (wobbler) depending on judicial discretion. Possible language includes: Every person who, with the intent to defraud, acquires, transfers, or retains possession of the means of identification of another person without the authorization of that person, is guilty of a public offense, and upon conviction therefore, shall be punished (terms equal to type of crime). The term "means of identification" means any name together with one or more other pieces of information which can be used to identify a specific individual, including a social security number, date of birth, state or federal issued driver's license or identification number, taxpayer identification number, or unique biometric data, such as fingerprint, voice print, retina or iris image.

11. Confidentiality and Protection of the Social Security Number (SSN)
Finding: The SSN is the golden key to financial identity theft. However, it is used by so many entities that it is nearly impossible for consumers to adequately protect it. New standards and laws need to be adopted that dictate collection, use, display, security and confidentiality of the SSN. It should not be used as an identifier by schools, insurance companies, employers, utility companies or businesses. SSNs should not be publicly displayed (i.e., printed on timecards or badges) or shared with other companies or organizations except where required by law. ITRC would hope that business groups would voluntarily adopt many of the recommendations in this section and that legislation be a last resort.

Finding: Companies often ask for information that is not necessary for the transaction of business. They claim that they may need it at a future time or for statistical purposes. There should be some restriction of the type of information asked on applications. For example, a self-storage company and a health club were recently asked why they requested the person's SSN. The response was that it was a convenient ID number to use as a member number.

Recommendation: Legislation prohibiting the use of the SSN as an identifier, except for specified governmental purposes. Entities that should not be using the SSN as an identifier include: schools, insurance companies, employers, utility companies or businesses. Both civil and business code penalties may need to be imposed on those who do not comply with these standards. Again, a phase-out program can be implemented to minimize costs to those entities that now use the SSN as the customer ID number.
Recommendation: Legislation restricting circumstances in which a company/governmental agency may ask for certain identifying information including SSN, birth date and driver's license

number. This recommendation includes the requirement that all states convert to non SSN for Dl# use rather than allowing the consumer an option.

Finding: Information is often exchanged in an unsafe manner. Those individuals collecting information must be trained on how to collect data in a manner that does not compromise the security of consumers or employees. That means that information should not be exchanged verbally in a public place, where the conversation may be overhead. How many times have you seen a pharmacist ask for a SSN in order to process a prescription? Who is overhearing that conversation? How many times have you seen a retail clerk phone in a credit application while standing in a workstation surrounded by shoppers? Even once is too often.

Finding: Personal information on databases should be encrypted and accessed only on a "need-to-know" basis. These people should have access audited and their computers must be password controlled. Ideally, these people should all have criminal and financial background checks performed on a regular basis.

Recommendation: Only personal information relevant to the purpose to be used should be requested. It must be limited to "need-to-know" personnel, and access of information strictly audited and controlled. Consumers and employees must be notified in advance as to the purposes of the data collection, to whom it will be distributed and the subsequent use after the fulfillment of the original purpose. Legislation should include anti-coercion language so that consumers will not be penalized if they wish to "opt-out" of additional services/lists or denied services if they do not wish to provide sensitive information that is not essential to business operations.

Recommendation: No person or entity shall sell, give away, or in any way allow distribution or use of information collected or provided to governmental agencies other than the original purpose for which the information was requested**.**

Recommendation: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. If this occurs, legislation should be in place to allow for civil litigation and possible punitive actions by the courts.

12. Effective Disposal of Records No Longer Needed

Finding: The privacy and financial security of individuals is increasingly at risk due to the widespread collection of personal information by both the private and public sectors. Credit transactions and applications, magazine subscriptions, telephone numbers, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, employee records, pharmacy records, mortgage or banking applications, and Internet sites are all sources of personal information and form the source material for identity thieves. Consumers must trust that companies are adequately destroying information no longer stored. Unfortunately, investigative reporters around the country are finding compromising information in Dumpsters behind buildings on a regular basis.

Recommendation: Legislation requiring businesses to take all reasonable steps to destroy, or arrange for the destruction of a customer's or employee's records within its custody or control

containing personal information which is no longer to be retained by the business by shredding, erasing or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means. This should include records on paper and those stored electronically.

13. Security Breaches (Workplace ID Theft)
Finding: The concealment and notification delay to concerned parties of information breaches involving the theft or possible theft of identifying information must stop. The incidents at the Stephen P. Teale Data Center and the University of Texas/Austin in which the personal financial information of hundreds of thousands fall into the hands of computer hackers is a dramatic demonstration of an all too common event. This bill MUST include both computer breaches and paper breaches of information or it will not be complete.

Recommendation: Legislation needs to be considered that would require a timely notification to all parties involved in a breach containing their personal identifying information.
Recommendation: An individual should have the right to verify the accuracy of information collected about him or her without charge and in a form that is readily intelligible to him or her. They should be able to challenge data recorded in error, and if the challenge is successful to have the data erased, rectified, completed or amended.

14. Protecting Information from Mail Theft
Finding: Mail theft is a major source of information for identity thieves. When consumers don't know that an item is being sent to them, they are unable to report its loss. We also have to make sure that any document being sent via mail does not include a full SSN or account number.

Recommendation: Require prior consumer consent via an opt-in program for pre-approved credit card offers and convenience/balance forward checks sent through the mail. This program would also require that consumers be notified of expected mailings so they can monitor in the event it is not received. Another way to tackle this problem is to prohibit any changes in the original form sent to the consumer or allow any forms that are incomplete (In other words- a thief may not know my birth date and leave it blank). In terms of other documents, the SSN must be eliminated from mailings, including paycheck stubs. The employee ID number (other than SSN) could be used in its place.

15. Consumer Notification of Excessive Applications or Negative Info on Credit Reports
Finding: Credit granters are aware that there are recognized warning signals that indicate possible financial identity theft: multiple applications within a short period of time, multiple applications with the same SSN but different addresses, etc. The problem has been that no one credit issuer sees all the applications. The only entities that have access to this information are the CRAs.

Recommendation: Legislation that requires the CRA to notify a consumer at all the addresses on record for the past 6 months of a possible fraud situation should more than four (4) credit applications be submitted within a 30 day period of time.

Finding: Consumers don't often find out about negative information on a credit report until the worst possible time – when applying for credit, a job or tenancy. This may be due to the consumer's own actions, those of an imposter or clerical errors.

Recommendation: Legislation that requires the CRAs to notify a consumer of any negative information submitted to the CRA at the time of submission. This legislation may stipulate that no more than four (4) notifications are required in any one calendar year unless a fraud or security alert is currently on that credit report.

ITRC'S POSITION ABOUT IDENTITY THEFT AND FCRA SUNSETTING:

1. Identity theft crosses state borders and many of the crimes we hear about are both cross-geographic and multi-jurisdictional in nature. This creates a loophole in which identity thieves thrive. It is one that we can, by working as a unit, finally close. National standards supported and aided by state involvement is essential.

2. A cohesive, uniform set of laws that would keep sensitive information out of criminal's hands, strengthen credit issuing standards and assist victims is badly needed. The question that has not yet been answered is whether a single set of federal laws can do the job.

3. While strong national laws will reduce the need or desire for fine-tuning via state laws there may always be a need for the states to address individual issues – in response to consumer/business needs of that state and to enhance the ability for local law enforcement and prosecutors to pursue actions on behalf of those who live in that state.

4. We do not agree with the concerns on businesses and other groups that they will need to conform to 50 different standards. That is speculative at best and prior to 1996 was not an issue. A dual regulatory system has worked well in other areas and can work to the betterment of all in regards to FCRA as well if needed.

5. We are well aware that as a victim resource center that interacts with business that to take a diehard approach that would drastically impair or negatively impact business ability to function will be just as devastating to the victims we assist. We seek a cooperative meeting point between the business, le, leg, consumer and victims so that we can defeat the one true enemy of all of us- the thieves.

6. To discuss FCRA preemptions is premature until we see the set of new, signed laws that are adopted as national laws. As in the last five years there has been much talk but little action in the last six months, since the preemption discussion was opened and identity theft was thrust into the spotlight. Once those laws are signed, then we can discuss preemption. Until that time, this is like filing for retirement before you've been offered your first job.

IN CONCLUSION:

Crime, like most things in our society grows, evolves and constantly changes. In 1970, the writers of the FCRA could not have predicted that credit transactions would be conducted via

Internet. All business was conducted in person, in communities where people were known and applications could be verified.

When FDR expanded the use of the SSN as an identifier, he could not have anticipated the Pandora's box that he would open. It was impossible to predict the impact of the information age and how computer technology would allow a crime like identity theft to flourish.

The FCRA preemption discussion has created more activity and talk of action in the last six months than in the last five years combined. In 2000, the FTC held a hearing on ID theft in which we participated. They have continued to monitor this crime through their database and through victim panels. The information has not changed, just the number of victims which has increased.

ITRC's staff members have attended hearings and provided information for years now to federal legislators and governmental agencies about changes that need to be made – to no avail. Few, if any, bills have been passed. The most recent was passed because of its link to Homeland Security (higher penalties- for all those criminals who are not caught in the first place).

While the federal government shows an interest in identity theft, it has been the states that have led the way in restricting information access and victim recovery. These legislative bodies have shown a responsiveness that is unmatched to date at the federal level. (see addendum)

If you are serious about identity theft and feel you can address it sufficiently on a national basis, this is your opportunity to prove it. But keep in mind- we (consumer, victims, law enforcement, advocates and the business community who cares about combating this crime) have high standards for the laws that you pass. We will not accept weak laws that either do little to help the situation or weaken existing laws that have a proven history.

ITRC's sole purpose is to combat this crime and to help victims. Our fear is that the public will be promised new laws, strong laws that allow for expansion and redirection as this crime grows and evolves but will never see them. Our fear is that the promise will be made but once groups interested in renewing the FCRA pre-emptions wins, these news laws will cease to be discussed let alone passed.

At this time, ITRC wants to see some action. We want to see what the new laws say, who they protect, what they address and how they will affect both businesses and consumers, neither of which can be disregarded or harmed. Until those laws are passed and signed by the President, discussing pre-empting states from passing laws is premature.

Thank you for your time and consideration.

Linda Foley
Jay Foley

Addendum: California vs Federal Laws that have been passed in the last three years in response to consumer/victim/law enforcement feedback.

Confidentiality of Social Security Numbers - California Civil Code section 1798.85-1798.86 and 1786.6 This law restricts businesses from publicly posting or displaying Social Security numbers. The law takes effect gradually from 7/1/02 through 7/1/05.

- **Consolidation of ID theft cases - Penal Code section 786. The jurisdiction for a criminal action for ID theft offenses may be the county where the theft occurred or the county where the information was illegally used. If similar ID theft offenses occur in multiple jurisdictions, any one of those jurisdictions is a proper jurisdiction for all of the offenses.**
- **Consumer Credit Reporting Agencies Act Civil Code section 1785.1-1785.36 This law, the state counterpart of the Fair Credit Reporting Act, regulates consumer credit reporting agencies. It requires them, among other things, 1) to provide free copies of credit reports to consumers who have been denied credit or who are identity theft victims, 2) to block information that appears on a report as the result of identity theft, 3) to place security alerts (effective 7/1/02) or freezes (effective 1/1/03) on the files of consumers who request them, and 4) to provide, for a reasonable fee, credit score information to consumers who request it.**
- **Credit Card Number Truncation - California Civil Code section 1747.9 No more than the last five digits of a credit card number may be printed on electronic receipts. Effective 1/1/01 for machines put in use on or after that date. Effective 1/1/04 for all machines that electronically print credit card receipts.**
- **Credit Card "Skimmers" - Penal Code section 502.6. The knowing and willful possession or use, with the intent to defraud, of a device designed to scan or re-encode information from or to the magnetic strip of a payment card (a "skimmer") is punishable as a misdemeanor. The devices owned by the defendant and possessed or used in violation may be destroyed and various other computer equipment used to store illegally obtained data may be seized.**
- **Destruction of Customer Records - California Civil Code sections 1798.80 - 1798.84 This requires businesses to shred, erase or otherwise modify the personal information in records under their control.**
- **Employment of offenders - Penal Code sections 4017.1 and 5071 and Welfare and Institutions Code section 219.5. Specified prison and county jail inmates may not have access to personal information. The same prohibitions apply to specific offenders performing community service in lieu of a fine or custody.**
- **Identity Theft: Access to Financial Records on Fraudulent Accounts - California Civil Code section 1748.95, California Financial Code sections 4002 and 22470. Similar to Penal Code section 530.8, these laws require certain types of financial institutions to release (to a victim with a police report or to the victim's law enforcement representative) information and evidence related to identity theft.**
- **Identity Theft - California Penal Code sections 530.5-530.8**

These code sections define the specific crime of identity theft, require the law enforcement agency in the victim's area to take a police report, allow a victim to get an expedited judicial ruling of factual innocence, require the Department of Justice to establish a database of identity theft victims accessible by law enforcement and victims, and require financial institutions to release information and evidence related to identity theft to a victim with a police report or to the victim's law enforcement representative.

- **ID theft Conspiracy/DMV - Penal Code sections 182 and 529.7. Courts can impose fines of up to $25,000 on individuals convicted of felony conspiracy to commit ID theft. This law also makes it a misdemeanor for any unauthorized person to obtain (or assist another person in obtaining) a driver's license, identification card, vehicle registration certificate, or other official document**

issued by the Department of Motor Vehicles, with the knowledge that the person obtaining the document is not entitled to it.

- **Identity Theft Victim's Rights Against Claimants - Civil Code section 1798.92-1798.97 This law protects identity theft victims who are being pursued for collection of debts which have been created by identity thieves. The law gives identity theft victims the right to bring an action against a claimant who is seeking payment on a debt NOT owed by the identity theft victim. The identity theft victim may seek an injunction against the claimant, plus actual damages, costs, a civil penalty, and other relief.**
- **Information Practices Act of 1977- California Civil Code sections 1798 and following This law applies to state government. It expands upon the constitutional guarantee of privacy by providing limits on the collection, management and dissemination of personal information by state agencies.**
- **Insurance Information and Privacy Protection Act, Insurance Code section 791 et seq. This law limits most insurance companies from disclosing personal information about a consumer that is collected or received in connection with an insurance transaction, for example, (1) when a consumer provides written authorization for a disclosure, or (2) when a disclosure is necessary for conducting business. The law permits the disclosure of non-sensitive information for marketing purposes unless the consumer opts-out.**
- **Investigative Consumer Reporting Agencies Act, California Civil Code sections 1786-1786.60 This law regulates the activities of agencies that collect information on consumers for employers, insurance companies and landlords.**
- **Legal and Civil Rights of Persons Involuntarily Detained - Welfare & Institutions Code section 5328 This law provides for the confidentiality of the records of people who are voluntarily or involuntarily detained for psychiatric evaluation or treatment.**
- **Mandated Blood Testing and Confidentiality to Protect Public Health - California Health & Safety Code sections 120975-121020 This law protects the privacy of individuals who are the subject of blood testing for antibodies to the probable causative agent of acquired immune deficiency syndrome (AIDS).**
- **Notice of Security Breach - Civil Code Sections 1798.29 and 1798.82**

This law requires a business or a State agency that maintains unencrypted computerized data that includes personal information, as defined, to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The type of information that triggers the notice requirement is name plus one or more of the following: Social Security number, driver's license or state ID card number, or financial account numbers. The law's intention is to give affected individuals the opportunity to take proactive steps to protect themselves from identity theft. These provisions take effect July 1, 2003.

- **Office of Privacy Protection - California Business and Professions Code section 350-352 A state law enacted in 2000 created the Office of Privacy Protection, with the mission of protecting and promoting the privacy rights of California consumers.**

http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=00001-01000&file=350-352

- **Payment by Check or Credit Card - Civil Code sections 1725 and 1747.8. Any person accepting a check in payment for most goods or services at retail is prohibited from recording a purchaser's credit card number or requiring that a credit card be shown as a condition of accepting the check (Section 1725). Any person accepting a credit card in payment for most goods or services is prohibited from writing the cardholder's personal information on forms associated with the transaction (Section 1747.8).**
- **Patient Access to Medical Records - California Health & Safety Code section 123110 et seq. With minor limitations, this law gives patients the right to see and copy information maintained**

by health care providers relating to the patients' health conditions. The law also gives patients the right to submit amendments to their records, if the patients believe that the records are inaccurate or incomplete.>

Personal Information Collected on Internet - California Government Code section 11015.5
This law applies to state government agencies. When collecting personal information electronically, agencies must provide certain notices. Before sharing an individual's information with third parties, agencies must obtain the individual's written consent.

Public Records Act - California Government Codes sections 6250-6268 This law applies to state and local government. It gives members of the public a right to obtain certain described kinds of documents that are not protected from disclosure by the Constitution and other laws. It also requires that state and local agencies be "mindful" of the laws that confer privacy rights. This law also provides some specific privacy protections.

Spam laws - California Business and Professions Code, Section 17538.4 and 17538.45 - Penal Code section 502 These code section establish the guidelines relating to unsolicited e-mail and faxes.

State Agency Privacy Policies, Government Code section 11019.9. This law requires state agencies to enact and to maintain a privacy policy and to designate an employee to be responsible for the policy. The policy must describe the agency's practices for handling personal information, as further required in the Information Practices Act.

Substitute credit cards - Civil Code section 1747.05. A credit card issuer that issues a substitute credit card must provide an activation process where consumers are required to contact the card issuer to activate the credit card before it can be used.

Supermarket Club Card Act - Civil Code Title 1.4B. This law prohibits supermarket club card issuers from requesting drivers license number or Social Security number and from selling or sharing personal customer information; limited exemption for membership card stores.

Telemarketing: State do-not-call list - Business and Professions Code sections 17590-17595. Effective April 1, 2003, Californians can put their residential and cellular telephone numbers on a State do-not-call list. For program details, visit the Attorney General's web site at http://caag.state.ca.us/donotcall/index.htm.

Unsolicited cell phone/pager text ads - Business and Professions Code section 17538.41. This law prohibits the sending of unsolicited text advertisements to cell phones or pagers.

Warranty cards - Civil Code section 1793.1. Product warranty cards must clearly state that the consumer is not required to return the card for the warranty to take effect.

Federal Laws

Children's Online Privacy Protection Act (COPPA) - 15 U.S. Code 6501 et seq. The Act's goal is to place parents in control over what information is collected from their children online. With limited exceptions, the related FTC Rule requires operators of commercial websites and online services to provide notice and get parent's consent before collecting personal information from children under 13.

Driver's Privacy Protection Act of 1994 - 18 U.S. Code 2721 et seq. This law puts limits on disclosures of personal information in records maintained by departments of motor vehicles.

Fair Credit Reporting Act (FCRA) - 15 USC 1681-1681u
This federal law is designed to promote accuracy, fairness, and privacy of information in the files of every "consumer reporting agency," the credit bureaus that gather and sell information about consumers to creditors, employers, landlords and other businesses.
www.ftc.gov/bcp/conline/edcams/fcra/index.html

Family Educational Rights and Privacy Act of 1974 (FERPA) - 20 U.S. Code 1232g This law puts limits on disclosure of educational records maintained by agencies and institutions that receive federal funding.

Federal Identity Theft Assumption and Deterrence Act of 1998 - 18 USC 1028 The Act makes it a federal crime to use another's identity to commit an activity that violates Federal law or that is a felony under State or local law. Violations are investigated by federal agencies including the Secret Service, the FBI and the Postal Inspection Service and prosecuted by the U.S. Department of Justice. www4.law.cornell.edu/uscode/18/1028.html

Federal Privacy Act of 1974 - 5 U.S. Code 552a This law applies to the records of federal government executive and regulatory agencies. It requires such agencies to apply basic fair information practices to records containing the personal information of most individuals.

Financial Services Modernization Act, Gramm-Leach-Bliley (GLB), Privacy Rule - 15 USC 6801-6827 The 1999 federal law permits the consolidation of financial services companies and requires financial institutions to issue privacy notices to their customers, giving them the opportunity to opt-out of some sharing of personally identifiable financial information with outside companies.
www.ftc.gov/privacy/glbact/index.html

Health Information Portability and Accountability Act of 1996 (HIPAA), Standards for Privacy of Individually Identifiable Health Information, Final Rule - 45 CFR Parts 160 and 164
HIPAA includes provisions designed to save money for health care businesses by encouraging electronic transactions and also regulations to protect the security and confidentiality of patient information. The privacy rule took effect on April 14, 2001, with most covered entities (health plans, health care clearinghouse and health care providers who conduct certain financial and administrative transactions electronically) having until April 2003 to comply.
http://aspe.hhs.gov/admnsimp/bannerps.htm#privacy

Telephone Consumer Protection Act (TCPA) - 47 U.S. Code 227 This law puts restrictions on telemarketing calls and on the use of autodialers, prerecorded messages, and fax machines to send unsolicited advertisements.

Video Privacy Protection Act of 1998 - 18 U.S.C. 2710
The Act strictly limits the conditions under which a video rental or sales outlet may reveal information about the outlet's patrons. The Act also requires such an outlet to give patrons the opportunity to opt out of any sale of mailing lists. The Act allows consumers to sue for money damages and attorney fees if they are harmed by a violation of the Act.