P.O. Box 26833
San Diego, CA 92196
858.693.7935
www.idtheftcenter.org

Testimony
Of
Eric Handy

On behalf of:

The Identity Theft Resource Center®

Information Policy, Census and National Archives Subcommittee

Oversight and Government Reform Committee

Identity Theft: A Victim's Bill of Rights

June 17, 2009

2154 Rayburn HOB

2:00 p.m.

In addition to my oral testimony, the ITRC theft victimization study, *Identity Theft: The Aftermath 2008 and be found online at:* ***http://www.idtheftcenter.org***

http://www.idtheftcenter.org/artman2/publish/a_overview/Corporate_Overview

Chairman Clay, Ranking Member McHenry and Members of the Information Policy, Census, and National Archives Subcommittee:

Thank you for the opportunity to provide both written and oral testimony for your committee today and for your interest in the topic of the "rights of victims of identity theft" and "the rights of consumers not to become victims." My name is Eric Handy and I am here on behalf of the Identity Theft Resource Center (ITRC) as a personal representative of Linda Goldman-Foley, founder of the ITRC. I am here today to represent the "voices of the victim."

I am a specialist in victimization, compliance law and identity theft issues. I have over 10 years of IT Security experience working with industry experience in the following business sectors: telecommunications, high tech, health care, transportation, consumer industrial & manufacturing, and the federal government. I also hold certifications as a CISSP - Certified Information Security Specialist, CIPP/G - Certified Information Privacy Professional with specialization in Federal Government and am a PMP - Project Management Professional. I am also a PhD candidate on the subject of identity theft.

Introduction

What are the challenges facing today's identity theft victims? What rights need to be added or modified to assist these victims? What needs to be provided to consumers to reduce their risk of victimization?

In the conclusion of *Identity Theft: The Aftermath 2008*. ITRC always allows victims to have the final word. Today I would like to start by sharing a few of the victim's comments:

- *Somebody filed a tax return and received my refund from the IRS. The IRS referred me to a taxpayer advocate who has NOT been an advocate! I have gotten the "run around" and I'm still going in circles!*
- *I am dealing with criminal identity. People with the same first and last name as mine, but with different middle names, have committed crimes in the State of Florida. Because our names are similar, there is erroneous criminal information attached to my name. According to the state of Florida, which keeps the records, I committed no crime. I still am frightened and fear I am going to be arrested for their crimes.*
- *The person is still using my identity to work in the U.S. and I cannot stop her. I have been denied credit and new services because of this, even though I have a very good credit score. I don't think the police are capable of finding her or solving this case. I have a lot of anxiety and fears as a result of my identity theft.*
- *I am still concerned because as far as I know my personal info is still out there. There needs to be better laws and methods to help victims have more of a sense of closure.*
- *Identity theft is a very isolating crime. You feel like no one understands or could. Some people say it is a victimless crime. I am a victim! I want people to know that!*

ITRC is honored by your invitation to be the "voice of identity theft victims" and will continue to make its opinions available upon request to your representatives over the next few months as you grapple with this complex crime.

The Classifications and Categories of Identity Theft Crime

The ITRC classifies identity theft into five main categories:

- Financial Identity Theft is when the imposter uses another individual's personal identifying information, primarily the Social Security number (SSN), to establish new credit lines. The imposter may apply for telephone or utility service, credit cards, loans, or lease cars and apartments leaving the victim with a ruined credit record and score.
  - Subcategories of this crime include, but are not limited to, credit and checking account fraud.

    Case history: *Somehow, my personal identifying information (SSN, name, birth date, etc.) were obtained and used to apply for instant store credit at various large stores, 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.*

- Criminal Identity Theft occurs when a criminal gives another person's personal identifying information, in place of his or her own, to law enforcement. These cases range from misdemeanor infractions up to and including felony level crimes. The victim problem is that there is a record created by an arrest or the issuance of an arrest warrant. As a result, these filter up through a system not designed to be altered, nor designed to allow for the removal of records. The victim faces rejection in seeking employment, the possibility of termination, possible incarceration, and the possible need to hire an attorney to prove his/her innocence.
  - Checking Account Fraud might result in Criminal Identity Theft. The victim's information is used by the imposter for passing bad checks. In some cases the victim's information may be the only real thing on the bad check. Many states prosecute on bad checks or opening accounts fraudulently. The victim is squarely in the sights of the DA.

    Case history: *A recent case 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. She was restricted by her doctor to bed (in Pittsburgh) and clearly incapable of committing this crime. The bank finally cleared her but forgot to notify the prosecuting attorney of the change of facts and status so the warrant could be withdrawn. She has incurred legal expenses as well as other expenses in clearing her name and rectifying the inaccurate records from various databases.*

- Identity Cloning or Identity Assumption is the third category. This imposter uses the victim's information to establish a new life. He or she actually lives and works in the victim's identity. This crime usually involves financial issues, governmental issues, and possibly criminal identity theft.

- The financial issues may include information on a victim's credit report that is not his. However, the bills are paid monthly. Many victims dealing with this find that companies prefer not to close the account because the account is current. These companies do not recognize that thieves may pay bills in order to maintain stolen identities for long periods of time.
- Governmental issues are represented by undocumented immigrants, wanted felons, those avoiding tracking (i.e. getting out of paying child support or escaping from an abusive situation), and those who wish to leave behind a poor work history, criminal record, and/or a bad financial reports. In essence, they are "starting over", but using your name and identity.
- This type of crime can necessitate having the victim deal with tax issues, benefit fraud, criminal records, and erroneous secondary data aggregator records.

Case history 1: *Two nights ago, I was arrested as part of a four-year ongoing 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.

Case history 2: *Victim lives in San Diego and is receiving disability benefits. The imposter is living and working in IL. The fraud is impacting her disability benefits. The 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.*

- Medical Identity Theft is a growing problem in multiple ways for the nation. It is best defined through the problems faced by the different victim groups affected by this crime:
  - For the person whose information was used, "the victim": The financial impact to the individual as negative debts and delinquencies are reported and recorded on the victim's credit report. When collection agencies get involved in debt collection, judgments/liens could be issued against the victim.
  - To the medical facility and health providers: The expenditure of dollars in treatment, in terms of time, equipment and medical resources, for which recovery will be nearly impossible. There are hundreds of hours expended in collection attempts, as well as the additional time spent by both the victim and the company to clear up the financial issues created.

- To the government and business systems: There is the issue of benefit fraud and the potential of improper denial of benefits due to abuse by imposters. Being denied care due to the exhaustion of benefits is a double edged sword. The individual's health could be placed in greater jeopardy by a delay in treatment while the fraud is detected, identified and then corrected. The provider could be open to lawsuits for failure to provide timely and adequate care to the true patient.
- The creation of data records containing information that do not correctly reflect the identity assigned. Due to HIPPA, it is nearly impossible to remove medical records "created" by the imposter. Privacy issues also prohibit a victim from seeing those records if they declare they are a victim of identity theft.
- The denial of coverage due to the consideration of "pre-existing conditions" listed as part of the imposter's health condition.
- The potential issues of mixed data which could cause an incorrect diagnoses or treatment.

  Case history: *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.*

- Commercial Identity Theft is similar to Financial Identity Theft except the victim is a commercial entity.
  - Commercial entities do not have credit reports. They have no means to find out if their EIN is being used by an imposter to open new lines of credit. As of this date, there is no credit reporting system for companies operating under an EIN. (Employer Identification Number)
  - Commercial entities don't have access to fraud alerts since they don't have credit reports.
  - Criminals open checking and credit accounts using the identifying information for a company, order products and may even try to conduct business as that entity. They can also create fake checks using the information from the commercial entity for payment. Due to the nature of many large businesses, this may not be caught until an audit is done and someone realizes there are extra checks, duplicate checks or checks out of order.
  - Unfortunately, this is a yet-to-be-explored topic and good resolution steps for these victims are few. Due to time limitations, ITRC will not be addressing the issues of this crime today.

Findings and Recommendations

In the next section, ITRC will introduce various issues that we believe if they were properly addressed would have a positive effect on identity theft victimization in the United States. This is not a complete set of guidelines, but focuses on some of the major issues facing victims today.

1. Child Identity Theft:

Finding: Children should have the right to have their identities protected in such a fashion that upon reaching their majority they are able to start their adult lives with a clean slate and not as a victim of identity theft.

With the above goal in mind, the first area of consideration should be with the current policy of issuing Social Security numbers (SSNs) to minors/infants. This practice creates an unrestricted 18-year window of opportunity for identity thieves. The issuance of SSNs to minors originated upon the request of the IRS to combat tax fraud. The flaw with the system is that there is no difference between a Social Security number issued to an infant today or one that is issued to an adult immigrant. Social Security numbers are tied to a **date of issue**, and not a date of birth. This allows imposters to acquire and use Social Security numbers of children for committing identity theft.

What most people do not realize is that the creation of a credit file is based on the information provided in the **first application for credit**. Until then, a credit file does not exist. That first application becomes the "de facto" baseline of information, taken at face value, as the true information about that "person." If a child's Social Security number is taken, and the date of birth is modified to indicate 18 years of age or older, a person can apply for credit thus creating a credit file. The thief can use a different name and address, and no one would know that this was a fraudulent application. The true recipient of the Social Security number may not even be aware of the situation until they apply for their first line of credit, after their 18th birthday.

Businesses and credit issuers complain that they have no way of knowing if a SSN belongs to a minor. That is factually true. In *The Aftermath* the following comments were provided by a compliance manager of a data privacy and identity theft program of a major utility company:

> *The void of a credible nationally recognized data source to validate minors' credentials leaves businesses blind to the facts. This void means businesses may not be able to deny credit or services under many very complicated regulations without reasonable information that the identity is fraudulent. Without a data source confirming the identity credentials belong to a minor, many businesses simply create an account and require a security deposit.*

Minors may not enter into a legally binding contract. In these cases, the companies always suffer the loss of services or goods. Clearly, they would like a solution to this issue. In today's economic environment businesses don't want to absorb the additional fraud loss.

Recommendation: The creation of a data file called the "17-10 Database." The "17-10 Database" would be a list that contains the name, month, year of birth, and Social Security number of every individual from the age of 1 day to 17 years and 10 months. This file should be sorted by Social Security numbers and provided twice a month, without charge, to the appropriate credit reporting agencies, all Departments of Motor Vehicles, and selected companies doing the prescreening of credit applications under the guidelines of the Federal Trade Commission. This solution has been discussed with the Social Security Administration

and is possible. Both children and businesses benefit from the 17-10 Database. According to the FTC Complaint Call Center Report, 5% of all complaints are about minors. ITRC feels that there are far more child related identity theft cases than are being reported. More investigation is necessary to quantify this debilitating crime.

The benefits of using this system are as follows:

- This would effectively freeze the Social Security numbers of all children until they are 17 years and 10 months of age. It would allow the CRAs to warn creditors that the Social Security number on the credit application belongs to a minor, ideally stopping the acceptance of the application and subsequent fraud loss.
- This would prevent the spread of any additional information that could be used for identity theft while alerting a business of a possible fraud. All that need be provided to the credit issuer is the comment: "the Social Security number belongs to a minor."
- This would provide age support information to all the DMV's for the issuance of drivers license.
- This would eliminate the practice of utilizing a child's Social Security number to obtain a fraudulent driver's license after real driver's license has been suspended or revoked.

2. Identity Theft and the Deceased

Finding: Death should not diminish a person's right to be protected against identity theft.

Despite a person's death, a SSN may continue to be active and could conceivably be used for the extension of credit. Currently, the Master Death Registry, which the Social Security Administration contributes to, does not include the names of all deceased. Information is added to this list in a variety of methods, some of which are consumer-generated.

Unfortunately, thieves scour the obituaries and even cemeteries for people who died as children or young adults. They then apply for birth certificates and Social Security replacement cards to assume that identity. These documents have been known to be reproduced many times and sold to multiple people. After all, who is watching a credit report of a deceased person or child?

Several years ago ITRC worked with a woman whose 6-year old deceased daughter's identity was continually being used by an adult woman for credit, work, and even to enroll in Reserve Training. Because all the records use her daughter's SSN information, collection agencies still call this bereaved mother 15 years later about accounts her daughter never could have opened.

Recommendation: All governmental agencies that issue death certificates shall notify the Social Security Administration of a death with a specified paper or electronic form within 10 business days of the issuance of a death certificate. Information would not be included in the Death Registry if submitted by any other entity. If the identity of the decedent is not known at time of death, the issuing agency would forward a copy of the certificate issued when positive identity is established.

- The SSA notifies all credit reporting agencies/repositories within 15 business days of any SSN that should be flagged as deceased.
- Any credit reporting agency that receives such notification shall:
    - Enter a "deceased alert statement" in the deceased's credit report declaring: *This person died on (date). New credit lines should not be extended to this name and/or social security number from that date forward.*
- In the event of credit applications made after date of death, the credit reporting agencies/repositories shall send a SAR (suspicious activity report, form to be determined) to the following groups of people: law enforcement agency in jurisdiction where the person last lived, law enforcement agency in the jurisdiction where the application originated, closest living relative/executor of estate.
- Credit reporting agencies/repositories shall include the "deceased alert" statement in reports provided to all credit issuers requesting information on said person, no matter whether a score, summary or full report is requested by the credit issuer.
- All credit issuers must observe the deceased alert.

3. Protecting the Social Security Numbers of Medicare Participants and Military Personnel

Finding: Seniors and military personnel should be protected from needless exposure to identity theft caused by the requirement of carrying a card with a SSN.

Currently the Social Security Administration and U.S. Government uses Social Security numbers as identifying numbers on cards carried by Medicare participants and military personnel. We must make progress in finding alternative solutions and stop exposing the SSN of these two special interest groups. This topic has been introduced by federal legislators for more than 7 years now.

On July 6, 2003, Parade Magazine's (in the Sunday paper) centerpiece discussed identity theft. Even then, people were concerned about lost and stolen wallet issues and were angry at governmental agencies (SSA, military) or health providers because of the placement of the SSN on a card they must carry on a daily basis.

> Case History: *T's identity was stolen by her doctor's receptionist from the information on her health card. 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.*

Recommendation: If the SSN must be in the federal database for benefit or identification purposes, then we must find a way to assign a random User ID number that will be printed on the card that is carried. This User ID number is then used as an identifier on multiple forms that are filled out by the individual. In the case of the military, this use might involve dozens of papers annually. The excessive exposure of SSN is a weak link in our national risk management system. If the federal government expects the business community to protect SSNs, it must lead by example.

4. Overuse of the SSN as an identifier by other entities

Finding: Every individual should have the right to have their Social Security number used responsibly. Over exposure of the SSN could lead to a higher risk of identity theft.

The following categories demonstrate the problem of the overuse of the SSN:

- Employer use of SSN as individual employee ID number, including public display of such, e.g., timecards, timesheets, cash register use number, badges, etc.
- The use of the SSN as an identifier by a business group, printed on a card carried by the person on a regular basis.
- The inclusion of a SSN on printed material that is mailed. This could lead to interception by another person at any point in the mail delivery system, starting with the printing company.
- Requests by business for Social Security numbers in situations that do not involve employment, taxes or the extension of credit.

Recommendations: Private entities may not use the SSN other than for tax purposes or purposes designated by either state or federal governmental agencies. They may not publicly display, use, sell or share the information. ITRC will be happy to assist in providing language for such a bill, modeled on several state laws that address this issue currently. This ruling would eliminate the use of a SSN as a student identification number and health insurance policy number.

5. Collection of Identity Theft Statistics

Finding: Victims of Identity Theft should have the right to accurate assessment of the prevalence of the crime.

There are constant requests for accurate statistics regarding the number of identity theft cases nationwide. Such information is not available due to the fact that identity theft is not a tracked crime. Crime data for certain crimes is collected annually by the Federal Bureau of investigation for study and analysis. Identity theft is not one of these crimes. Even if identity theft were added to the list of tracked crimes this would not generate accurate statistics. There are still states within the United States that do not have laws that require local law enforcement to take a report.

Recommendations:

- Identity Theft should be added to the current list of tracked crimes for statistical analysis.
- Mandate that to qualify for any federal financial support, law enforcement must report on identity theft crimes in their jurisdiction. Use of the Federal Trade Commission's *Identity Theft Statement* should make the required reporting time a non-issue.
- Creation of a program where all identity theft reports are gathered for review and analysis. Data and intelligence gained from this program to be provided to LEA for case use.

6. Criminal Identity Theft:

Finding: Criminal Identity Theft victims should have standard mitigation processes for their cases.

The victim in Criminal Identity Theft faces a secondary wounding due to the placement of his/her personal information on a criminal record. Warrants and records under the victim's name can be cleared however the re-issue contains the victims information as an AKA (Also Known As) descriptor. The victim faces the obstacle of proving that they are not the person being sought by law enforcement, as well as to employers or prospective employers. To remove the AKA information would be detrimental to the law enforcement community, while providing the imposter with a cleaned identity to use to mislead law enforcement again.

Recommendation: In any case where an NCIC file has been created using the information of a real person as an alias, the biometric and personal data of the real person should be captured and marked to clearly identify the true victim. Additionally, there should be a standardized method of clearing one's name in the event of criminal identity theft at the local, state, and federal level.

Recommendation: The creation of a national NCIC Identity Assumption Victim's Registry. Through this system victims would receive a card they could use anywhere in the U.S. to show that a pre-existing criminal case of identity theft has been recorded. Currently, only a few states have a "passport" program and it can not be used out of state. Details of the creation of said registry and the development of the program would need to be assigned to a taskforce including the FBI, other government agencies, and victim advocates.

Recommendation: It should be required that any data aggregator or background screener must have a working policy to correct any incorrect information in their possession when they are notified by consumers that their information is not correct. Secondary data aggregators must maintain updated records reflecting monthly changes in the primary records they purchase.

7. Security Breach Notification

Finding: A national security breach notification law would add to best practices against fraud and identity theft. A breach notification should be a right provided to all individuals.

While people receiving breach notification letters are not identity theft victims, their information could be at higher risk of being used fraudulently. The American public is highly concerned about the lack of security of personal identifying information in the workplace and marketplace. ITRC has been studying data breaches since 2005, observing trends in the causal factors that lead to a breach of personal identifying information. It is clear from the passage of laws in 44 states and the District of Columbia that breach notification is a topic consumers want addressed. However, this patchwork of laws has made it difficult and costly for businesses to comply with said laws.

Recommendation: The creation of a federal breach notification law that would equally apply to all governmental agencies and companies. ITRC recommends the following items for inclusion of this bill:

- Notification of a breach should be done in a timely manner, without any hint of "a need to prove risk of or substantial harm." Due to the sophistication of fraudsters and their intimate knowledge of laws and law enforcement procedures, it is impossible to declare that information that has been out of the control for even a short period of time could not have been read or copied. It could be warehoused until people stop looking for any indication of a breach.
- What information fields were breached should be included in the notification letter so that consumers can take appropriate steps. This would also avoid having the consumer take unnecessary steps that could harm the consumer as well as be costly for industry.
- The extension of a 7-year fraud alert with the notification letter, or the allowance of a free credit freeze, should the consumer prefer that option. This extension should also permit the affected person to receive a credit report twice a year, the same as victims of identity theft.
- This law should be the standard for all breach notifications, but should not pre-empt state laws with tighter requirements.
- There should be a state right of action, plus a business right of action in the event that a subcontractor costs a business expenses it would not incur otherwise.
- Notification needs to be provided no matter in what form the exposed data was stored. Currently most legislation seems to have overlooked that we are still a paper driven society. According to ITRC statistics, in 2009 about 25% of all breaches were paper breaches
- A requirement that the notification letter include a contact phone number in case a consumer has additional questions.
- The legislation should have a provision giving industry the ability to use substitute means of notification in specific circumstances to save money should the affected population be of significant size.
- ITRC recommends the creation of one national master database which includes copies of all notification letters and the electronic publication of said list. One agency that might be tasked with this would be the Federal Trade Commission. This list should be updated weekly. It should be set up similar to the one used by the New Hampshire Attorney General which allows various field sorting.
    - This national breach database should be considered a way for victims to find out about breaches. However, equally important, a single database provides a source

to research data breaches and provide further information needed to help control this problem. That information could be added into the "Red Flags Compliance Guidelines" or become the basis for a new set of information protection guidelines.

- This legislation should not require entities to purchase any consumer products for remediation purposes.
- To encourage safe information handling practices, and reward responsible companies or agencies that have adopted good security measures, if the data lost was encrypted or rendered unreadable by strong protective measures (password protection not included), then the entity should not be required to send out notification letters to the affected individuals and should not be included in the master notification list.
- However, the company should still be required to notify the agency designated to compile the national breach list so that statistics about these breaches (encrypted or strongly protected) can be monitored.

8. Patient/Victim Rights as a Result of Medical Identity Theft:

Finding: Medical identity theft victims should have the right to see their medical records, including records in which an imposter has used their information fraudulently, and have that fraudulent information removed from their files.

When a person finds out that an imposter has gained medical care using their medical insurance policy number, name or Social Security number, he/she has both financial and medical record issues to correct. When attempting to correct or remove the medical records created by the imposter, the victim is fighting multiple HIPPA rules that were not written in a manner to allow correction of medical identity theft.

Years ago, when a victim asked a creditor for records on a account they claimed was identity theft, they were denied access to those records because the records "belonged" to the imposter and it might be a violation of privacy. That was corrected with the passage of FCRA Section 609e and 605b which allows for the blocking of fraudulent information.

Recommendation: A similar process needs to be put into place for medical files. The victim needs to see what information is on their own medical records that **may be part of the records of the imposter,** and have the right to redact this information from their own medical files. HIPPA does not allow medical records to be deleted. This could be addressed by the creation of a second file linked to the primary true file and a notation that a second person may be using the victim's information. Red Flag Guidelines for authentication of patients will help but not solve existing problems. This could become a growing problem as we move toward centralized electronic medical records.

9. Collection Agency Issues

Finding: Identity theft victims should have the right be treated as victims by the collection industry, and have a process created that will regulate collection agencies when dealing with "reported" fraudulent accounts.

The Fair Debt Collections and Practices Act (FDCPA) was created to regulate the collection industry while trying to recover legitimate debts. This industry is a necessary part of the business community and plays a vital role in minimizing business loss.

The law does not, however, address the issues that are presented by victims of identity theft who are not **disputing a collection**, but rather are reporting that the **account never belonged to them**. These victims have the right to a regulated process that collection agencies must follow once they have been presented with the proper credential indicating that a fraud has occurred.

> Today, many collection agencies bounce victims back to creditors who then refer the person back to the collection agency that "owns the account." Victims deal with customer service representatives who are used to "getting the money."

Recommendation: Congress should either create new regulations or add language to the FDCPA regarding identity theft issues. This language should include:

- Once a victim has provided standardized documentation of a fraudulent case, a set of procedures should be created to clear the record from both the collection agency files and the original creditor (or company that now in possession of the record).
- Once a victim has provided this documentation, all communications will be of a nature to help resolve the situation. Debt collection and "asking for the money" will not be legally allowed after documentation has been provided in legal format.
- Once a case has been declared "closed due to fraud," it cannot be sold, traded or provided to another collection agency. Additionally, the initial collection agency contacted by the victim is to complete the investigation/transaction until complete even if it exceeds the 7-year deadline discussed in the FDCPA.
- A letter of clearance shall be provided to the victim indicating the fraudulent account has been marked as such, removed from the victim's credit report, and notice has been provided to the creditor.
- Private right of action shall be provided to governmental agencies and the victims for disregard of the new standardized identity theft procedures.

10. Secondary Impacts of Identity Theft

Finding: Identity theft victims should have the right to protection from punitive actions taken against them by secondary entities until an investigation is complete and credit reports and credit scores have been corrected.

In the *Aftermath Study* questionnaire, and while working as victim advocates, ITRC has asked victims if there are any secondary effects we need to deal with due to identity theft. Many victims still find out about the crime when being denied credit, employment or loans. This occurs because their credit and consumer reports have already been impacted by fraudulent activities of the imposter. This misinformation may take months to clear. While the *Aftermath Study* shows a steady decrease in the time needed to clear all issues of misinformation, 53% of

respondents reported it took up to six months. Nearly 30% reported it took 7-23 months and another 20% took more than two years to clear their name.

Unfortunately, that delay does not help a victim who found out about the crime while applying for a home loan or other time-sensitive issues. While "trade-line blocking," a right under FACTA, does provide some relief, it does not apply to consumer reports used for employment. It is sometimes refused by the creditor, who has found the victim "guilty" despite a police report and/or proof of other crimes by the perpetrator. Lower credit scores have resulted in the denial of new lines of credit or tenancy, higher auto and home insurance rates. It may cause the closure of credit cards not affected by the case, and denial of employment or promotions. These are situations that are not easy to rectify. The denial of new credit and the closure of existing cards appear to be at an all-time high.

Recommendation: Our legal system is based on the principle of "innocent until proven guilty." The opposite is true in identity theft. Victims must prove they did not create the fraudulent accounts or records that resulted in a "risky" credit or consumer report. Victims should have the right to have their report marked as "under investigation due to reports of fraudulent activity" if they provide a confirmed and valid police report. Companies that might take an adverse action based upon a negative consumer/credit report, should be required to suspend such action until that remark is removed and the report reflects the correct information. Additionally, victims should have the right to send affidavits with valid police reports to the individual companies if that company has already taken negative actions. Upon receipt of that paperwork, the company must restore the victim to their prior status until the case is resolved.

In Conclusion:

The crime of identity theft continues to grow and evolve along with the changes in our society. The thieves take advantage of new opportunities provided by weaknesses in technology and document handling, and changes in consumer patterns. In 1970, the writers of the FCRA could not have predicted the credit trends and practices of 2003, let alone 2009.

There will be a continual need for updating laws to provide identity theft victims the rights and tools they need to restore their good names. Congress should consider having a subcommittee specific to identity theft and cybercrime issues. This would allow members to stay as current about this crime as the industry experts, businesses and criminals. As a PhD candidate in identity theft, I know that even a short gap in reading the research and media articles about identity theft makes one out-of-touch with this fast-changing subject.

As you consider the rights of victims and laws that will either assist victims or limit the risk of becoming a victim, it is critical that the Members of Congress remember that these laws will need to be revisited and modified over time. **In the world of identity theft, today is tomorrow**. Criminals are already planning ways to commit new crimes we have not yet anticipated.

Information trafficking and the selling of fraudulent documentation was not even a consideration by many 10 years ago, but they are now a major area of concern. ITRC is constantly researching, reviewing and considering methods to adequately address the identity theft issues of today. We continuously consider these questions from the perspectives of "What is good for all parties involved," and "How can the crooks exploit this?"

ITRC believes that our nation may have become desensitized to the average victim of identity theft due to the sensationalism of extreme cases that make the news. The average victim has deep feelings of rage, a sense of powerlessness, annoyance, isolation, personal financial fears, betrayal, and a sense of being an outcast. Their crime is not over in a matter of minutes but can be measured by months and sometimes years. In the *Aftermath Study* this year, 31% of all respondents felt "sick of being suspect or fighting the system" and 12% felt "they had lost everything." Most people truly don't understand how long it takes to emotionally recover from the life changing events that follow the initial identity theft moment.

ITRC will continue to take a strong stance for identity theft victims' rights, and continue to be the voice of the victim. When a victim faces so many obstacles that they give up, or commit suicide, something is seriously wrong. This is not a victimless crime. Identity theft victims are trauma victims. They need to be validated, informed, and acknowledged as victim and not the cause of the crime. Victims of identity theft need to know they are not alone and that the crime committed against them is real, and taken seriously by their government.

The recommendations in this written testimony are not structured in legal language, but rather are guidelines for legislative action. ITRC would be honored to serve in any manner to help create the language of these laws. It is a daunting task to both help victims, and also make sure that few loopholes are created in this type of legislation.

Through our testimony we introduced you to some of the victims who have helped us to understand the changes that must be made in the areas of victims' rights. We hope their stories illuminate the issues as clearly for you as they have for us.

Thank you for your time and consideration.

Eric Handy on behalf of the Identity Theft Resource Center

Addendum:

Case history: *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 talked to a detective on a regular basis; only to find out they would do nothing. They had the address to which the credit cards and computer were sent 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. 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.*