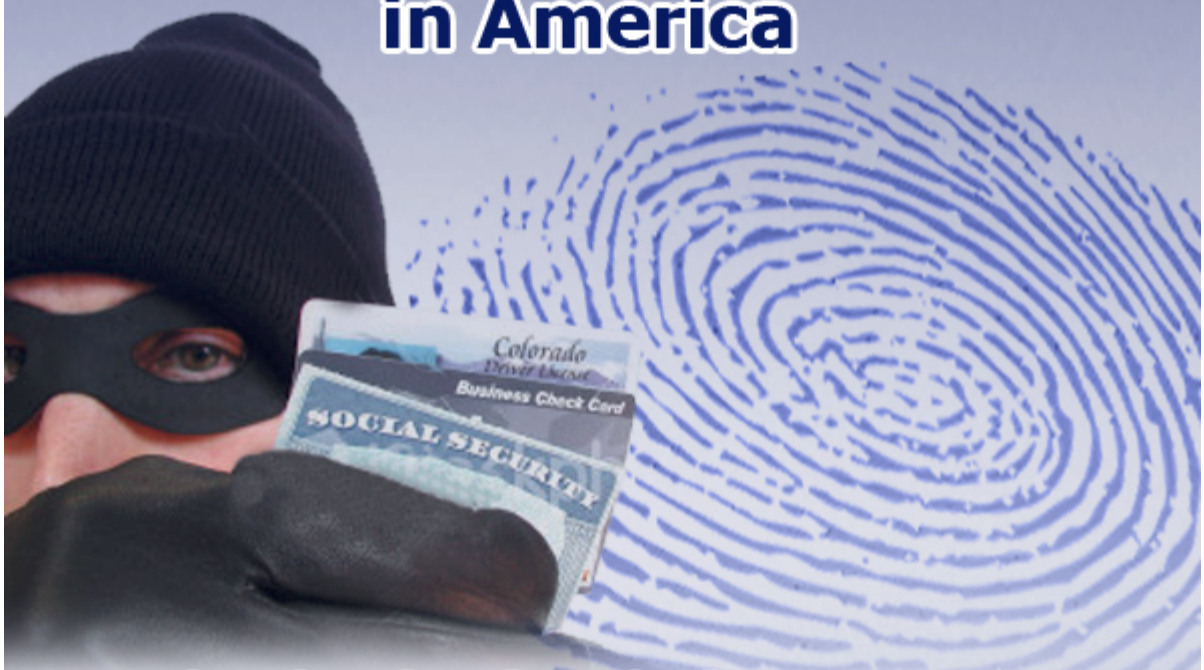
How to Avoid IDENTITY THEFT

The #1 White Collar Crime in America



1. What is Identity Theft?
2. How Your Identity is Stolen
3. What is Done With Your Identity!
4. How to Avoid Being Victimized
5. What To Do If Your Identity Is Stolen

Ronald E. Hudkins

Table of Contents

Chapter One Introduction

Chapter Two Who Am I and Why Do I Care?

Chapter Three What Exactly is Identity Theft?

Chapter Four Identity Theft Statistics

Chapter Five How Do Thieves Steal an Identity?

Chapter Six How Long Can ID Theft Impact You?

Chapter Seven What Can You Do About ID Theft

Chapter Eight Identity Theft Resource Center

Chapter Nine Identity Theft Statement (Letter Sample Format)

Chapter Ten What Is an Identity Theft Report?

Chapter Eleven ID Theft Service Providers Compared

Appendix One LifeLock ID Theft Protection

Resources

Recommended Products and Services

Legal Notice

Chapter One

Introduction

It Really is Time to Worry About Identity Theft!

All of us, no matter how careful, can become victims of identity theft. In fact, it was determined every three seconds another identity is stolen. In 2007 there were seventy nine million credit card and Social Security Number thefts according to major news media investigations. That was an increase of four million additional people over the previous years statistics, that had their identity or financial information compromised. This makes identity theft one of the fastest growing crimes in America.

Anyone with a Social Security number and assets to loose should be concerned with identity theft. Unfortunately, a common belief by many people is they assume they have nothing significant for thief's to take advantage of. Bear in mind criminals are much better than you are at making use of your information. For example; there is credit card theft where someone steals your credit card and runs up charges. Identity theft is where someone steals your personal information (social security number, date of birth, name, etc.) and uses your identity to open a new line of credit, gain employment or even establish citizenship.

You must realize that your information is stored locally and nationally. Your dentist, doctor, banking facility(s), college transcript and club memberships are examples of data configurations where your personal information is stored. I don't have to remind you there have been numerous sophisticated agencies and institutions hacked into and identities stolen. How easy it would be to have your identity stolen from neighborhood businesses, your mailbox or even your trash receptacles. Yes shredding papers listing your personal information is a great step to protect your identity but as indicated, your information is everywhere.

It's no secret that many savvy consumers have learned to place fraud alerts (more on this later) on their accounts which prompt creditors to call them if someone is trying to establish credit in their names. But did you know these alerts are generally only valid for a period of ninety days? Are you really confident enough to believe your going to take the time or for that matter, even remember to renew fraud alerts every three months? Remember too, just because you have fraud alerts placed does not guarantee you from becoming a victim.

There is an option to implement a credit freeze which locks down all of your personal information making it impossible for anyone to open a line of credit in

your name, including you. There are also fees involved with many credit freezes. When you place a freeze, you pay a fee. From there on, if you want to open any new line of credit (loan, credit card, cell phone) the freeze must be lifted; there will be a fee for that as well. Currently 33 states and the District of Columbia offer the credit freeze option, but if you are not living in one of them, you cannot do this. We'll also later cover credit freezes in complete detail.

Credit watch services have come into prominence thanks to the many breaches that have been publicized. What exactly is a credit watch, and what benefit does such a service offer the consumer? Credit Monitoring (or a watch) is the credit bureau selling the consumer their own information. After there has been a change on your credit report, the bureau notifies you in 24 to 72 hours that there has been a change. It is then the consumer's responsibility to check the information for accuracy and by the way, if they find that it is a case of identity theft, the consumer is responsible for any losses, expenses and has to spend the time to clean up the mess. The Bureaus do nothing to actually prevent the crime of identity theft, nor do they help fix the problem. The FTC says it takes an average of 177 hours and over two years to clean up an identity or credit compromise, if you can clean it up at all.

I'm not trying to come off as a fatalist and give anyone the impression there is nothing that can be done about criminal activity. If you worry about identity theft, then it's time you got to know about identity theft services. These agencies provide proactive identity theft protection. We'll cover your many available options!

On your behalf, ID theft companies request that fraud alerts be placed on your accounts. By placing these fraud alerts, you are asking that creditors take extra care to identify who you are and to investigate the validity of any pending transaction. These services also request that your name be removed from pre-approved credit card lists and junk mail lists. Additionally, services annually order your free credit reports from the three major credit reporting bureaus. In the event that your identity is compromised, qualified professionals are available to assist you in addressing whatever complications may arise.

In summary one might ask; if the consumer can do these things by themselves, what is the need for an identity theft service? The simple answer is nothing more than convenience and protection. The assurance that nothing is overlooked in the shuffle and required responsibilities in everyday living that would keep you from taking the measures necessary to protect your identity. These services have but one concern and mission, to safeguard your identity and assets.

You and I well, we have a lot of ground to cover! I'll do my best to give you a pretty complete understanding of identity theft, the tactics criminals use to steal your good name and assets as well as; your many courses of proactive measures to implement so as to reduce your risks of identity theft. But, most importantly; I'll walk you through the actions you need to take once you realize you have become a victim of identity theft.

Bear in mind even the Federal Trade Commission advises us that putting together a defense that provides complete safety and protection with a 100% probability; can not be 100% guaranteed. I am most certainly not telling you to surrender here and now. My encouragement to keep you reading and educating yourself to thwart criminal activity is really very inspiring. Just think of it this way – Make yourself a less likely target. Let the thief's know that messing with you is less rewarding and a high risk probability of them being caught prosecuted and jailed. Never lesson you vigilance because statistically in 2007 - identity theft remains the number one white collar crime in the United States. The analogy here is really quite simple.

If you were a burglar cruising a neighborhood looking for a home to target you'd of course avoid one in the middle of an active crime watch program. You wouldn't likely try to get into a home that looked occupied, had alarms, guard dogs or an angry person standing on the porch with a shotgun. You'd either be a crack head in serious desperation or, as dumb as a rock. There are just as many measures you can take that alert the identity thief to move on and target a more susceptible person. It's not passing the buck but rather, good old fashioned self preservation.

Visit www.adultwishfoundations.com/Life_Lock.html to learn more about a proactive identity theft protection service that offers - Proactive Identity Theft Protection, Reduced Junk Mail, Reduced Credit Card Offers, $1 Million Service Guarantee, Child Protection Program, Wallet Watch and more for Only $10 per Month.

Chapter Two

Who Am I and Why Do I Care?

Hello, my name is Ronald Hudkins and I retired from the United States Army Military Police Corps honorably in 1993. It doesn't matter if you are a rookie in the civilian or military law enforcement environments; the one thing that always gets a good measure of emphases during training is to NEVER take anything as routine! Never assume – Always anticipate and never think something (anything) can not happen to you.

The one thing great about working law enforcement in the military is during 20 years plus of law enforcement one gets exposed to people (good, bad and indifferent) from every race, color, creed and religious domination. The military contains people that come from every walk of life, small towns, large cities and every country on the planet. It is the mixing bowl where all ingredients get dressed in a uniform that demands cohesion and team work without exception and - despite any personal beliefs otherwise. So realistically when Rodney King screamed up to some overly enthusiastic and miss directed police officers "Why Can't We All Just Get Along?" The military demands it (within its ranks) despite any and all circumstances we get along and succeed at doing so.

While in the military I maintained a Top Secret security clearance for nearly my entire career and than some. It took 18 months to get it and investigators doing the background checks talked to people I no longer remembered or didn't even think I knew. They knew more about me than I even knew or know today. Apparently, despite an unusual sense of humor and inordinate level and capacity for pulling pranks, I was deemed a person of responsibility. It took the military a good measure of attention to get me there but, that's a stand alone story (that would fill a book) and a conversation for another time.

When you are awarded a high security clearance you become a person that is under a microscope constantly. There is always someone somewhere watching you make it from one day to the next. Making sure you don't develop kinky characteristics, unusual sums of money, aren't going mental, Anti-government, bitter, sour and or in any way miss-directed. Your friends, family, acquaintances and every hi and good-by is securitized. It's a national security mind set.

When you have a security clearance you get exposed to things that are hard to believe or, you wish you had never seen or knew. When you retire from the organization, agency or whatever, you are debriefed and advised as to what is to be forgotten and subject to criminal prosecution if leaked. This conversation usually concludes that if something is divulged intentionally or

unintentionally it could result in someone (you choose) being buried so deep, their own family won't even know where they are.

My point here is when you have a security clearance; you don't worry too much about identity thieves as your life is pretty much watched over. Overly curious, criminals, reporters and any capacity of prying personnel somehow magically disappear. When I reached a point in my life where anything I ever knew wasn't worth a reporter from some tabloid buying me a cup of coffee, my life changed. I was no longer a part of that safeguarded environment. Most military and for that matter, civilians don't have a security blanket. Every Superman has their Luther. Another word, not all criminals are stupid. There are brilliant masterminds in every country that use their intelligence capacities for evil in contrast to doing humanly good things.

So yes, despite my one time ability to find the weak links and breach able physical security measures put into place here and there, I became a victim of identity theft. I'm still not over the irritation and audacity of the criminal that ran up a thousand dollar phone bill in my good name. This is minor compared to what identity thieves have done to other people's lives. I still shutter over what it took to clear the whole mess up. It was a lengthy, drawn out requirement of actions needed to put things right. I carried a whole parcel of aggravations, stresses, frustrations and system disappointments. It's over now but, I still remember the comparable migraine string of events it took to put it all behind. There may not be any such thing anywhere that is secure absolutely to include one's identity but, there is deflection, avoidance and minimal impact.

I don't like criminals in any capacity or any excuse they have for being one. It is because of this and my minor victimization by an identity thief that I now make it my mission in life to do the best I can to make sure you don't fall victim as well. That is exactly why this book is free and I encourage you to pass it along to everyone you know or don't know. So, with that said – let's get cracking on how to take apart the identity thieves.

Visit www.adultwishfoundations.com/Life_Lock.html to learn more about a proactive identity theft protection service that offers - Proactive Identity Theft Protection, Reduced Junk Mail, Reduced Credit Card Offers, $1 Million Service Guarantee, Child Protection Program, Wallet Watch and more for Only $10 per Month. It is the service provider that is personally used and highly recommended by the author.

Chapter Three

What Actually is identity theft?

According to the Federal Trade Commission identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

The FTC estimates that as many as 9 million Americans have their identities stolen each year. In fact, you or someone you know may have experienced some form of identity theft. The crime takes many forms. Identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make—or until you're contacted by a debt collector.

Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

Definitions of Identity theft on the Web:

- This is the crime of obtaining the personal or financial information of another person for the purpose of assuming that person's name to make ...
  https://www.fnb.co.za/legallinks/securitycentre/terms.html
- When an unauthorized party fraudulently represents themselves as another party.
  www.hfc.com/learn-about-loans/help/additional_resources/glossary.html
- Please see the Damage Control: Identity Theft page.
  www.albany.edu/its/glossary.htm
- a crime where somebody deliberately impersonates an individual for personal gain. Examples of identity theft are credit card frauds and gaining access under a guise of somebody else.
  www.assaabloyfuturelab.com/FutureLab/Templates/Page2Cols 1503.aspx
- (or identity fraud) occurs when someone wrongfully acquires or uses another person's personal data, typically for their own financial gain. Interest - the price paid for borrowing money. ...
  www.marketprosecure.com/financial-glossary-terms.php

- The act of impersonating another, by means of using the person's information, such as birth date, Social Security number, address, name, and bank account information.
  www.white-collar-crimes.com/criminal_terms.shtml
- The fraudulent act of collecting sufficient personal information about an individual in order that their identity can be assumed for the purposes of carrying out some other illegal or malicious activity.
  www.h-spot.net/threat_glossary.htm
- the co-option of another person's personal information (e.g., name, Social Security number, credit card number, passport) without that person's knowledge and the fraudulent use of such knowledge
  wordnet.princeton.edu/perl/webwn
- Identity taker is a term first appearing in U.S. literature in the 1990s, leading to the drafting of the Identity Theft and Assumption Deterrence Act.
  en.wikipedia.org/wiki/Identity theft
- A crime of stealing personal and/or financial information, such as name, Social Security Number, or account numbers from a person, with the intent to commit fraud.
  www.awbank.net/security_glossary1.asp

According to the Internets Wikipedia Free Encyclopedia at http://en.wikipedia.org/wiki/Identity_theft Identity theft is a catch-all term for crimes involving illegal usage of another individual's identity. The most common form of identity theft is

According to the non-profit Identity Theft Resource Center, identity theft is sub-divided into four categories:

- Financial Identity Theft (using another's identity to obtain goods and services)
- Criminal Identity Theft (posing as another when apprehended for a crime)
- Identity Cloning (using another's information to assume his or her identity in daily life)
- Business/Commercial Identity Theft (using another's business name to obtain credit)

Identity theft may be used to facilitate crimes including illegal immigration, terrorism and espionage. Identity theft may also be a means of blackmail. There are also cases of identity cloning to attack payment systems, including medical insurance.

We will cover specific examples of identity theft in proceeding chapters. For now however, you have a pretty good realization of its extent just based upon some limited definitions.

Chapter Four

Identity Theft Statistics

If you really do not care about statistics, you can skip this chapter however, there are some proactive measures listed in the data that you can take to avoid identity theft. I'll cover these and other measures in greater detail in later chapters. There are live links left imbedded for the agencies to expand upon their reports and - I also like to give credit to everyone else's research and professional capacities.

There is a lot of information about identity theft. It is a real and expanding problem. Do a Google search "identity theft" and you will get as of the date of this writing over 20 million pages of information. I'll reduce it down to bite size increments for your better understanding of the problem and measures needed for you to undertake in the face of it all be it proactive or in the capacity of a victim.

How Many Identity Theft Victims Are There?
What Is the Impact on Victims?

Recent Surveys and Studies from Javelin Strategy & Research,
Better Business Bureau, Identity Theft Resource Center,
Federal Trade Commission,
Gartner, and Privacy & American Business

Contents:

Javelin Strategy & Research Survey - February 2007

In February 2007, Javelin Strategy and Research released its 2007 Identity Fraud Survey Report. The report is issued as a longitudinal update to previous Javelin Identity Fraud Survey reports and the Federal Trade Commission's (FTC) 2003 Identity Theft Survey Report.

Survey findings Include:

- The number of US adult victims of identity fraud decreased from 10.1 million in 2003 and 9.3 million in 2005 to 8.4 million in 2007.
- Total one year fraud amount decreased from $55.7 billion in 2006 to $49.3 billion in 2007.
- The mean fraud amount per fraud victim decreased from $6,278 in 2006 to $5,720 in 2007.

- The mean resolution time was at a high of 40 hours per victim in 2006 and was reduced in 2007 to 25 hours per victim. The median resolution time has remained the same for each Survey year at 5 hours per victim.

Javelin/Better Business Bureau Survey - January 2006 (no charge for Consumer Version)

In January 2006, Javelin Strategy and Research co-released its 2006 Identity Fraud Survey Report with the Better Business Bureau. The report is issued as a longitudinal update to the Javelin 2005 Identity Fraud Survey Report and the Federal Trade Commission's (FTC) 2003 Identity Theft Survey Report. The Consumer Version of the survey is available at no cost.

Survey findings Include:

- The number of US adult victims of identity fraud decreased from 10.1 million in 2003 and 9.3 million in 2005 to 8.9 million in 2006.
- Total one year fraud amount rose from $53.2 billion in 2003 and $54.4 billion in 2005 to $56.6 billion in 2006.
- The mean fraud amount per fraud victim rose from $5,316 in 2003 and $5,993 in 2005 to $6,278 in 2006.
- The mean resolution time is at a high of 40 hours per victim in 2006 compared to 28 hours in 2005 and 33 hours in 2003.

Javelin/Better Business Bureau Survey - January 2005

On January 26, 2005, the Better Business Bureau in conjunction with Javelin Strategy and Research released its Identity Theft survey as an update to the Federal Trade Commission's 2003 Identity Theft Survey Report. The full report is available online at http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html.

Survey findings include:

- Within the last twelve months, 9.3 million Americans were victims of identity theft.
- The total U.S. annual identity fraud cost remains essentially unchanged since [the FTC's] 2003 [results], at $52.6 Billion, an increase of 2.3% from the 2003 inflation-adjusted level of $51.4 Billion.
- Most thieves still obtain personal information through traditional rather than electronic channels. In the cases where the method was known, 68.2% of information was obtained off-line versus only 11.6% obtained online.
- Conventional methods such as through lost or stolen wallets, misappropriation by family and friends, and theft of paper mail are among the most common ways thieves gain access to information.

Recommendations for consumers include:

- Cancel your paper bills and statements wherever possible and instead check your statements and pay bills online. Monitor your account balances and activity electronically (at least once per week).
- If you do not have access to online accounts, review paper bank and credit card statements monthly and monitor your billing cycles for missing bills or statements.
- Use email based account "alerts" to monitor transfers, payments, low balances and withdrawals and review your credit report (now available for free annual review).

Identity Theft Resource Center - September 2003

On September 23, 2003, the Identity Theft Resource Center (www.idtheftcenter.org) released its survey of the impact of identity theft on 173 known victims. To read the full survey, see: www.idtheftcenter.org/idaftermath.pdf

Survey findings include:

- Nearly 85% of all victims find out about their identity theft case in a negative manner. Only 15% of victims find out due to a proactive action taken by a business.
- The average time spent by victims is about 600 hours, an increase of more than 300% over previous studies.
- While victims are finding out about their cases earlier, it is taking far longer now than before to eliminate negative information from credit reports.
- A large majority of respondents indicates the opening of a credit card (73%) or takeover of a card account (27%) to be among crimes committed.
- The emotional impact of identity theft has been found to parallel that of victims of violent crime.
- The responsiveness toward victims by the various entities with which they must interact continues to be lacking in sensitivity in most cases and has not improved since studies released in 2000 (Nowhere to Turn).

Federal Deposit Insurance Corporation - December 2004

On December 14, 2004, the Federal Deposit Insurance Corporation (FDIC) released a study on phishing and account-takeover including information about fraudulent automated clearing house (ACH) payments. A complete copy of the FDIC's study is available online at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

Key findings include:

- While precise statistics on the prevalence of account hijacking are difficult to obtain, recent studies indicate that unauthorized access to checking accounts is the fastest growing form of identity theft.
- Another recent study has estimated that almost 2 million U.S. adult Internet users experienced this fraud during the 12 months ending April 2004. Of those, 70 percent do their banking or pay their bills online and over half believed they received a phishing e-mail.
- Consumers are attributing risk to their use of the Internet to conduct financial transactions, and many experts believe that electronic fraud, especially account hijacking, will have the effect of slowing the growth of online banking and commerce.
- Up to 5 percent of the recipients of spoofed e-mails respond to them.
- An estimated 19 percent of "those attacked" have clicked on the link in a phishing e-mail. Most, if not all, large financial institutions and electronic bill-paying services (such as PayPal) have been hit with phishing attacks.
- Because many phishing attacks originate overseas and because the average life span of a phishing Web site is 2.25 days, the sites are hard to shut down.

Federal Trade Commission Survey - September 2003

On September 3, 2003, the Federal Trade Commission (FTC) issued a survey on identity theft. The survey was conducted in March and April of 2003 with a random sample of over 4,000 households. To read the survey, go to http://www.ftc.gov/os/2003/09/synovatereport.pdf

Key findings include:

How Many Consumers Are Victims of Identity Theft?

- 27.3 million Americans have been victims of identity theft in the last five years, including 9.91 million people or 4.6% of the population in the last year alone.
- In the past 12 months, 3.23 million consumers or 1.5% of the population discovered that new accounts had been opened, and other frauds such as renting an apartment or home, obtaining medical care or employment, had been committed in their name. 6.6 million experienced their existing accounts compromised by an identity theft. A total of almost 10 million individuals were victims of identity theft.
- 52% of all ID theft victims, approximately 5 million people in the last year, discovered that they were victims of identity theft by monitoring their accounts.

Misuse of Personal Information

- On average, 49% of victims did not know how their information was obtained.
- Another 26% - approximately 2.5 million people - reported that they were alerted to suspicious account activity by companies such as credit card issuers or banks.
- 8% reported that they first learned when they applied for credit and were turned down.
- 15% of all victims - almost 1.5 million people in the last year - reported that their personal information was misused in nonfinancial ways, to obtain government documents, for example, or on tax forms.
- 67% of identity theft victims - more than 6.5 million victims in the last year - report that existing credit card accounts were misused.
- 19% reported that checking or savings accounts were misused.
- Nearly one-quarter of all victims - roughly 2.5 million people in the last year - said their information was lost or stolen, including lost or stolen credit cards, checkbooks or social security cards.
- Stolen mail was the source of information for identity thieves in 4 percent of all victims - 400,000 in the last year.

Costs to Businesses and Consumers

- Last year's identity theft losses to businesses and financial institutions totaled $47.6 billion and consumer victims reported $5 billion in out-of-pocket expenses.
- In those cases, the loss to businesses and financial institutions was $10,200 per victim totaling $32.9 billion. Individual victims lost an average of $1,180 for a total of $3.8 billion.
- Where the thieves solely used a victim's established accounts, the loss to businesses was $2,100 per victim totaling $14.0 billion. For all forms of identity theft, the loss to business was $4,800 and the loss to consumers was $500, on average.

Gartner Survey - July 2003

On July 21, 2003, Gartner (www.gartner.com) released the results of a survey of 2,445 households regarding identity theft. To read the press release, go to: http://www3.gartner.com/5_about/press_releases/pr21july2003a.jsp

The survey found the following:

- Identity theft is up nearly 80 percent from last year.
- 7 million U.S. adults or 3.4 percent of U.S. consumers were identity theft victims in the past 12 months.

- Because this crime is often misclassified, the thieves have just a one in 700 chance of being caught by the federal authorities.

Privacy & American Business Survey - July 2003

A July 30, 2003, *Privacy & American Business* survey found the following. To read the press release, go to http://www.pandab.org/id_theftpr.html.

How Many Consumers Are Victims of Identity Theft?

- 33.4 million Americans were victims of identity theft since 1990.
- Over 13 million Americans have become victims of identity theft since January 2001.
- Consumer out-of-pocket expenses have totaled $1.5 billion annually since January 2001.
- 34% say someone obtained their credit card information, forged a credit card in their name, and used it to make purchases.
- 12% say someone stole or obtained improperly a paper or computer record with their personal information on it and used that to forge their identity.
- 11% say someone stole their wallet or purse and used their identity.
- 10% say someone opened charge accounts in stores in their name and made purchases as them.
- 7% say someone opened a bank account in their name or forged checks and obtained money from their account.
- 7% say someone got to their mail or mailbox and used information there to steal their identity.
- 5% say they lost their wallet or purse and someone used their identity.
- 4% say someone went to a public record and used information there to steal their identity.
- 3% say someone created false IDs and posed as them to get government benefits or payments.
- 16% say it was a friend, relative or co-worker who stole their identity.
- The seven million victims the survey identified in 2002 represent an 81% rise over victims in 2001.
- Identity theft incidents reported so far in 2003 suggest a major rise over 2002. The victims level and upward trend parallel findings of a Gartner survey released last week.

What Are Victims' Out of Pocket Expenses?

- While 62% of victims did not incur any out-of-pocket expenses, 38% did, representing 13-14 million Americans.
- Since January 2001, these 38% have paid approximately $3.8 billion, or an average of $1.5 billion per year. Based on actual amounts

volunteered by respondents themselves, the average cost per victim for this time period is $740.

- An earlier June 2002 survey on ID theft by *P&AB* and Harris found that a majority of Americans, 91%, do not see light at the end of the tunnel; they expect heavy ID theft incidents to increase rather than decrease in the near future.
- The 2002 survey also found that 49%, or 98 million adults, feel they do not know how to protect themselves against identity theft.
- One in six consumers, representing almost 34 million, say they have bought a privacy protection product to help avoid identity theft, to check their credit report, and to surf or shop online anonymously. At $75, the average annual price for these products, these figures represent a $2.5 billion expenditure.

Chapter Five

How do thieves steal an identity?

The Federal Trade Commission tells us that identity theft starts with the misuse of your personally identifying information (PII) such as your name and Social Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold. Skilled identity thieves may use a variety of methods to get hold of your information, including:

1. Dumpster Diving. They rummage through trash looking for bills or other paper with your personal information on it.
2. Skimming. They steal credit/debit card numbers by using a special storage device when processing your card.
3. Phishing. They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. Changing Your Address. They divert your billing statements to another location by completing a change of address form.
5. Old-Fashioned Stealing. They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access to your personal information.
6. Pretexting. They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.
7. Retrieving (Wekipedia adds) information from redundant equipment which has been disposed of carelessly, e.g. at public dump sites, given away without proper sanitizing etc.
8. Stealing payment or identification cards, either by pickpocketing or surreptitiously by skimming through a compromised card reader
9. Remotely reading information from an RFID chip on a smartcard, RFID-enabled credit card, or passport
10. Trojan horses, hacking Stealing personal information in computer databases.
11. Advertising bogus job offers (either full-time or work from home based) to which the victims will reply with their full name, address, curriculum vitae, telephone numbers, and banking details
12. Infiltration of organizations that store large amounts of personal information
13. Obtaining castings of fingers for falsifying fingerprint identification.
14. Browsing social network (MySpace, Facebook, Bebo etc) sites, online for personal details that have been posted by users
15. Simply researching about the victim in government registers, at the Internet, Google, and so on.

What is "pretexting" and what does it have to do with identity theft?

Pretexting is the practice of getting your personal information under false pretenses. Pretexters sell your information to people who may use it to get credit in your name, to steal your assets, or to investigate or sue you. Pretexting is against the law.

Pretexters use a variety of tactics to get your personal information. For example, a pretexter may call, claim he's from a research firm, and ask you for your name, address, birth date, and social security number. When the pretexter has the information he wants, he uses it to call your financial institution. He pretends to be you or someone with authorized access to your account. He might claim that he's forgotten his checkbook and needs information about his account. In this way, the pretexter may be able to obtain other personal information about you such as your bank and credit card account numbers, information in your credit report, and the existence and size of your savings and investment portfolios.

Keep in mind that some information about you may be a matter of public record, such as whether you own a home, pay your real estate taxes, or have ever filed for bankruptcy. It is not pretexting for another person to collect this kind of information.

By law, it's illegal for anyone to:

- use false, fictitious or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution.
- use forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution.
- ask another person to get someone else's customer information using false, fictitious or fraudulent statements or using false, fictitious or fraudulent documents, or forged, counterfeit, lost, or stolen documents.

Why Do We Need to Worry About Dumpster Diving?

The best thing about it for people who make a living off the practice is that generally this is a LEGAL livelihood! Stealing trash is not illegal according to The Supreme Court ruling in 1988 that stipulated once an item is left for trash pickup, there is no expectation of privacy or continued ownership. If you do a Google search on the Internet, there are over 842,000 pages dedicated to dumpster diving. There are thousands of WebPages dedicated to the fine art, techniques and guidelines to successful dumpster diving.

It should in my opinion and others, be a first step consideration in any serious business or personal intrusion. The dumpster diving hacker can map out the target, understand the interpersonal relationships that can be subverted, and most important, can glean technical details, often passwords and account names from the tons of trash they are swimming in.

When it comes to businesses, taking papers from dumpsters outside offices is a common tactic used by commercial information brokers as well as foreign intelligence services. "Trash cover" is a standard methodology used by investigators and intelligence agents throughout the world. It involves collecting and going through the trash left out for collection in front of residents and businesses. Trash may also be stolen from waste baskets by cleaning crews.

In the aspect of residential trash; It is estimated that upwards of 80 percent or more households do not take the necessary steps to prevent dumpster diving or make it less of an effective tactic for thieves. Instead, they let their sensitive, personal information sit at the curb--waiting to be harvested.

Consider the fact that we all get mail and have documents that contain some very personal information. Credit card and bank statements, utility bills, insurance polices medical records and more. All of which, contain critical pieces of the puzzle that once put together by an identity thief, can be used to exact a financial quagmire that could literally, take years to recover from.

There is an old saying that "one man's trash is another man's treasure." That is certainly true in the intelligence world.

Some of the things that dumpster diving, hackers look for are as follows:

- Phone lists

Helps map out the power structure of the company, and gives possible account names, and is essential in appearing as a member of the organization.

- Memos

Reveal activities inside the target organization.

- Policy manuals

Today's employee manuals give instructions on how not to be victimized by hackers, and likewise help the hacker know which attacks to avoid, or at least try in a different manner than specified in the policy manual.

- Calendars of events

Tells the hackers when everyone will be elsewhere and not logged into the system. Best time to break in.

- System manuals, packing crates

Tells the hackers about new systems that they can break into.

- Print outs
- Source code is frequently found in dumpsters, along with e-mails (revealing account names), and Post It & tm; notes containing written passwords.

- Disks, tapes, CD-ROMs

People forget to erase storage media, leaving sensitive data exposed. These days, dumpsters may contain larger number of "broken" CD-Rs. The CD-ROM "burning" process is sensitive, and can lead to failures, which are simply thrown away. However, some drives can still read these disks, allowing the hacker to read a half-way completed backup or other sensitive piece of information.

- Old hard drives

Like CD-ROMs, information from broken drives can usually be recovered. It depends only upon the hacker's determination.

- Organizational changes, such as mergers, acquisitions, and "re-orgs" leave the company in disarray that can be exploited by hackers (in much the same way those hackers look upon January 1, 200X as a prime hacking day).

Dumpster Diving is when an identity thief will go through your trash in order to obtain copies of your checks, credit card or bank statements, or other records--all for the sake of harvesting your personally identifiable information to steal your identity.

Another thing to consider is Tax Season is Bringing Out Identity Thieves!

A number of clients have recently reported to their tax preparation services that they have been receiving calls from someone posing as a representative from the Social Security Administration. The caller began the conversation by talking about the pending Congressional leader's announcement where a deal with the White House on the economic stimulus package would give most tax filers refunds of $600 to $1,200, and more if they have children. The caller went on to solicit from consumers their Social Security number stating confirmation of their number would ensure they received their rebate checks within the next 6 – 7 months.

The Social Security Administration is not making a conscience effort to confirm consumer identification numbers. You need to be aware that identity thief's are however and they use a number of tactics to steal your identity.

Spoofing is generally used by thieves as a means to convince individuals to provide personal or financial information that enables the perpetrators to commit credit card/bank fraud or other forms of identity theft. An attempt to fraudulently acquire sensitive financial or personal information, such as credit card information or a Social Security number, by impersonating a business representative or trustworthy person is also known as a Phishing attempt and is usually initiated through e-mail, phone calls or Instant Messaging.

Thieves do not just collect Social Security Numbers. They are also after your telephone records, date of birth and your bank and credit card account numbers. This information is a personal asset as well and people who illegally solicit this information are also known as pretexters. It is yet another name for identity theft and Pretexting is (like the other practices mentioned) a means of getting your personal information under false pretenses. Pretexters sell your information to people who may use it to get credit in your name, steal your assets, or to investigate or sue you. Pretexting is against the law.

Whether it is by means of Spoofing, Phishing or Pretexting the tactics are all designed to get your personal information. According the Federal Trade Commission For example, a pretexter may call, claim he's from a survey firm, and ask you a few questions. When the pretexter (let's just call it a thief) has the information they want, it is used to call your financial institution. The thief pretends to be you or someone with authorized access to your account. They might claim that they have forgotten their checkbook and need information about their account. In this way, the criminal may be able to obtain personal information about you such as your SSN, bank and credit card account numbers, information in your credit report, and the existence and size of your savings and investment portfolios.

Keep in mind that some information about you may be a matter of public record, such as whether you own a home, pay your real estate taxes, or have ever filed for bankruptcy. It is not pretexting for another person to collect this kind of information.

The United States Department of Justice advises us that, "Many people do not realize how easily criminals can obtain our personal data without having to break into our homes. In public places, for example, criminals may engage in "shoulder surfing" i.e. watching you from a nearby location as you punch in your telephone calling card number or credit card number or listen in on your conversation while you give your credit-card information."

They further advise us "If you receive applications for "preapproved" credit cards in the mail, but discard them without tearing up the enclosed materials, criminals may retrieve them and try to activate the cards for their use without your knowledge. (Some credit card companies, when sending credit cards, have adopted security measures that allow a card recipient to activate the card only from his or her home telephone number but this is not yet a universal practice.) Also, if your mail is delivered to a place where others have ready access to it, criminals may simply intercept and redirect your mail to another location."

Additionally, The Department of Justice states, "In recent years, the Internet has become an appealing place for criminals to obtain identifying data, such as passwords or even banking information about you. In their haste to explore the exciting features of the Internet, many people respond to "spam" unsolicited E-mail that promises them some benefit but requests identifying data, without realizing that in many cases, the requester has no intention of keeping his promise. In some cases, criminals reportedly have used computer technology to obtain large amounts of personal data."

Examples of identity theft provided by Wikipedia (The free Internet Encycopedia are as follows;

Financial identity theft

A classic example of credit-dependent financial crime (bank fraud) occurs when a criminal obtains a loan from a financial institution by impersonating someone else. The criminal pretends to be the victim by presenting an accurate name, address, birth date, or other information that the lender requires as a means of establishing identity. Even if this information is checked against the data at a national credit-rating service, the lender will encounter no concerns, as all of the victim's information matches the records. The lender has no easy way to discover that the person is pretending to be the victim, especially if an original, government-issued id can't be verified (as is the case in online, mail, telephone, and fax-based transactions). This kind of crime is considered non-self-revealing, although authorities may be able to track down the criminal if the funds for the loan were mailed to him. The criminal keeps the money from the loan, the financial institution is never repaid, and the victim is wrongly blamed for defaulting on a loan he never authorized.

Other forms of examples of bank fraud associated with identity theft include "account takeovers," passing bad checks, and "busting out" a checking or credit account with bad check, counterfeit money order, or empty ATM envelope deposits.

Identity cloning and concealment

In this situation, a criminal acquires personal identifiers, and then impersonates someone for concealment from authorities. This may be done by a person who wants to avoid arrest for crimes, by a person who is working illegally in a foreign country, or by a person who is hiding from creditors or other individuals. Unlike credit-dependent financial crimes, these crimes can be non self-revealing, continuing for an indeterminate amount of time without being detected.

Criminal identity theft

When a criminal identifies himself to police as another individual it is sometimes referred to as "Criminal Identity Theft." In some cases the criminal will obtain a state issued ID using stolen documents or personal information belonging to another person, or they might simply use a fake ID. When the criminal is arrested for a crime, they present the ID to authorities, who place charges under the identity theft victim's name and release the criminal. When the criminal fails to appear for his court hearing, a warrant would be issued under the assumed name. The victim might learn of the incident if the state suspends their own drivers license, or through a background check performed for employment or other purposes, or in rare cases could be arrested when stopped for a minor traffic violation. It can be difficult for a criminal identity theft victim to clear their record. The steps required to clear the victim's incorrect criminal record depend on what jurisdiction the crime occurred in and whether the true identity of the criminal can be determined. The victim might need to locate the original arresting officers, or be fingerprinted to prove their own identity, and may need to go to a court hearing to be cleared of the charges. Obtaining an expungement of court records may also be required. Authorities might permanently maintain the victim's name as an alias for the criminal's true identity in their criminal records databases. One problem that victims of criminal identity theft may encounter is that various data aggregators might still have the incorrect criminal records in their databases even after court and police records are corrected. Thus it is possible that a future background check will return the incorrect criminal records.

Even though the laws are on your side, it’s wise to take an active role in protecting your information. The Federal Trade Commission recommends the following actions;

1. Don’t give out personal information on the phone, through the mail or over the Internet unless you’ve initiated the contact or know who you’re dealing with. Pretexters may pose as representatives of survey firms, banks, Internet service providers and even government

agencies to get you to reveal your SSN, mother's maiden name, financial account numbers and other identifying information. Legitimate organizations with which you do business have the information they need and will not ask you for it.

2. Be informed. Ask your financial institutions for their policies about sharing your information. Ask them specifically about their policies to prevent pretexting.
3. Pay attention to your statement cycles. Follow up with your financial institutions if your statements don't arrive on time.
4. Review your statements carefully and promptly. Report any discrepancies to your institution immediately.
5. Alert family members to the dangers of pretexting. Explain that only you, or someone you authorize, should provide personal information to others.
6. Keep items with personal information in a safe place. Tear or shred your charge receipts, copies of credit applications, insurance forms, bank checks and other financial statements that you're discarding, expired charge cards and credit offers you get in the mail.
7. Add passwords to your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.
8. Be mindful about where you leave personal information in your home, especially if you have roommates or are having work done in your home by others.
9. Find out who has access to your personal information at work and verify that the records are kept in a secure location.

Checking your credit report annually can help you catch mistakes and fraud before they wreak havoc on your personal finances. Order a copy of your credit report from the three nationwide consumer reporting companies every year. To order your free annual report from one or all the nationwide consumer reporting companies, call toll-free 1-877-322-8228, or complete the Annual Credit Report Request Form avail at their Website www.annualcreditreport.com , and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. We'll go into some

additional proactive measures in further detail in later chapters. We are far from being completely informed! I have more to say about credit reports, proactive measures (pros and cons) in later chapters as well. Do not mean to be redundant but, there is just so much to consider about this ever expanding criminal activity, countering it and self preservation measures.

If you do not have the time or expertise to put measures in place to protect you and your family's identity consider visiting a credit protection service that can put the appropriate measures in place to preserve your good name, credit and assets.

Chapter Six

How long can the effects of identity theft last?

It's difficult to predict how long the effects of identity theft may linger. That's because it depends on many factors including the type of theft, whether the thief sold or passed your information on to other thieves, whether the thief is caught, and problems related to correcting your credit report.

Victims of identity theft should monitor financial records for several months after they discover the crime. Victims should review their credit reports once every three months in the first year of the theft, and once a year thereafter. Stay alert for other signs of identity theft.

Don't delay in correcting your records and contacting all companies that opened fraudulent accounts. Make the initial contact by phone, even though you will normally need to follow up in writing. The longer the inaccurate information goes uncorrected, the longer it will take to resolve the problem.

Chapter Seven

What can you do to help fight identity theft?

A great deal says the Federal Trade Commission;

Awareness is an effective weapon against many forms identity theft. Be aware of how information is stolen and what you can do to protect yours, monitor your personal information to uncover any problems quickly, and know what to do when you suspect your identity has been stolen.

Armed with the knowledge of how to protect yourself and take action, you can make identity thieves' jobs much more difficult. You can also help fight identity theft by educating your friends, family, and members of your community. The FTC has prepared a collection of easy-to-use materials to enable anyone regardless of existing knowledge about identity theft to inform others about this serious crime. To learn more, click here.

What are the steps I should take if I'm a victim of identity theft?

If you are a victim of identity theft, take the following four steps as soon as possible, and keep a record with the details of your conversations and copies of all correspondence.

1. Place a fraud alert on your credit reports, and review your credit reports.

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too. If you do not receive a confirmation from a company, you should contact that company directly to place a fraud alert.

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you place the fraud alert in your file, you're entitled to order one free copy of your credit report from each of the three consumer reporting

companies, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports. Once you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information, like your Social Security number, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed. See Correcting Fraudulent Information in Credit Reports to learn how. When you correct your credit report, use an Identity Theft Report with a cover letter explaining your request, to get the fastest and most complete results.

Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

Does a Security Freeze Stop Identity Theft?

With identity theft on a continued advance upward and noted as the number one white collar crime in America today a popular option is for consumers to shut down (lock) access to their credit reports. This makes it nearly impossible for some criminal intent to reek financial havoc on an individuals well being and the process is known as a security freeze or credit lock.

As of the first of November in 2007, all three credit reporting agencies gave consumers in America the ability to limit access to their individual credit reports. Of course unless you are an actual victim of identity theft, the process is not actually free in most states. To put a freeze on your credit report as a simple proactive measure to avoid criminal theft of your information; costs in most states and fees very widely. One would have to go to each of the three credit bureau's web sites for specific instructions and individual state fees. Additionally, to implement a freeze completely, the process to freeze your credit report has to be done at each agency: all of whom have various methodologies.

A credit freeze does provide substantial identity theft protection however, it is not without loopholes. It can not stop non-credit-related forms of ID theft, such as the creation of a duplicate driver's license or criminal identity theft (when a suspect gives your name to police when booked for a crime). It also won't stop an illegal immigrant or undocumented worker from using your Social Security Number to obtain employment.

Additionally, it won't stop every company from accessing your credit report. New creditors are largely blocked out, yet still existing lenders i.e. your current credit card company (for example) can still view your report and offer you new credit cards. Also, collection agencies acting on behalf of these companies with your current account(s), state or local agencies that includes law

enforcement, child support agencies, trial courts pursuant to a warrant or subpoena, credit monitoring companies and companies that sell credit reports to consumers are still viable accesses.

It also won't stop those pre-approved credit card offers. The bureaus can still give your name and address to credit card companies. Of course, you can stop those mailings by making a simple call to 1-888-5OPTOUT or by visiting http://optoutprescreen.com.

Putting a freeze in place requires some time consuming paperwork like sending certified letters. And it means keeping track of freezing and subsequent lifts of an imposed freeze. As stated earlier, it does no good to freeze one or two reports. If you want real identity theft protection, you'll have to go through the motion and requirements to freeze all three credit agencies. If you want to get a new credit card, you'll have to lift at least one agencies credit report freeze. To undertake a major investment such as buying a new home, you'll most likely have to lift all three credit agency freezes then; turn around and make sure they are frozen again to safeguard your identity after the purchase is closed.

Gail Hillebrand, Consumers Union credit bureau expert, compares freeze fees to paying for insurance and stated "If you are the person in the household who will have to unravel an identity theft after it happens, then you probably think $10 a pop is a good deal." Additionally, "Consumers who are already paying for $10-per-month credit monitoring services should cancel and pay for security freezes instead." she concluded.

Despite the time consumption and varying requirements, a credit freeze is likely the most optimal thing you can do to stop most identity theft before it lurks its aggravating head. Think of it like the sign you place in your window that announces the premise is protected by an alarm system. Yes, the home can still be broken into but, many thieves who see an alarm would move on to another target. Identity thieves who come upon a security freeze when trying to get services in your name such as credit cards or loans are just as likely to move onto the next Social Security number. Only the individual can decide what is best for their own circumstances. My only input would be with identity theft on the rampage, some kind of proactive measure is warranted to lesson chances of identity theft.

Resource – Visit www.adultwishfoundations.com/Life_Lock.html to learn more about a proactive identity theft protection service that offers – the best Identity Theft Protection, Reduced Junk Mail, Reduced Credit Card Offers, $1 Million Service Guarantee, Child Protection Program and more for Only $10 per Month.

2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers.

If the identity thief has made charges or debits on your accounts, or has fraudulently opened accounts, ask the company for the forms to dispute those transactions:

- For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. If the company doesn't have special forms, use the sample letter to dispute the fraudulent charges or debits. In either case, write to the company at the address given for "billing inquiries," NOT the address for sending your payments.
- For new unauthorized accounts, you can either file a dispute directly with the company or file a report with the police and provide a copy, called an "Identity Theft Report," to the company.
    - If you want to file a dispute directly with the company, and do not want to file a report with the police, ask if the company accepts the FTC's ID Theft Affidavit (PDF, 56 KB). If it does not, ask the representative to send you the company's fraud dispute forms.
    - However, filing a report with the police and then providing the company with an Identity Theft Report will give you greater protection. For example, if the company has already reported these unauthorized accounts or debts on your credit report, an Identity Theft Report will require them to stop reporting that fraudulent information. Use the cover letter to explain to the company the rights you have by using the Identity Theft Report. More information about getting and using an Identity Theft Report can be found here.

Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

3. File a complaint with the Federal Trade Commission.

You can file a complaint with the FTC using the online complaint form; or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Be sure to call the Hotline to update your complaint if you have any additional information or problems.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

Additionally, you can provide a printed copy of your online Complaint form to the police to incorporate into their police report. The printed FTC ID Theft Complaint, in conjunction with the police report, can constitute an Identity Theft Report and entitle you to certain protections. This Identity Theft Report can be used to (1) permanently block fraudulent information from appearing on your credit report; (2) ensure that debts do not reappear on your credit report; (3) prevent a company from continuing to collect debts that result from identity theft; and (4) place an extended fraud alert on your credit report.

4. File a report with your local police or the police in the community where the identity theft took place.

Call your local police department and tell them that you want to file a report about your identity theft. Ask them if you can file the report in person. If you cannot, ask if you can file a report over the Internet or telephone. See below for information about Automated Reports.
If the police are reluctant to take your report, ask to file a "Miscellaneous Incident" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.

When you go to your local police department to file your report, bring a printed copy of your FTC ID Theft Complaint form, your cover letter, and your supporting documentation. The cover letter explains why a police report and an ID Theft Complaint are so important to victims.

Ask the officer to attach or incorporate the ID Theft Complaint into their police report. Tell them that you need a copy of the Identity Theft Report (the police report with your ID Theft Complaint attached or incorporated)to dispute the

fraudulent accounts and debts created by the identity thief. (In some jurisdictions the officer will not be able to give you a copy of the official police report, but should be able to sign your Complaint and write the police report number in the "Law Enforcement Report" section.)

Chapter Eight

The Identity Theft Resource Center

This organization contains a wealth of information and fact sheets that are a great resource and time saver for those of you who are a victim of identity theft. To save time in your reporting and agency letters needed to correct the impact of identity theft – use their prewritten letter formats.

Fact Sheet 100 - Financial Identity Theft - The Beginning Steps
http://www.idtheftcenter.org/artman2/publish/v_fact_sheets/index.shtml
Posted in: Fact Sheets, Identity Theft News
By Identity Theft Resource Center
May 2, 2007 - 12:55:25

Fact Sheet 100
FINANCIAL IDENTITY THEFT – THE BEGINNING STEPS

Other guides on the ITRC website will address other aspects of this crime including Lost and Stolen Wallets, Dealing with Collection Agencies, Check Fraud/Theft, Family Identity Theft, The Evidence Trail, Medical Identity Theft, Enhancing Communications with Law Enforcement, and Financial Identity Theft: The More Complex Cases.

WHAT YOU NEED TO KNOW BEFORE YOU START:

Your rights under the law:

1. To have a police report taken. Many states do not have a specific law about this but if you are persistent you should be able to get a report in the jurisdiction where you live. With a police report you are entitled to:

A 7-year fraud alert
A credit freeze in the states that have adopted this procedure into law
Have inaccurate or fraudulent information blocked from your credit report
Receive a copy of all application and transaction records on accounts opened fraudulently in your name (FCRA Section 609e)

2. Have the account removed from your credit report once you have provided evidence the account is fraudulent. This includes any collection actions or inquiries.

Organizing Your Case: See ITRC Fact Sheet 106 for detailed information

1. Keep a detailed log in a spiral or composition book of all phone calls you receive or make. Including the names or people, their title, phone numbers, company name, and what was said during the conversation. Keep loose papers in a notebook or an accordion folder.

2. Send all correspondence to collection agencies, credit issuers and other entities via certified mail, return receipt requested to confirm the letter has been delivered. Keep the postcard that you receive for evidence if necessary.

3. Confirm all conversations and agreements in writing. The person who made an oral agreement with you may not be at that company two months later.

4. Keep all receipts of expenses and copied of correspondence.

Working with the Right People:

The biggest waste of time is talking with the wrong people. Keep in mind that whenever possible you want to speak with someone on the investigative or fraud side of a company or governmental agency.

Collection agencies and credit issuers: Customer service helps with billing. You want to speak with a fraud investigator or the legal department of a small company.

The Social Security Administration does not work on financial identity theft cases. SSA only gets involved through their Office of Inspector General if there is benefit fraud or theft of benefit checks.
Law enforcement: Talk with your local police department or the department where the crime is occurring. The Secret Service and FBI only get involved upon the request of local law enforcement or the U.S. Attorney General's Office. Typically these are large money or multiple victim cases or cases involving cyber crime.

When mail theft or fraud is an issue, speak only with the Postal Inspector's Office, not a post office manager.

When speaking to a Department of Motor Vehicles, ask for a fraud investigator.

TERMS you should know:

FCRA – Fair Credit Reporting Act
FACTA – Fair and Accurate Credit Transaction Act
FDCPA – Fair Debt Collections Practices Act: you can get a copy of this at www.ftc.gov

SSN – Social Security Number

CRAs – These are the 3 major Credit Reporting Agencies – Equifax, Experian, and TransUnion
Fraud Alert – Federal law instructs credit issuers to contact you prior to approving an application. However, it is not widely enforced and not 100% reliable. ITRC has found fraud alerts to be about 65-70% effective. They don't affect your credit score but might slow down the credit issuing process for a thief! (see ITRC-Debix message)

Security or Credit Freeze – With a freeze, a company may not look at your credit report for the purposes of establishing new lines of credit. Companies you already have an existing relationship with (example: a credit card, loan or utility service) may view your reports but only to review your credit-worthiness. Placing a freeze is a strong step to take and will affect your ability to get instant credit since it can take up to 3 days to thaw a report. However, it also locks out thieves, and that is the purpose. In those states with freezes, most laws state that victims with a police report get this service for free. Some states also allow the consumer to buy a freeze. You may thaw your freeze anytime you wish to apply for credit but you will need to plan ahead. See Fact Sheet 124 for more information or our State & Local Resources to see if your state has a freeze program.

Passwords – Your mother's maiden name should never be used as a password or a word that is easily known to you such as a pet's name. Use an unusual or made-up word such as "banapple." Place passwords on all bank accounts and credit cards as a proactive prevention action against account takeover.

FTC – Federal Trade Commission: the governmental agency that oversees identity theft issues. All victims should report their case when they have time to 877-IDTHEFT or to the website: www.consumer.gov/idtheft . The information the FTC collects is vital statistical information and they have a booklet that will also help guide you.

EPTA – Electronic Transfer Act: provides consumer protection for all transactions using a debit card or electronic means to debit or credit an account. It also limits a consumer's liability for unauthorized electronic fund transfers.

STEP ONE – Assess the Damage and Beginning Recovery Steps

1. Stolen credit cards, checks, ATM or debit cards – Contact the financial institution immediately and close the affected accounts. Put passwords on the new accounts. If you never made a copy of the card, you should be able to find a 24/7 phone number on the back of a billing or bank account statement.

2. Account Takeover – If a bank, credit card or debit account has been taken over by another person (charges you didn't make appear on your monthly statement), close the account and open a new one. In most cases you need to notify the company (bank or credit card issuer) within 30 days, so act quickly. It is vital to check statement monthly as few financial institutions allow a "grace" period longer than the contractual agreement (on the back of your monthly statement). Add a password for protection. If checks are involved see Fact Sheet 126 for details. A password on the account will also prevent a thief from changing the billing address or adding a name to the account.

3. Stolen-Lost Wallets – If your wallet has been taken follow the steps in Fact Sheet 104

4. If your Social Security Number has been taken, order your credit reports from all three CRAs.

The best way to evaluate how bad your case might be is to examine your credit reports. You may call the CRAs 24 hours a day, 7 days a week. At this time, English is the only language being used.
When ordering your credit reports, you will have an opportunity to place a FRAUD ALERT (see Terms to Know). The initial fraud alert will only last for 90 days. (see ITRC-Debix message). It is renewable, using the same phone number and procedure you used to place your first fraud alert. It may be extended to 7 years when you write the agency and send a copy of your police report verifying you as an identity theft victim. A fraud alert will not affect your credit score.

Please understand, you will NOT be speaking with a person. These are automated systems and it is safe to give them your Social Security Number. You will be asked a number of questions to confirm you are you. This is for your security and to ensure they don't send out a credit report to the wrong person. You will have access to a fraud assistance advisor once you receive your reports in the mail.

While the first credit reporting agency you call will state that they will contact the other two agencies for you, ITRC recommends you empower yourself and make sure the job is done by calling all three agencies. These are separate companies and they may have different information about you causing one of them to not send a report to you.

You may also ask that your entire SSN is not on the report mailed to you, a good safety measure. Be sure that you have a locked mailbox in which you receive mail – a good tip for everyone.

The primary contact numbers for the CRAs are:

Equifax: Call (800) 525-6285. TDD: (800) 255-0056

TransUnion: Call (800) 680-7289. TDD: (877) 553-7803. Fraud victims can also email fvad@transunion.com but we recommend that you do not send Social Security numbers via email if avoidable.

Experian: Call (888) 397-3742
5. Don't rush into taking a short-cut and buying a "tri-report" (three-in-one report). It could cut you off from fraud investigators at the CRAs. The reports generated by placing a fraud alert will have additional information that is not on a "tri-report."

Credit reports generated by banks and businesses do not contain much of the necessary information to deal with an identity theft issue. Credit reports generated by placing a fraud alert include contact information for companies with open accounts in your name. (See ITRC/Debix message)
When placing the fraud alert, should you hear that the information you have provided does not match the information on file, this is a clear indication that there is a problem. This may mean that a thief has used an address with such frequency that it appears to be your primary address. In that case, follow the directions given and mail your request (with the requested documents) to the address given, which may vary from state to state.

During the time the fraud alert is in place, if there is an inquiry into your credit status, you should be notified by a phone call from the company making an inquiry to confirm with you that you really requested the new line of credit.

6. Review Your Credit Report Carefully:

See Fact Sheet 128 How to Read Your Credit Report for more detail on reading your credit reports.

Credit reports are divided into five major sections. These sections may not be in the same order as listed below.

The header: This is where you will find your information such as name, date of birth, address, Social Security Number and spousal information. There may be information about your yearly income or employer.

Section 1: These are the accounts that you have open or have had opened during the last seven years. You will need to verify that it is an account that belongs to you. These are cases where the name of the company will not be

familiar. You may need to verify the account by comparing the account number to the number on your credit cards or billing statements. Some credit reports separate this section into "Accounts in Good Standing," and "Accounts that Negatively Affect Your Report."

Section 2: This is the section where inquiries are logged. Inquiries come in several different versions. One is that the company making the inquiry has an application in their possession and wish to verify your worthiness for credit. The other inquiry is by companies that you currently have a financial relationship with and it serves as an account review.

Section 3: This section will display lists of companies that have acquired your information so that they can offer you a pre-approved credit card solicitation.

Section 4: Will display a list of previous addresses where you have lived (if not in the header section).

Section 5: Consumer alert information. This is where information about fraud alerts and other information from the consumer are placed.

STEP TWO: Continuing the Recovery Process

1. Contact the Police in the jurisdiction where you live and file a Police Report. You will need to obtain a physical copy of this police report, not just a case number. This is a critical document required to clear your name.

2. Contact all credit issuers, utility companies and collection agencies that have opened a fraudulent account. Speak only to a FRAUD INVESTIGATOR. Then:

Request to close the account(s)
Request the company mail you a fraud alert or an address to send either our Letter Form 100 - 1 or the FTC affidavit (www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf) along with your police report. Always mail out certified with return receipt. If the company does not request document information from you, then they are most likely not clearing the account.
Inform then that they may not sell, share, exchange, give away, donate, and/or trade this account to any other entity for the purposes of collection while it is under investigation.

3. Get Application and Transaction Records – FCRA section 609e requires companies to send you any documents they have. You will need to send an affidavit and a police report to receive copies of transaction and application records. A copy may also be sent to a designated police department. These

documents may contain valuable evidence to point to the thief or help you to clear your name. The credit issuers must send you this information within 20 days (FCRA/FACTA). This demand is already part of Letter Form 100-1. Highlight it if you wish.

4. Once you get the information from the credit issuers, contact the investigating law enforcement agency and provide the information to them.

5. Contact the 3 CRAs using the form they provide for "correction of errors." The Fair Credit Reporting Act (FCRA) says they must remove the information unless credit issuers prove it is a true account. Ultimately the credit issuer must be the one to remove fraudulent accounts from your credit report permanently. The credit issuers also must correct any erroneous information including addresses, phone numbers, birthdates and other information falsely provided by the thief. (see ITRC/Debix message)

6. Get Letters of Clearance from the credit issuers. Keep these for at least 10 years.

7. Check your credit reports and make sure all corrections have been made.

8. If your state has a credit freeze law – look carefully at that option. The steps to take are in Fact Sheet 124 Credit Freeze and Fraud Alerts . This is a strong step to take and will affect your ability to get instant credit because it can take up to 3 days to thaw a report. In many ways this is the only truly proactive step you can take to stop a thief.

STEP THREE: COLLECTION AGENCIES

ITRC has written an entire guide for this activity. See Fact Sheet 116 Collection Agencies and Identity Theft for complete details.

ADDITIONAL RESOURCES:

See Fact Sheet 108 Overcoming the Emotional Impact about the Emotional Impact of this crime. Please note that the identity theft recovery process may take time. It will not be resolved overnight and you must be mentally prepared to take the necessary time to clear it up. Find a healthy stress reduces and build a support team to help you during this period of your life.

The FTC has a publication entitled "Take Charge." You can get a copy mailed to you or download this document from
www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm . You may call them at
877-ID-THEFT or review their website: www.consumer.gov/idtheft

www.identitytheft.org – This resource material was written by an attorney and identity theft expert, Mari Frank. Please remember to indicate that the Identity Theft Resource Center referred you.

To report fraudulent use of your checks:
Chexsystems: (800) 428-9623
Certigy/CPRS: (800) 437-5120
International Check Services (ICS): (800) 526-5380
SCAN: (800) 262-7771
TeleCheck: (800) 710-9898
FBI/NW3C Internet Fraud Complaint Center: www.ic3.gov
California Office of Privacy Protection, (Dept. of Consumer Affairs), (866) 785-9663. Web: www.privacy.ca.gov
Florida AG ID Theft Hotline: www.myfloridalegal.com/identitytheft or 866-966-7226

State and Local Resources and Laws

Sample Letters:

Letter Form 100-1 Initial Victim of Identity Theft Statement and Fraudulent Account Information Request to Credit Issuers or Merchants (Listed at Chapter Nine)

Letter Form 100-2 Confirmation of Conversation - Letter of Clearance

Letter Form 100-3 To Credit Issuers: Requesting a Fraudulent Inquiry to be Removed

Letter Form 124D To the Credit Reporting Agencies: Request the Removal of a Fraudulent Inquiry

---

Chapter Nine

Posted in: Letter Templates
By Identity Theft Resource Center
May 9, 2007 - 2:41:39 PM

INITIAL VICTIM OF IDENTITY THEFT STATEMENT AND
FRAUDULENT ACCOUNT INFORMATION REQUEST
Credit Issuers or Merchants

Date:_____
Sent certified, return receipt mail: Number _____

TO : [Credit Issuer] FAX

ACCOUNT NO. REFERENCE NO.

FROM: [Your Name]

I have learned that an unauthorized account has been opened with your company or bank. I did not open this account and have not given permission to anyone else to open this account for me. I have not benefited by this account. You shall consider this account to be fraudulent and a case of identity theft.

Below is my identifying information. I have filed a report with my local police department. Under CA (PC 530.8) and WA law, all lenders and credit issuers must provide documentation regarding all fraudulent accounts opened in another's identity and do so within ten days. The Cantwell-Enzi amendment to the nationally approved FACTA (effective June 2, 2004) will require compliance with this request within 30 days.

Further, credit issuers must provide that documentation and information to a police agency designated by the impersonated party. I am designating the below named detective(s)/prosecutors as additional recipients of all account information and documents:

Application Records or screen prints of Internet/phone applications
Statements, Billing and Payment Records
Transaction Records/Charge Slips
Log of outgoing calls if a cell phone account or telephone utility
Investigator's Summary
Delivery addresses
Any other documents associated with the account

All records of phone numbers used to activate the account or to access the account
Additionally, I hereby request you immediately start an investigation, and remove any entries of this account, the application or inquiry records and collection notices from my credit report at once. I also wish to speak with a fraud investigator within 30 days about the status of this case. Once resolved, I expect a letter of clearance to be sent to me within 10 days.

Do not sell, distribute, trade, exchange, share, donate, giveaway and/or transfer information about this fraudulent account with any other entity except with the designated law enforcement agencies and prosecutors involved in this case.

Please notify any collection agencies that you may have sent this account to. Please do not assign this account to another collection agency. So far these criminals have stolen approximately $_____ in checks or credit charges in my name. We suspect there will be more until they are caught.

Be advised that reporting these items to the credit bureaus as collection items or continuing to pursue these debts from me would be considered a violation of the state and federal level Fair Debt Collection Practices Act and the Fair Credit Reporting Act.

Victim Information

1. My full legal name is:_____

(If different from above) When the events described in this affidavit took place, I was known as: _____

2. My birth date is (day/month/year): _____

3. My Social Security number is_____

4. My driver's license or identification card number is: State_____ #_____

5. My current address is:
_____

City: _____ State:_____Zip Code:_____

6. I have lived at this address since
_____(month/year)

7. (If different from above) When the events described in this affidavit took place, my address was:

_____

City: _____ State:_____Zip Code:_____

8. I lived at that address from _____ until _____(month/year)

9. My daytime telephone number is (____)_____
Cell (____) _____

10. My evening telephone number is (____)_____

11. My e-mail address is _____

How the Fraud Occurred (Check all that apply):

___ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

___ I did not receive any benefit, money, goods, or services as a result of the events described in this report.

___ My identification documents (ie., credit cards; birth certificate; driver's license; Social Security card, etc.) ☐ were stolen ☐ were lost on or about _____(day/month/year)

___ I don't know who the imposter is at this time or how this happened.

___ I have proof that the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to obtain money, credit, loans, goods, or services without my knowledge or authorization: (only fill out if you are certain)

_____ _____

Name (if known) Name (if known)

_____ _____

Address (if known) Address (if known)

_____

_____

Phone number(s) (if known) Phone number(s) (if known)

_____

_____

additional information (e.g. relationship) additional information (if known)

A report has been made with the following police/sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that by checking here _____. Instead of a police report I filed an official affidavit with the following agency _____ (case #_____)

Name of agency:

_____

Case

#_____

Name of investigator if known:

_____

Contact information for law enforcement: (address/phone)_____

_____

Signature of victim: _____ Date

_____

I declare under penalty of perjury that this declaration is true and correct to the best of my knowledge. Knowingly submitting false information on this affidavit could subject me to criminal prosecution for perjury.

Have one witness (non-relative) sign below that you completed and signed this declaration.)

Witness:

_____

_____

(signature) (printed name)

_____

_____

(date) (telephone number)

List of enclosed documents:

Chapter Ten

What is an Identity Theft Report?

An Identity Theft Report is a police report with more than the usual amount of detail. The Identity Theft Report includes enough detail about the crime for the credit reporting companies and the businesses involved to verify that you are a victim—and to know which accounts and inaccurate information came from identity theft. Normal police reports often don't have many details about the accounts that were opened or misused by identity thieves.

The printed copy of your ID Theft Complaint Form can provide additional details for the police report. The police are not legally required to use the FTC's ID Theft Complaint Form as part of their report. Your police department may have another way to incorporate the details of your crime. In these cases, the police report by itself may serve as an Identity Theft Report.
When you file your Identity Theft Report, the credit reporting companies will permanently block fraudulent information from appearing on your credit report. Filing an Identity Theft Report with the credit reporting companies or with the companies where the thief used your information should ensure that these debts do not reappear on your credit report. An Identity Theft Report can prevent a company from continuing to try to collect debts that result from identity theft, or sell those debts to others for collection. It also allows you to place an extended fraud alert on your credit report. The credit reporting companies may decline your Identity Theft Report if it does not contain enough detail for them to verify that you are a victim of identity theft. In that case, the credit reporting companies have certain timeframes for responding to your Identity Theft Report with requests for additional information.

Creating and using an Identity Theft Report may require two steps:

Step One begins with filing your report with a local, state, or federal law enforcement agency. These agencies may include your local police department, your State Attorney General, the FBI, the U.S. Secret Service, the FTC, or the U.S. Postal Inspection Service. Some state laws require local police departments to take reports, but there is no law requiring federal agencies to take a report.

In your report, you should give as much information as you can about the crime, including anything you know about the dates of the identity theft, the fraudulent accounts opened and the alleged identity thief. It may help you give the necessary level of detail if you file an online complaint with the FTC, and then ask your local police department to incorporate a copy of the printed ID Theft Complaint into its police report.

Step Two begins when you send the businesses involved and the credit reporting companies a copy of your Identity Theft Report, which you should do by certified mail, return receipt requested. The companies may ask you to give them more information or documentation to help them verify your identity theft. They have to make their request within 15 days of receiving your Identity Theft Report. The credit reporting company or business then has 15 more days to work with you to make sure your Identity Theft Report contains everything they need. They are also entitled to five days to review any information you give them. For example, if you give them information 11 days after they request it, they have until day 16 to make a final decision.

How do I get an Identity Theft Report?
The officer taking your police report can attach or incorporate your ID Theft Complaint into their police report to add more detail. Ask the officer to give you a copy of the official police report that incorporates or attaches your ID Theft Complaint. In some places the officer will not be able to give you a copy of the official police report, but should be able to sign a copy of your ID Theft Complaint and write the police report number in the "Law Enforcement Report" section. Be sure to keep a copy of the police report number.

The police are not legally required to use the FTC's ID Theft Complaint Form as part of their report. Your police department may have another way to include all the details of your identity theft information in their police report. In these cases, the police report by itself may serve as an Identity Theft Report.

Because the detailed Identity Theft Report is required for you to get many important protections, you may wish to use the Law Enforcement Cover Letter to explain to the police department how important it is for you to get a police report – as well as the legal protections that a detailed Identity Theft Report gives you.

How do I submit my Identity Theft Report to the credit reporting companies, or to businesses where the thief used my information?
When you send a copy of your Identity Theft Report to the fraud departments of the three major credit reporting companies, include a copy of the credit reporting company cover letter, along with copies of your supporting documentation. Send your information by certified mail with return receipt requested. The mailing addresses for sending Identity Theft Reports to the three major credit reporting companies are on the cover letter.

When writing to the fraud departments of each of the companies where the identity thief has committed fraud using your personal information, include copies of the Identity Theft Report, your supporting documentation, and the appropriate cover letter: for fraud on your existing accounts, or for fraud on

new accounts. Always send this information by certified mail, with a return receipt requested.

The credit reporting companies have certain timeframes for responding to your Identity Theft Report with requests for additional information.

What do I do if the police only take reports about identity theft over the Internet or telephone?

The FTC ID Theft Complaint has a special section for police reports that are not filed face-to-face, to help you use it to supplement an automated police report. If you file a police report online or over the phone, complete the "Automated Report Information" block of the ID Theft Complaint. Attach a copy of any filing confirmation received from the police.

If you have a choice, however, you should file your police report in person and not use an automated report. It is more difficult for the consumer reporting company and information provider to verify the information in an automated report, and they will likely require additional information and/or documentation.

What do I do if the local police won't take a report?

There are efforts at the federal, state and local level to ensure that local law enforcement agencies understand identity theft, its impact on victims, and the importance of taking a police report. However, we still hear that some departments are not taking reports. The following tips may help you to get a report if you're having difficulties:

- Provide the officer with a copy of the Law Enforcement Cover Letter that explains why the police report and the Identity Theft Report are so important to both victims and industry.
- Furnish as much documentation as you can to prove your case. Debt collection letters, credit reports, a copy of your printed ID Theft Complaint, and other evidence of fraudulent activity can help demonstrate the legitimacy of your case. Provide the police a copy of "Remedying the Effects of Identity Theft," which shows that police reports are necessary to secure your rights.
- Be persistent if local authorities tell you that they can't take a report. Stress the importance of a police report; many creditors require one to resolve your dispute. Remind them that consumer reporting companies will automatically block the fraudulent accounts and bad debts from appearing on your credit report, but only if you can give them a copy of the police report. In addition, a police report may be needed to obtain the fraudulent application and other records the company has.

- If you're told that identity theft is not a crime under your state law, ask to file a Miscellaneous Incident Report instead.
- If you can't get the local police to take a report, try your county police. If that doesn't work, try your state police.

Some states require the police to take reports for identity theft. Check with the office of your State Attorney General, which can be found at www.naag.org, to find out if your state has this law.

How do I prove that I'm an identity theft victim?

Applications or other transaction records related to the theft of your identity may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement. By law, companies must give you a copy of the application or other business transaction records relating to your identity theft if you submit your request in writing, accompanied by a police report. Read more about getting information from businesses, and use this model letter to request this information.

Chapter Eleven

Comparison of ID Theft Protection Services
NextAdvisor.com is
The trusted, independent source for
Comparing the most valuable new services for Avoiding
ID Theft and other consumer services

They are located at
http://www.nextadvisor.com/identity_theft_protection_services/compare.php
They Advise

Identity Theft Protection

Just being careful isn't enough to prevent or detect identity theft, the fastest growing crime in the U.S. with over 9 million victims each year. If you are serious about preventing identity theft, sign up for one of our recommended identity theft protection services below. Not only will they set fraud alerts on your credit files so that any business opening an account in your name must contact you to confirm your identity, but they'll help you cut down on junk mail and give you copies of all three of your credit reports, too. If you don't want to be contacted every time you open a new credit account or also want to keep close tabs on your credit report and score, then sign up for an identity theft detection service to ensure you catch any theft before it hurts you. Or get Identity Guard Total Protection, which provides both prevention and detection services. Have more questions about identity theft and which service might be best for you? Visit their individual sites.

But you must first know this before proceeding to reviews…

How does NextAdvisor.com come up with its reviews?

We thoroughly test and research all the services in the category. We order each and every service ourselves and test out every feature available. We contact customer service and cancel and reorder each service to make sure that process works as well. After our initial tests, we continue to use all the services and update our reviews as situations change. We also monitor the providers' sites for any service changes or specials. In addition, we research each provider by reading all news and ordering and reading third-party research reports. We only include providers on our site that we believe offer a good value proposition. If there is a provider you know of that is not on our site, you can be fairly certain we did not rate that provider good enough to include in our comparison. If you think we are missing a quality provider or have any other suggestions or comments, please let us know.

And that……

Service, Price, Type Credit Reports Delivered, Fraud Monitoring, Mail List Removal, ID Theft Insurance and Overall Rating all contribute to your best Bottom Line service need.

++

LifeLock Review

LifeLock is a great "preventive" identity theft protection service at a great price. As a special offer for visitors to NextAdvisor.com, you can now get 30 days free AND $21 off the price of the service. You must click the link from our site to get this special promotion. "Preventive" services employ tools like setting fraud alerts on your credit file with all 3 bureaus, which means that lenders must call or write you for verification before they can issue new credit. Since most identity theft occurs when thieves use your personal information to open new credit accounts (credit cards, bank accounts, phone accounts, etc.), fraud alerts prevent identity theft by stopping the fraudulent accounts from being opened in the first place. (There are also what we call "detection" services that monitor any changes to your credit report and are a great way to catch identity theft in its early stages and before damage is done. They do not, however, help prevent ID theft.) The CEO of LifeLock stands behind his product so firmly that he will gladly hand out his social security number on the website. While it is a great testimony for his service, we don't recommend you try it at home! LifeLock is a preventive identity theft protection service - their sole purpose is identity protection and recovery for you and your family. (They have reduced-price plans for children as well.) LifeLock works by installing and maintaining fraud alerts on your data with the 3 major credit bureaus. What this does is force a bank or other credit issuer to contact you personally before any new account can be opened in your name. Fraud alerts are a method of extra protection and they do not hurt your credit or score in any way. They also send you a 3-bureau credit report annually, at the time of and the anniversary of your signup with the company. LifeLock also stops pre-approved credit offers and junk mail with your name on it from circulating, thereby reducing your chance of having your identity stolen. LifeLock recently added a new feature that is included in their service called WalletLock, which we think is excellent. If your wallet is ever stolen, you just call LifeLock and speak to a WalletLock specialist, who will contact each credit card, bank or document issuing company, cancel your affected accounts and complete the paperwork and steps necessary to replace your lost documents, including your credit/debit cards, driver's license, social security card, insurance cards, checkbook - even travelers checks - at no additional cost. LifeLock's guarantee is one of the best out of any of the top companies for identity protection, and it is clearly stated on their web site. They offer $1 million towards reimbursement, lawyers' fees, and clearing your name if your identity is ever stolen. While this guarantee is great, direct monetary losses from identity theft

are almost always much smaller since you are not legally responsible for paying any fraudulent debt a thief accumulated. The real cost of identity theft is the loss of ability to get credit for an extended period of time, the time and effort it takes to restore your good name, and many other adverse consequences that can even include mistaken incarceration.

Signing up was quick for us, and after 2 screens the company clearly labeled what we could expect from our account over the next 12 months or so. (For example, within 2 weeks we will be notified about the fraud alerts from the bureaus, within 2 months our junk mail will be drastically reduced, and every 90 days our fraud alerts will be reissued.) Upon contacting customer service by phone with some questions, we didn't have to wait more than a moment for someone to pick up the phone, and they are available 24/7 for any questions or problems. Unlike other services, LifeLock offers no login services at their site - you will have to call their number for any adjustments to your account. While this may be a bit inconvenient, it makes their system completely hacker-proof, as they claim that very few people at LifeLock ever get near customer data. LifeLock offers both monthly and yearly payment options for individuals and families, as well as a Business-class service. Overall, LifeLock is a great service to help you prevent identity theft. Relative to TrustedID, another top service, it lacks the credit card protection technology and the credit freeze option, but it does add the junk mail unsubscribe (TrustedID has preapproved credit card offer unsubscribe but not general junk mail unsubscribe) although this is certainly not 100% effective and you can easily do it yourself. LifeLock also has more generous customer service hours.

LifeLock
Go To Site
Read Review

$9.00/mo. or $99.00/yr.; 30 days free Protection - sets and renews fraud alerts 1 3-bureau credit report each year No Preapproved credit and general junk mail $1,000,000 Best overall value in identity theft protection

++

Identity Guard Level 4 - Total Protection Review

Identity Guard Total Protection is by far the most comprehensive identity theft product and really lives up to its "Total Protection" moniker. It's the only service that offers both identity theft protection and detection. Plus, it has the most extensive fraud monitoring we've found and offers them all at a great price, just $14.99 per month plus one month free (this special deal is only available through our site). Identity theft detection services help to detect that

you have become a victim of identity theft by monitoring your credit file at all 3 credit bureaus. Identity theft protection services aim to stop identity theft from happening in the first place by setting fraud alerts on your credit file at all 3 credit bureaus, meaning a lender must take the extra step of calling you to verify your identity before processing a new application from you. If you are very concerned about identity theft or at least mildly concerned and also want to keep tabs on your credit and credit scores, we recommend you get both types of services, and Identity Guard Total Protection is the only service that offers both in one package. Identity Guard Total Protection is not only a great fraud prevention service, but is also a credit monitoring service on steroids. Like many credit monitoring services, it completes daily scans of all 3 of your credit files and notifies you of any changes. It also gives you all 3 of your credit reports and all 3 of your credit scores every quarter. Identity Guard goes far beyond other credit monitoring services in detecting identity theft by also monitoring public records for any changes in your name, scanning for application or social security fraud, and monitoring the internet's black market for any use of your credit cards. If anything is found, they will alert you by e-mail immediately. Additionally, they provide card registration services to help you in case your wallet gets lost or stolen. Finally, if you are not all that concerned about identity theft or don't want to have to be contacted when you apply for new credit, you have the option to turn fraud alerts off with Identity Guard or never turn them on and still enjoy all the other great services they offer. The only thing Identity Guard Total Protection doesn't do is remove you from junk mail lists, but you can do that yourself for free and it more than makes up for it with all its other great services.

The signup process is relatively quick - you will go through a short series of screens asking you for information, including payment information. To verify your identity, you will be asked for your social security number, date of birth, and the answers to 5 multiple-choice questions of information in your file. By default, the credit reports and alerts are available online and through e-mail. If you want hard copies mailed to you however, you can call their customer service number and get them at no extra charge. Your subscription includes access to a very useful credit analyzer. You can try out different scenarios, such as paying off your credit card by a certain amount or opening up a new loan, to see how your credit score will be affected. If you are monitoring your credit, this analyzer can help you to make the best choices to raise your credit score. In the event of a credit card theft, you can report the incident to Identity Guard and they will handle all the details for you, including reporting the cards as stolen and getting new cards issued to you. Identity Guard offers generous customer service phone hours (8am-11pm M-F and 9a-6p Sat) as well as postal mail and e-mail contact methods. When we tried contacting them, a customer service representative answered almost immediately, and was able to provide useful advice about the service. Reporting for lost or stolen cards can be done on the phone or through your account, 24 hours a day, 7

days a week. If you like this service but are looking for a cheaper alternative, you may want to try another Identity Guard service, Extra Caution, that is just $11.99 per month ($3 per month cheaper)plus one month free when ordered through this link. It has all the same services as Total Protection except for public record reporting and scanning for application and social security fraud. For those really serious about identity theft protection, though, Total Protection is the best service you will find.

$14.99/mo. & 1 month free protection & Detection - 3-bureau credit monitoring & sets and renews fraud alerts 3-in 1 credit reports and Scores from all 3 bureaus Credit cards, Public records, social security, applications (cell phones, loans, etc.) No $20,000 Most complete service - only one offering protection & detection; extensive fraud monitoring

++

TrustedID Review

TrustedID starts with setting fraud alerts (they call this "Lender Doublecheck") at all 3 bureaus as soon as you sign up. They have developed an automated tool to set these alerts, so they happen essentially as soon as you sign up. The downside to any preventive service that sets fraud alerts is that it might delay a credit application process because your identity must be confirmed, but this is a small price to pay to prevent ID theft and it will not hurt your credit or prevent you from getting credit. TrustedID's credit card monitoring service, which monitors your credit cards for any suspcicious activity, also starts the moment you sign up, using the card number you use to pay for your order. Adding additional card numbers to your account is quick and easy. This service monitors the internet's black market for your credit card numbers and immediately alerts you if it finds any of your numbers are being bought or sold. TrustedID's credit offer opt out and identity theft insurance starts the moment you sign up as well. The credit offer opt out immediately prohibits credit card issuers from sending you preapproved credit card offers. Not only do these clog your mailbox and kill trees, but they are also a prime target for identity thieves to steal, gain your personal information and open a credit card account in your name.

TrustedID's ID Theft Insurance covers you for up to $1,000,000 in costs to recover from identity theft. While this is a great benefit, direct monetary losses from identity theft are almost always much smaller since you are not legally

responsible for paying any fraudulent debt a thief accumulated. The real cost of identity theft is the loss of ability to get credit for an extended period of time, the time and effort it takes to restore your good name, and many other adverse consequences that can even include mistaken incarceration. Your free credit reports are mailed to your house, and the address is verified through the credit bureaus before doing so. As part of your account, you are offered a service called CreditLock, which makes your credit report at all 3 bureaus unavailable to everyone without permission. While this may be good for those who never use their credit, or those who are stationed overseas, it does cost $44.95 to lock your credit reports with all 3 bureaus and $39.95 to unlock them - every time! We typically only recommend using this feature if you know you have been the victim of an identity thief. In that situation, it is extremely valuable. TrustedID scored the lowest on customer service however, as their phone hours are only 7:30 am to 4:30 pm (pacific time, and it took me over 6 minutes of hold time do get a representative on the phone. She was helpful once I did get on the phone, and she did mention their phone hours would be expanding soon. Logging in to their system does not offer much information - just the ability to sign up for CreditLock and add card numbers to your watch list. TrustedID's service was activated fastest out of all the services tested - which could be extremely useful to lock down your information if your identity is ever stolen. Overall, TrustedID is a great preventive identity theft solution and an excellent option for those serious about preventing I.D. theft.

$12.95/mo. or $109.95/yr. protection - sets and renews fraud alerts 1 3-bureau credit report each year Credit cards Preapproved credit $1,000,000 Great ID theft protection service; includes credit card fraud monitoring

++

LoudSiren Review

LoudSiren has done a nice job of differentiating themselves from similar services LifeLock and TrustedID by developing an easier system to manage fraud alert inquiries. All three of these identity theft protection services work by setting and renewing fraud alerts on your credit files with the three bureaus, meaning that whenever you (or a potential ID thief) applies for credit, the lender must call you to verify that it is indeed you submitting the application. If the lender cannot reach you, your application will be held up until you are able to speak with them. LoudSiren avoids this problem by creating a new contact number for lenders to call and leave their information. LoudSiren then automatically conatacts you at up to 3 numbers, where you

can approve or disapprove the application through their automated system. If you cannot be reached, you can call back to LoudSiren at any time and approve or disapprove the application at your convenience. In addition to saving time and being more efficient, LoudSiren's system adds extra levels of security because you have a PIN number that you enter to approve every transaction and a recording of your own voice assures you that each call is legitimate.

Other than their automated fraud alert system, LoudSiren is very comparable to LifeLock. Just like LifeLock, you can get a copy of your credit report from each of the three credit bureaus, you can stop getting preapproved credit offers through the mail, and you've got a $1 million insurance policy in case your identity gets stolen. LoudSiren also will automatically put your phone numbers on the national Do Not Call Registry to stop unsolicited telemarketing calls. However, LoudSiren's customer service hours (M-F, 9am-5pm CT) are not as generous as LifeLock's. Overall, though, LoudSiren has added a valuable level of automation to identity theft protection and is an excellent choice for those that will be using their credit often.

$9/mo. or $99/yr. Protection - sets and renews fraud alerts 1 report from all 3 bureaus each year No Preapproved credit; tele- marketing, too $1,000,000 Innovative automated phone system makes managing fraud alerts easy

++

Equifax Gold 3-in-1 Monitoring w/ ScorePower Review

Equifax Credit Watch Gold 3-in-1 Monitoring Plus Score Power is another great identity theft detection service. Designed primarily as a service to monitor your credit reports and scores (it is our top rated service in our credit monitoring reviews), it also works very well in detecting identity theft. As a special promotion for ConsumerCompare.org visitors, you now get a free 30-day trial when you sign up from our site. When you sign up for the free 30 day trial, you also get a free Equifax FICO score and a free 3-Bureau credit report (reports from 3 bureaus laid out side-by-side for easy comparison). Since the FICO score is the score most lenders use to make decisions, this is the best score you can get. Equifax actually gives you an entire Score Power report which not only includes your FICO score but also a FICO Score Simulator that estimates what your score would be if you took certain actions, as well as a full explanation of factors affecting your credit score. Equifax is giving you both the report and score free just for trying their monitoring service for 30 days,

so if you don't like it you can cancel and have paid nothing for your FICO score and 3-Bureau report, which you would have to pay $40 for if you bought it separately. Canceling would defeat the purpose, though, since what is going to detect identity theft is their excellent 3-bureau monitoring service. We think monitoring all three bureaus is very important for both monitoring your credit and protecting against identity theft because sometimes lenders will only report a credit event to one bureau. Equifax constantly monitors all 3 bureaus and sends you an email alert within 24 hours of a change to any one of your 3 credit reports. You can also get an updated Equifax credit report any time you want. At only $14.95 per month after the free 30-day trial, this service is an excellent value. If you're looking for an identity theft detection service and also want to keep tabs on your credit reports and scores, Equifax Credit Watch Gold 3-in-1 Monitoring Plus Score Power is a great solution.

$14.95/mo.; Free 30-day trial Detection - 3 bureau credit monitoring Free 3-bureau credit report and Equifax FICO score No No $20,000 Great combination of credit monitoring and id theft detection

++

What type of identity theft protection is right for me?

"Preventive" identity theft protection services, like TrustedID and LifeLock, are a very strong form of identity theft protection. Both place a fraud alert on all of your credit files (TrustedID allows you the additional and more extreme option of placing a "credit freeze" on your credit files) which means anyone opening a credit account for you must make an extra effort to confirm your identity, which usually means calling you to confirm you opened the account. We recommend this type of service for most people that are concerned about identity theft, but it does come with some drawbacks. Mainly, it makes it a bit harder to open credit accounts as you must first wait to be contacted by the new account grantor, which can sometimes take as long as a few days or longer if the grantor can't connect with you. For those who want to take a less extreme approach or who also want to have the benefit of keeping close tabs on their credit reports and scores, one of the "detection" type of services we recommend is a great approach. These are credit monitoring services that monitor your credit file ("credit monitoring"), as well as the internet black market, for any unusual activity occurring in your name. They also give you regular updates of your credit reports and credit scores. While detection of something means that your information has already fallen into the wrong hands, it almost always occurs before the situation has become a more serious problem and it is not as difficult to deal with. A "detection" service is good for someone who opens credit accounts often but is not overly concerned with identity theft.

What do I do if I think I am a victim of identity theft?

If you are a member of one of our recommended identity theft services, call your service provider immediately and they will help you handle the situation. Similarly, if you are a member of one of our recommended credit monitoring services, call your service and they will help you take care of the situation. If you have not subscribed to one of our recommended services, visit the FTC's site for further instructions.

Appendix 1

What is LifeLocks Job?

The job of LifeLock is to protect your good name. As a consumer, you have rights that allow you to take more control over who uses your identity and how they use it. We do the mechanics, the details if you will, to enforce those rights. And we stand behind our service with our $1,000,000 Service Guarantee. We charge $10 per month to do it.

Some of what LifeLock does, you can do yourself for free. The difference is that the only thing Life Lock thinks about is how to protect your Identity. Think of it this way: all of us can change our own oil, but most of us have it done by specialists. We'd like to think that what we do is more complicated than changing oil, but you get the idea.

Here's What LifeLock Can Do:

First, we ask the credit bureaus to set fraud alerts on your behalf. Usually, this is done through our automated systems and the alerts are set within an hour. From time to time there may be a hitch and we have to do the first one manually, usually because they have a different address on file for you. If this happens, we'll tell you right away and do what needs to be done to get the alerts set. (In case you're wondering, we don't charge anything more for this and our Total Service Guarantee is still in effect from day one.)

Second LifeLock Action, unless your circumstances change and you tell us not to, every 90 days or so we ask the credit bureaus to do it again. You can do this for free if you'd prefer, but we make sure it gets done and that it gets done right. That's where the oil change analogy we were talking about kicks in.

Third LifeLock Action, we request that your name be removed from pre-approved credit card and junk mail lists and we keep making the requests as they expire. Statistics show that this is one of the most common ways that thieves hijack identities. Plus, all that mail is just so irritating. Many of our clients tell us that this alone is worth the price. If you are a do-it-yourselfer, you can do this for free, but why not let us do it for you?

Fourth LifeLock Action, we order your free credit reports on your behalf from the major credit bureaus and they are sent directly to you. We do this every year. You can also do this yourself for free (Pennzoil anyone?).

Fifth LifeLock Action, hassling with lost or stolen wallets is no longer a problem with WalletLock™. If ever your wallet goes missing, just give us a call - anytime, anywhere - and a WalletLock specialist will contact each credit card, bank or document issuing company, cancel your affected accounts and complete the paperwork and steps necessary to replace your lost documents*, including your credit/debit cards, driver's license, social security card, insurance cards, checkbook - even travelers checks - at no additional cost.

Last, but certainly not least LifeLock Action: If your Identity is stolen while you are our client, we're going to do whatever it takes to recover your good name. If you need lawyers, we're going to hire the best we can find. If you need investigators, accountants, case managers, whatever, they're yours. If you lose money as a result of the theft, we're going to give it back to you.

We will do whatever it takes to help you recover your good name and we will spend up to $1,000,000 to do it.

We don't think you will see a guarantee like this anywhere else from any other company. If you do, let us know because we'd like to do business with them. There isn't much fine print in our Guarantee. To see the details, click here.

If you have a reason to think that you will become a victim of Identity Theft, we can help you stop looking over your shoulder, because we've got your back.

*Pictures, cash and other monies are excluded.

LifeLock Frequently Asked Questions:

The following is a list of FAQs about LifeLock, its service and other important facts. As a consumer, it is important for you to fully understand what we provide and how we provide it; it will help you feel comfortable about the services LifeLock provides.

Please take a few moments at your leisure to review the FAQs below.

How big a problem is Identity theft?

According to the Federal Trade Commission, identity theft is the fastest growing crime in America. Roughly 10 million Americans have their personal information stolen and misused in some way every year, costing consumers $5 billion and businesses over $40 billion annually.

What does LifeLock do?

On your behalf, LifeLock requests that fraud alerts be placed on your accounts. By placing these fraud alerts, you are asking that creditors take extra care to identify who you are and to investigate the validity of any pending transaction. LifeLock also requests that your name be removed from pre-approved credit card lists and junk mail lists. In addition, LifeLock annually orders your free credit reports from the three major credit reporting bureaus.

Why do children need protecting?

The identities of children are stolen more often than you think. Criminals know they can use a child's information for years before being identified. By then, the thieves have run up major accounts and ruined credit for that child. LifeLock is just $25 a year for a child age 15 and younger with an adult paying annually.

If a child has a valid credit report, LifeLock will request that the fraud alerts are placed on the child's file. LifeLock also requests that a notation is placed on the report indicating that there should not be any activity on the file because the child is a minor. If a child does not have a credit report, as is usually the case, LifeLock confirms every 90 days that that no credit report exists. In addition, LifeLock prepares a request to the Social Security Administration for a copy of the child's work history to confirm that the child's social security number is not being used fraudulently.

Do I have to give all my credit card numbers to you when I sign up?

No, LifeLock does not prevent anyone from using your existing accounts. However, those accounts would be covered by the guarantee. Through the information you provide, Life Lock will place alerts to help protect against anybody other than yourself opening new lines of credit. LifeLock suggests you place all your account numbers in a secure place if your wallet or purse is stolen. If that occurs, call LifeLock so we can help with contacting the credit card companies to cancel the stolen cards and reissue new ones.

Who will represent me if my identity gets stolen?
In the event that your identity is compromised, LifeLock will hire qualified professionals to assist you in addressing whatever complications may arise.

What happens when I apply for credit?
After a fraud alert has been placed in your credit file, any creditor using that credit file to grant new credit or an extension of credit in your name must contact you by telephone (using the phone number specified in the fraud alert) or take reasonable steps to verify your identity and confirm that the credit application is not the result of identity theft. If someone else is trying to use your identity to get credit, the fraud alert usually stops them cold. We say "usually" because nothing is perfect. That's why we have our Service Guarantee.

Is LifeLock going to call me if someone tries to use my information?
No. LifeLock's system is designed for you to have control, so you will know before we do. The fraud alerts placed on your accounts ask creditors to call you if someone is trying to establish credit in your name.

I have been a victim of identity theft, can you help me?
We can direct you to competent and reputable firms that specialize in identity remediation. Our service can prevent further damage to your identity, however, our Service Guarantee does not cover issues which occurred prior to you becoming our client.

Who needs this protection the most?
Any individual who has a social security number and assets to lose should be concerned with identity theft. While we have heard people say, "I don't have anything for them to take," criminals are better than you at making major purchases with your information.

What makes you different than insurance companies?
First and foremost, LifeLock aims to prevent ID theft. Insurance companies do nothing to prevent anyone from using your personal information. Insurance companies will give you a policy to provide some financial coverage if you become a victim. However, there are also several disclaimers on what is covered and not under these plans.

Who is LifeLock?
LifeLock is a private company headquartered in Tempe, Arizona. The company began offering its service in April of 2005. LifeLock is the largest and fastest growing identity theft prevention company in the United States.

What is the price for the LifeLock service?
$110/ year per adult OR $10/ month per adult
$25/year for children 15 and under

Does LifeLock have a family discount plan available?
No, we do not. Everyone has a different SSN and identity, so Life Lock must charge a rate per person. The guarantee is also based upon per person membership.

Why does the entire family have to pay annually if there is a minor child listed in the family?
LifeLock now provides the option to pay either monthly or annually regardless of if there are minors on the account.

I prefer signing my family up monthly as opposed to annually. Can you do this?
Yes, you can choose between paying annually or monthly during signup.

How do I access my account after enrollment?
If you need to make a change to your account, contact client services at 1-877-LIFELOCK.

What happens if I get a fraud alert letter from the credit bureaus stating they cannot find my minor child's credit profile?

That is good, because your minor shouldn't have one. This letter can be ignored. If the child is a client, they too are protected by the guarantee.

What if I get a fraud alert letter from the credit bureaus that says my minor child's fraud alerts have been set?
That is good because this means that your child's account is protected to the same extent as yours. We will also make sure that the credit bureaus are notified that this is a minor's account and there should be no activity on it.

Why do I need to add a previous address to my account?
If you have been at your current address for less than 2 years, the credit bureaus want your previous address in order to set the fraud alerts on your credit file. If you don't give a previous address, then we need documentation to send to them to verify that it is you. To do this, we need a copy of your DL license and a utility bill with your name and address on it.

Why does LifeLock need to know my personal information?
In order to request that the credit bureaus place fraud alerts on your behalf, we need your personal information to do so.

How do I know LifeLock's system won't be hacked by criminals or employees of LifeLock?
LifeLock is certified ISO 27001. This is the most stringent security certification within the industry and LifeLock was the first company in the identity theft prevention field to achieve this status. Life Lock has taken every measure possible to keep information secure. Nevertheless, as a client of LifeLock, you are still covered by our guarantee.

Can I enroll other family members later?
Yes, call client services to enroll them.

Can I obtain my credit score through your service?
While receiving one free credit report from each bureau each year is part of the standard LifeLock service, your credit score is not included. By law, you are allowed one free credit score a year but you would have to initiate the request through the bureaus yourself. If you wish to obtain additional credit reports, those too would need to be obtained directly from the bureaus.

Are there any plans for LifeLock to go public?
LifeLock is a private company and at this time has no plans to go public.

How long has your company been in existence?
While the LifeLock system has been in testing and development for more than three years, the company first started selling its services in April 2005.

How many customers do you have?
We are growing very quickly. As of September, 2007, we have more than 300,000 individual clients.

Who backs up LifeLock financially?
LifeLock is funded by private equity investment and venture funds.

How long does it take to obtain my credit reports?
The credit bureaus have been getting a substantial amount of fraud alert requests and may take up to 4-6 weeks for you to receive your report. Although you may not have received your credit report, you are still covered by LifeLock from the time you signed up.

Does LifeLock cover my business as well as my personal credit?
LifeLock can only cover individuals with Social Security numbers.

Who calls me to let me know that someone is attempting to obtain credit in my name?
It will be the creditor who is determining whether to issue a line of credit.

I'm applying for new credit and I'm a client, do I need to call Life Lock?
No, it is not necessary to contact LifeLock. However, if you run into any problems or undue delays, call us at any time and we'll expedite the process for you.

I already have alerts on my credit file, what will happen to them when I become a client of LifeLock?
Once your fraud alerts have expired, LifeLock will request on your behalf that the fraud alerts are reset and continue to do so as long as you stay a client or until you no longer believe that you may become a victim of identity theft. If you sign up as a client while these initial alerts are placed you will be covered by our guarantee at the time you sign up for the LifeLock service.

Do I need to call you if any of my information changes on my account?
Yes, contact client services with any account changes.

If someone steals my credit card number, how would LifeLock handle this?
The fraud alerts that LifeLock requests are designed to help prevent someone from opening a new line of credit. If someone gets your credit card number, first report that credit card as stolen. If charges were placed on that card, your credit card company should credit your account for some or all of the charges. Should you need assistance resolving the issue, call us and we'll expedite the process for you.

Will signing up for LifeLock damage my credit score?
No, LifeLock will not affect your credit score in any way.

What questions will the creditor ask me for verification?
The creditor will ask you questions that only you would know the answer to. Most questions will be taken off your credit report. For instance, your previous address, who your mortgage is through, what your car payment is, etc.

What if there's a dispute? Will you handle it for me?
If there is a dispute, we will hire qualified professionals to do whatever it takes, for as long as it takes, to resolve the problem.

If the consumer can do these things by themselves, what is the need for LifeLock?
Convenience and protection; for instance, most people could change the oil in their car but don't. LifeLock requests on your behalf that fraud alerts are placed on your credit report every 90 days so you don't have to worry about it. However, the most important value is the $1 million dollar Service Guarantee. Remember just because you have fraud alerts placed does not guarantee you from becoming a victim.

Will I get $1 million if I become a victim of identity theft?
Not necessarily. We will reimburse you for any money you lose because of the theft and we will pay the costs associated with repairing the problem up to $1 million.

What is the most important part of the LifeLock service?
The overall peace of mind you'll get when you know you are completely protected from identity theft.

What is the process if my information is taken while a customer?
You should contact LifeLock immediately. We and our expert partners will take care of the rest.

Where does the $1 million come from that covers the guarantee?
Our service guarantee is funded through funds in reserve accounts, coupled with insurance coverage from one of the highest rated insurers in the nation.

Can LifeLock stop someone from removing money from my bank account?
No, but the LifeLock guarantee will replace any funds the bank doesn't.

If credit card companies will pay me back for anything criminals use, what does LifeLock do?
While most credit cards will pay back items purchased by someone else once the card is reported stolen, there is still small print and a time period where everything must be reported. In any case, the Life Lock guarantee is intended

to protect your credit and new cards and or bank accounts that could be issued.

If I lost my wallet and someone used my credit cards and drained my bank account, what would LifeLock do?
After you let the bank and credit card companies know your wallet is no longer in your possession and they do what they can, LifeLock will reimburse you for the rest of your losses. LifeLock can also hire professionals to work on your behalf to oversee the process so you are not out any time.

Is it true that I need to sign a power of attorney with LifeLock?
No. The power of attorney we require is ONLY IF YOUR ID is compromised and we need to act on your behalf in instituting our $1 million service guarantee. Additionally, the power of attorney we require at that point is very limited and only allows us to work on your behalf regarding issues surrounding your identity. You may revoke this at any time.

Is there anyone else that does what LifeLock does?
There are companies similar but no one has the experience, process or expertise. No other company provides a $1 million dollar service guarantee.

If I shred papers and check my credit reports, will I be protected?
Shredding personal papers is a great step to protect your identity, but you must understand that your information is everywhere. Your doctor, dentist, your college, your bank and your health club are examples of places your personal information is stored.

What would you consider to be the two or three most important things a consumer can do to protect his/her privacy?
1. Set fraud alerts! They expire every 90 days, so you will need to continually renew them yourself or sign-up for LifeLock (www.lifelock.com) at $10 per month and we not only request that the alerts be renewed, we stop most pre-approved credit card offers and junk mail, and we back it up with a $1 million service guarantee.
2. Check your credit report every three to four months to look for fraudulent activity.
3. Shred your mail and unneeded personal information.

Does LifeLock monitor credit cards?
No, credit card companies do a fine job monitoring their own cards. LifeLock helps provide protection against someone applying for new credit cards in your name.

What is the difference between credit card theft and identity theft?
Credit card theft is when someone steals your credit card and runs up charges. Identity theft is when someone steals your personal information (social security number, date of birth, name, etc.) and uses it to open a new line of credit, gain employment or even establish citizenship.

What's the difference between fraud alerts and a credit freeze?
A credit freeze locks down all of your personal information making it impossible for anyone to open a line of credit in your name, including you. There are also fees involved with many credit freezes. When you place a freeze, you pay a fee. From there on, if you want to open any new line of credit (loan, credit card, cell phone) the freeze must be lifted; there will be a fee for that as well.

Currently 33 states and the District of Columbia offer the credit freeze option, but if you are not in one of them, you cannot do this. Everyone can subscribe to LifeLock.

Why doesn't LifeLock offer credit monitoring?
Credit monitoring will alert you after someone has stolen or used your identity. LifeLock wants to protect you before that ever happens. We have found that once our systems are in place, credit monitoring provides no additional benefit.

Why does everyone recommend credit monitoring and not a service like LifeLock?
Credit monitoring is the old technology, but it is something with which people are familiar. LifeLock represents the new generation in Identity protection.

Credit watch services have come into prominence thanks to the many breaches that have been publicized. What exactly is a credit watch, and what benefit does such a service offer the consumer?
Credit Monitoring (or a watch) is the credit bureau selling the consumer their own information. After there has been a change on your credit report, the bureau notifies you in 24 to 72 hours that there has been a change. It is then the consumer's responsibility to check the information for accuracy and by the way, if they find that it is a case of identity theft, the consumer is responsible for any losses, expenses and has to spend the time to clean up the mess. The Bureaus do nothing to actually prevent the crime of identity theft, nor do they help fix the problem.

How does a credit watch service work, and are there significant differences between the three major services (Experian, TransUnion, Equifax)?
All three work basically the same, but it should be noted that each bureau only notifies you when there has been a change on their credit report, not the other two.

When an organization offers a free credit watch subscription in response to a breach that may have affected a consumer, is the service different than what he or she would receive if they subscribed on their own?
Monitoring may give the victim of the data breach a false sense of security. Again, the bureaus do nothing to actually stop the crime before it happens and do nothing to help after a person has been victimized. They only provide quick notification of a change, nothing more.

What is the consumer's responsibility once a credit watch service is initiated? Is it a "turn it on and it works" proposition, or must the service be actively managed by the consumer to have any real effect?
The burden is on the consumer. They must check the credit report after they have been notified of a change and then they are responsible for cleaning up any mess of identity theft. The FTC says it is an average of 177 hours over two years, if you can clean it up at all.

Are there hidden costs, dangers, etc. to working with the credit agencies?
What should consumers know that might be otherwise difficult to find out on their own?
Consumers should know that the credit reports you buy will not include any "non-match" name and social security numbers. That means that if someone steals your social security number for employment, but uses their name, you will not see the accounts on your credit report. However, your credit score could be affected and lenders would be able to see the data.

Resources

Chapter 1 – Article, Ronald E. Hudkins, Jan 2008, no other references.
Chapter 2 – Introduction by Ronald E. Hudkins, Feb 2008, no other references.
Chapter 3 – What is Identity Theft – Internet definitions, resources listed following individual descriptions.
Chapter 4 – Identity Theft Statistics as listed by;
Javelin Strategy & Research Survey - February 2007
Javelin/Better Business Bureau Survey - January 2006
Javelin/Better Business Bureau Survey - January 2005
Federal Deposit Insurance Corporation - December 2004
Identity Theft Resource Center - September 2003
Federal Trade Commission Survey - September 2003
Gartner Survey - July 2003
Privacy & American Business Survey - July 2003
Chapter Five How Do Thieves Steal an Identity? – Extracted from The Federal Trade Commission's Consumer Information Section, Feb 2008 at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html
Extracts from the Department of Justice Consumer Information Section, Feb 2008 at http://www.usdoj.gov/criminal/fraud/websites/idtheft.html
Examples of Identity Theft provided by Wikipedia, the free Internet encyclopedia, Jan 2008 at
http://en.wikipedia.org/wiki/Identity_theft#Examples

Chapter Six How Long Can ID Theft Impact You? - Extracted from The Federal Trade Commission's Consumer Information Section, Feb 2008 at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

Chapter Seven What Can You Do About ID Theft? – Extracted from the Department of Justice Consumer Information Section, Feb 2008, at http://www.usdoj.gov/criminal/fraud/websites/idtheft.html

Chapter 8 – The Official site of the Identity Theft Resource Center, Feb 2008, http://www.idtheftcenter.org/artman2/publish/v_fact_sheets/index.shtml

Chapter Nine – The Official site of the Identity Theft Resource Center, Feb 2008,
http://www.idtheftcenter.org/artman2/publish/v_templates/index.shtml
Where you can find the following Sample Letter Templates as needed to correct identity theft victimization;

Form Letter 117-1 Request a Credit Report for the Deceased

To request a copy of your deceased love ones credit report.

+++

Form Letter 117-2 When Your Deceased Love One is a Victim of Identity Theft

A letter form to send to the CRA's when your deceased love one is a victim of identity theft.
++

Letter Form 100 - 1 Initial Victim of Identity Theft Statement and Fraudulent Account Information Request to Credit Issuers for Merchants

Send this letter to Merchants who appear on your credit report to request information on the fraudulent account that has been opened.

++

Letter Form 100 - 2 Confirmation of Conversation - Letter of Clearance

Confirmation of Conversation - Letter of Clearance

++

Letter Form 100-3 To Credit Issuers: Requesting a Fraudulent Inquiry to be Removed

If an inquiry has been made to your credit report that you did not initiate, this is the letter form to send to that credit issuer to request that they remove it from their records.
++

Letter Form 115-1 A Letter from the Victim to the Credit Issuer when the imposter will not cooperate

Letter Form 115-1 When You Know The Imposter
A Letter from the **Victim** to the **Credit Issuer** when the imposter will not cooperate and sign Letter Form 115-2
++

Letter Form 115-2 Imposter Accepting Responsibility for Accounts or Charges

Letter Form 115-2 - Letter Forms for When You Know the Imposter
<u>To be written by the imposter</u> accepting responsibility for accounts or charges.
++

Letter Form 115-3 When Both Parties Reach an Agreement to Resolve the Case

Letter Form 115-3 When You Know the Imposter
A Letter to be used when both parties privately reach an agreement with each other to resolve the case.

+++

Letter Form 116-1 Collection Agencies Sample Letter to Merchant

Letter Form 116-1 Collection Agencies Sample Letter to Merchant
++

Letter Form 116-2 Collection Agencies Sample Letter

Letter Form 116-2 Collection Agencies Sample Letter

++

Chapter 10 – What is an Identity Theft Report – Extracted from the Federal Trade Commission's Consumer Information Section, Jan 2008 at;

http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html#Whatisanidentitytheftreport

Chapter 11 - Comparison of ID Theft Protection Services

NextAdvisor.com is
The trusted, independent source for
Comparing the most valuable new services for Avoiding
ID Theft and other consumer services

They are located at
http://www.nextadvisor.com/identity_theft_protection_services/compare.php

Legal Notice - Reminder

You may give this book away to your subscribers, friends or customers; offer it as a free download from your website, or anything you like. The only restriction is that you not sell this book and must leave all pages, references, graphics, banners, links and ownership rights in place. Another words – Do not alter it in any manner!

Recommended Products and Other Services

Consumer Goods (Food)

Learn how you can make a perfect cup of coffee or Tea...every time...with no messy clean-up

- HerbaGreen Teas
  Not your ordinary green tea, HerbaGreen Teas contain **a balanced antioxidant formula** with standardized extracts of carefully selected, wild crafted herbs from the mountains of China for optimum therapeutic benefits for you and your entire family! Contains NO calories or caffeine.

- PURJAVA HONDURAN DARK ROAST
  PurJava liquid coffee concentrate is the easy way to make just the amount of coffee you want -- with no waste. Just add a 1/2 tablespoon to 8 ounces of hot water and you've instantly got a delicious cup of fresh coffee. One 8 oz. bottle of PurJava Honduran Dark Roast makes 32 (8 oz.) cups of coffee.

- PURJAVA SUMATRA DECAFFEINATED
  PurJava liquid coffee concentrate is the easy way to make just the amount of coffee you want -- with no waste. Just add a tablespoon to 8 ounces of hot water and you've instantly got a delicious cup of fresh coffee.
  One 8 oz. bottle of PurJava Sumatra Decaffeinated makes 16 (8 oz.) cups of coffee.

Business Owner Advertising

Great for you, great for your customers! Simply put, Nice Offers can save your customers big money – because you, likewise, can save big money by securing customers through Nice Offers unique pay-only-for-results advertising system.

To Learn more about Increasing Customers and Your Bottom Line Profits visit

http://www.adultwishfoundations.com/customers.html

Business Owner Merchant Services

Merchant Services Just Got More Streamlined and Economical!

Designed as a complete, money-saving transaction solution for merchants, the suite of Merchant Services includes credit card processing, debit card processing, bad check recovery, check verification, gift cards, and more. Start increasing your profits NOW. To learn more or to get started please visit;
http://www.adultwishfoundations.com/credit.html

Veriuni Advanced Antioxidant with Red Wine Extract

Our **Advanced Antioxidant** with Red Wine Extract helps safeguard your immune system, retard the aging process, and protect your health. Research has shown antioxidants also support heart health and eye health - both important to older adults. One dose delivers 500 mg of Vitamin C, 400 IU of Vitamin E, and 30 mg of red wine extract.

https://www.ezinfocenter.com/9999222/Department.vstore?id=34#item1565

Veriuni Advanced Joint Support

Veriuni Advanced Joint Support contains FOUR of today's best selling joint health neutraceuticals to promote better joint health, maintain strong muscles and muscle tone, increase connective tissue regeneration and repair, and help with muscular energy (ATP) levels and joint function and mobility.

https://www.ezinfocenter.com/9999222/Department.vstore?id=34#item1565

Veriuni Advanced Weight Loss

Advanced Weight Loss is the perfect "full-meal" replacement drink. Advanced Weight Loss will help you lose weight with 10g of protein per serving for lean muscles and a full array of vitamins, minerals, and calcium to replace any well balanced meal. Only 214 calories per serving in 8 oz. of skim milk. Available in three delicious flavors: Chocolate, Vanilla, & Strawberry.

https://www.ezinfocenter.com/9999222/Department.vstore?id=34#item1565

Veriuni Advanced Whey Protein

Veriuni's Advanced Whey Protein is the overwhelming choice for athletes, dieters, and weekend recreational warriors. Critical to any individual looking to build and maintain muscle mass. Available in four delicious flavors: Vanilla, Chocolate, Strawberry and Banana.

https://www.ezinfocenter.com/9999222/Department.vstore?id=34#item1565

Veriuni Antioxidant Plus with Grape Seed Extract

Veriuni Antioxidant Plus is one of the most powerful antioxidant formulas available today to combat "free radicals" that can cause oxidative stress leading to premature aging and development of various ailments.

https://www.ezinfocenter.com/9999222/Department.vstore?id=34#item1565

Veriuni Creatine - Micronized Creatine Citrus

Veriuni Creatine is a blended, water-soluble form of creatine. Creatine Citrus has 90% absorption compared to Creatine Monohydrate's 40%. Creatine is a naturally occurring metabolite that helps recycle the body's supply of ATP for increased energy output, strength and endurance.

https://www.ezinfocenter.com/9999222/Department.vstore?id=34#item1565

Veriuni Diet Assist CLA - Conjugated Linoleic Acid

Veriuni Diet Assist CLA works by reducing fat and increasing muscle. CLA is both an appetite suppressant and fat reducer and can help people to lose weight and keep it off.

Daily supplementation with Veriuni Diet Assist CLA can result in 1 to 2 pounds per week of weight loss.

https://www.ezinfocenter.com/9999222/Department.vstore?id=34#item1565

Veriuni Ginseng Energy!

This formulation definitely will give you an energy boost and give you a heightened sense of awareness. The formulation is designed to improve circulation and promote oxygen levels in the brain. Tablets contain Siberian Ginseng, Kola Nut Extract, Lysine, Phenylalanine, Glycine, and Cyanocobalamin.

https://www.ezinfocenter.com/9999222/Department.vstore?id=34#item1565

Veriuni Joint Health

Veriuni Joint Health is a nutraceutical that promotes joint health with a highly absorbable form of glucosamine, which nutritionally supports connective tissue and joint structure and function and is a basic building block for cartilage, synovial fluid, and other connective tissues.

https://www.ezinfocenter.com/9999222/Department.vstore?id=34#item1565

Veriuni Natural Digestion - Digestive Enzyme Aid

In order to restore health and well-being to digestive problems, food (plant) enzymes are used to improve digestion and absorption of essential nutrients. Enzymes are an important link in stamina, energy level, utilizing vitamins and minerals and boost the natural immune system.

https://www.ezinfocenter.com/9999222/Department.vstore?id=34#item1565

Veriuni Super 25 Multivitamin & Minerals

Our **Veriuni Super 25** offers the most complete daily supplement, with 25 essential vitamins, minerals, and antioxidants. This vitamin is designed specifically to bolster immune systems. It contains unique ingredients and is loaded with the powerful antioxidant CoQ10, which plays a critical role in the production of energy within each cell in the human body and can help promote weight loss.

https://www.ezinfocenter.com/9999222/Department.vstore?id=34#item1565

Veriuni Thermo! Fat-Burner Formula

Veriuni Thermo! is a NON EPHEDRA Thermogenic agent that provides unique ingredients to promote weight loss and fat burning safely. Pure Thermo Burn will give you energy and appetite suppressant activity.

https://www.ezinfocenter.com/9999222/Department.vstore?id=34#item1565

Fill life with Veriuni Nutritional Products. Give peace of mind that you are investing wisely in you and your family's wellness and nutrition. Making Health for the future is a specific purpose of Veriuni in cleaning products too.

Internet Shopping Mall

MaxMalls organizes hundreds of the Web's biggest and best stores. New stores will be added regularly. Many additional features are planned to create the optimum online shopping experience. To tour the mall businesses that all offer secure check outs visit;

http://www.adultwishfoundations.com/mall.html

Coupons, Discounts – Savings!

Nice Offers works directly with merchants all over the world to create exciting and exclusive offers for you, which are made available at this Nice Offers Website.

Nice Offers makes it easy for everyone everywhere to find great moneysaving deals on specific products and services you're looking for, while also providing a fun and exciting way to discover new and different products, services, businesses, restaurants, and more. See how you can save visit;

http://www.adultwishfoundations.com/offers.html

Home Based Business Free Opportunity

SFI is a totally FREE Home Business to join. And there's absolutely NO OBLIGATION. SFI provides you with FREE Websites, a FREE course that teaches you everything you need to know to make money online ($295 value), and hundreds of exciting products to stock your online store shelves with. Start earning an additional income now – sign up here;

http://www.adultwishfoundations.com/free.html

Needed Education for Those Running a Home Based Business

The International Association of Home Business Entrepreneurs IAHBE is an organization that champions the home-business lifestyle and provides its members with a multitude of resources designed to achieve maximum home-business success. Learn what they are offering by visiting;

http://www.adultwishfoundations.com/IAHBE.html