

E. Avoid using your Social Security number unless absolutely necessary. Consider replacing it with another number on your driver's license. Most states now offer the option of choosing an alternate number.

F. Secure your personal computer, using firewall programs, anti-virus software, and secure browsers. Minimizing online access to your personal information can help deter uninvited guests from your computer.

It Happened — What Do I Do?

Even after taking precautions, you may still be susceptible to this damaging crime. If you have become the victim of identity theft, there are ways you can help ensure the process of clearing your name moves smoothly.

1. Contact the Federal Trade Commission's Identity Theft Hotline 1-877-IDTHEFT (877-438-4338).
2. Create a list of all the creditors whom you suspect have received fraudulent information. Keep records of all communication with them, including written transcripts of phone conversations and copies of correspondence.
3. Inform the fraud departments of the three major credit bureaus (numbers on page 4), and ask that a "fraud alert" be attached to your file. Although the credit bureaus are not required to offer "fraud alerts," they generally will. This temporarily alerts a creditor that fraudulent activity may have been conducted on your accounts.
4. Terminate any accounts you were not responsible for opening and any existing accounts that were fraudulently used.

5. Report any information you have to the police, and be sure to give them copies of all relevant documents.

Depending upon the type of fraud that has been committed, you may need to take some additional steps. For example, if your Social Security number was used under false pretenses, contact your local Social Security office. Or, if an identity thief created a cell phone account with your billing information, contact the Federal Communications Commission (FCC).

Where Can You Go for Help?

There are many resources that can provide you with more information about identity theft prevention and protection, and offer you guidance should you unfortunately become a victim. The following are some useful phone numbers and websites:

The Federal Trade Commission:
877-IDTHEFT, www.ftc.gov

The Social Security Administration Office of
Inspector General (Fraud Hotline):
800-269-0271, www.ssa.gov

Internal Revenue Service:
800-908-4490, www.irs.gov

Federal Communications Commission:
888-CALL-FCC, www.fcc.gov

It may seem that each new technological convenience generates a new possibility for the invasion of your privacy. However, remember that taking a few, simple preventative measures can help you deter potential identity crimes against you. A strong *offense* may be your best *defense* against identity theft.

Identity Theft

How to Avoid the Nightmare and Protect Your Good Name



Consider the following scenario: After weeks of test drives and some negotiating with auto dealerships, you finally decide on the new car you want to buy. You're able to make a significant down payment, and you choose to finance the balance with a loan provided by the manufacturer. You have visions of leisurely weekend drives through the country, but they suddenly come to a screeching halt when the salesperson tells you that your loan has been turned down. Like many people, you carry some debt with a mortgage, but you pride yourself on making timely payments on all your bills.

In order to determine why your loan was denied, you order a copy of your credit report. When it arrives, you are surprised to see there are accounts under your name that you never opened — and none of them have been paid. Your existing credit card balances are higher than you remember them being since paying your last bill. How could this have happened? You may have been the victim of **identity theft**.

What Is Identity Theft?

On October 30, 1998, Congress passed the Identity Theft and Assumption Deterrence Act. The law defines identity theft as the following: when someone “*knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.*”

While once a virtually unknown crime, the National Association of Attorneys General (NAAG) reports that hundreds of thousands of people are now plagued by identity theft each year. The increased prevalence of this crime prompted a bill called the Identity Theft Penalty Enhancement Act.

Signed into law on July 15, 2004, it established harsher penalties for perpetrators of identity theft crimes.

How Does It Happen?

In today's technologically advanced society, identity theft is easier to commit than you might think. The Internet and Automated Teller Machines (ATMs), now widely used for a variety of financial transactions such as shopping online and making cash withdrawals, are often cited as two contributing factors to what many perceive to be an identity theft epidemic.

If you become a victim it can be *financially*, as well as *emotionally*, devastating. With your personal information, a criminal might be able to simply open a credit card account and make fraudulent charges, or in more extreme cases, a thief may even assume your identity and open bank accounts under *your* name. If you worry about your personal information getting into the wrong hands, familiarize yourself with the following ways a criminal might obtain information with the intent to steal money or commit other crimes:

“Shoulder Surfing.” Shoulder surfing occurs when someone lurks near you while you give personal information to another person or enter it into a machine. Usually, the perpetrator peers over your shoulder and procures your information while you continue with your transaction. For example, if you are in a public place on a cell phone making hotel reservations, an eavesdropper might be able to remember, or write down, your name and credit card information. That information can then be used to make fraudulent purchases. Or, if you make a store purchase with a credit card and lose your receipt, someone — even the store employee — may take the receipt with your information and commit fraud. Shoulder

surfing can also be a hazard at ATMs. If someone inconspicuously standing in line manages to get your personal identification number (PIN), it may help him or her gain access to your bank account.

Pickpocketing and Lost Wallets. Years ago if you lost a wallet or were pickpocketed, you probably only worried about the cash that was inside. However, today being pickpocketed or losing a wallet can mean facing thousands of dollars in fraudulent purchases with credit cards.

“Dumpster Diving.” Dumpster diving is as obvious as it sounds. If you dispose of trash containing personal information, such as credit card offers in a dumpster, others may have access to it. Identity theft perpetrators might “dive in” and easily find the information they need to wreak financial havoc under your name.

Intercepting Mail. Identity thieves watch mailboxes every day, waiting for the next credit card pre-approval letter to arrive. They then call the credit card company posing as the victim in order to open an account. While you cannot stop *all* solicitations, you can choose to “opt out” of receiving *some* of these letters. Calling 1-888-5-OPTOUT can help you limit the amount of unsolicited mail and phone calls you receive.

The Internet. Many Americans rely on the Internet to help them handle their personal finances. While it can be a useful tool for banking or paying bills, the Internet can also be a haven for prospective identity thieves. Entering your personal information into an unsecured website may allow an experienced hacker to obtain that information and use it at your expense.

Protecting Yourself

The aforementioned methods are just some of the ways you might fall victim to identity theft,

the effects of which can be difficult and time-consuming to correct. Everyone is a potential victim. However, there are a number of steps you can take to help keep your good name — and good credit — protected:

- A. If you must give out personal information while making a purchase, be aware of your surroundings and do it *discreetly*.
- B. Order a copy of your credit report *now* and check it for accuracy. Remember to do this once a year to stay informed of any significant changes in your credit history. You can contact any of the three major credit bureaus (listed below) for a copy.

EXPERIAN
Phone 888-EXPERIAN (888-397-3742)
Fraud Dept. 888-EXPERIAN
Website www.experian.com

EQUIFAX
Phone 800-685-1111
Fraud Dept. 800-525-6285
Website www.equifax.com

TRANSUNION
Phone 800-888-4213
Fraud Dept. 800-680-7289
Website www.transunion.com

- C. Do not give out personal information over the phone unless *you* have made the call yourself. This will help ensure that only the people and businesses *you* have chosen to contact are privy to your information.

- D. Purchase a paper shredder to properly destroy any documents, receipts, or pieces of mail that contain information an identity thief might find useful, such as bank statements and credit card pre-approval forms.