What To Do If You're a Victim

If you're a victim of identity theft, the Federal Trade Commission (FTC) recommends that you do the following:

- *Contact the fraud department* of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts.
- *Close the accounts* that you know or believe have been tampered with or opened fraudulently. Use the ID Theft Affidavit (available on the FTC website and accepted by the three major credit bureaus) when disputing new unauthorized accounts.
- *File a police report.* Get a copy of the report to submit to your creditors and others who may require proof of the crime.
- *File your complaint with the FTC* at www.consumer.gov/idtheft. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. Filing a complaint also helps the agency learn more about identity theft and the problems victims are having so that it can better assist you.

NCPC

Crime Prevention Tips From

NATIONAL CRIME PREVENTION COUNCIL
2345 Crystal Drive
Fifth Floor
Arlington, VA 22202
202-466-6272
www.ncpc.org

and

NEW YORK STATE POLICE
EXCELSIOR

www.troopers.ny.gov

BJA Bureau of Justice Assistance
Office of Justice Programs ■ U.S. Department of Justice

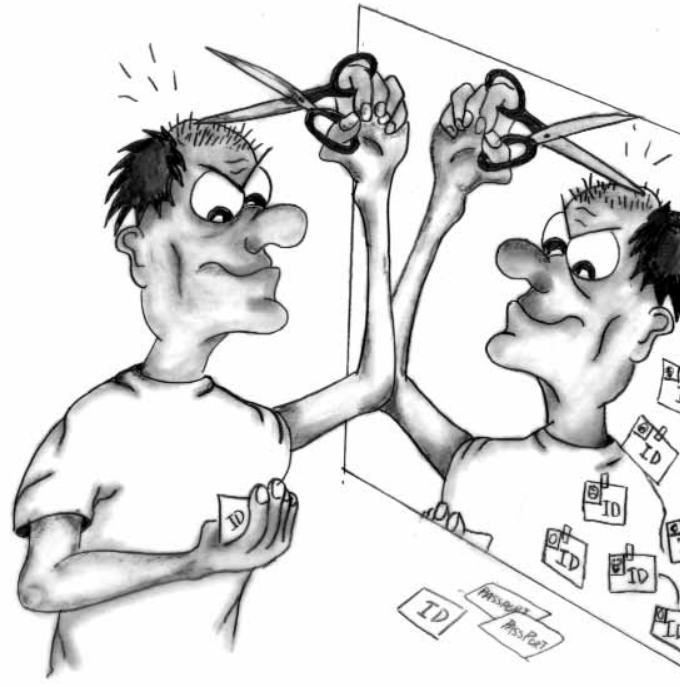
The National Citizens' Crime Prevention Campaign, sponsored by the Crime Prevention Coalition of America, is substantially funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.

tyco / Fire & Security ADT

Production made possible by a grant from ADT Security Services, Inc., a unit of Tyco Fire & Security Services.

2005

Identity Theft



NATIONAL CRIME PREVENTION COUNCIL

In the course of the day you may write a check at the drugstore, charge tickets to a concert, rent a car, call home on your cell phone, or apply for a credit card. Chances are you don't give these routine transactions a second thought. But others may.

Identity theft is the fastest growing crime in America, affecting half a million new victims each year.

Identity theft is the taking of a victim's identity to obtain credit and credit cards from banks and retailers, steal money from a victim's existing accounts, apply for loans, establish accounts with utility companies, rent an apartment, file for bankruptcy, or obtain a job using the victim's name. Thousands of dollars can be stolen without the victim knowing about it for months or even years.

How Identity Theft Occurs

All an identity thief needs is any combination of your Social Security number, birth date, address, and phone number. This makes it possible to create a fake driver's license and then pose as you in order to apply for credit. The identity thief might put in a change of address with a credit card company so you will not know that someone else is running up charges. Once an identity thief opens one account, opening a second and a third is easier.

Identity thieves can get information about you from doctors, lawyers, schools, health insurance carriers, and other places. They may pick up your discarded personal information, such as utility bills, credit card slips, and bank statements. They may hack into your computer and steal your Social Security or account numbers and credit card information. They may send you an email message asking you to "update" your account information and link you to a bogus website so they can steal your personal information.

How To Prevent Identity Theft

- *Do not give out personal information* over the phone, through the mail, or over the Internet unless you have initiated the contact or know with whom you're dealing.

- *Shred all documents,* including preapproved credit applications, insurance forms, bank checks and statements you are discarding, and other financial information.

- *Protect your computer from Internet intruders*—use "firewalls." Also use anti-virus software and keep it up-to-date.

- *Create hard-to-guess passwords* that cannot be found in any dictionary. Select passwords with at least eight characters and that include a mix of numbers and both uppercase and lowercase letters.

- *Minimize the identification information* and the number of cards you carry. Take only what you'll actually need.

- *Do not put your Social Security number* on your checks or your credit receipts. If a business requests your Social Security number, give an alternate number.

- *Be careful when using ATM machines and long-distance phone cards.* Someone may look over your shoulder and get your PIN numbers.

- *Make a list* of all your credit card account numbers and bank account numbers with customer service phone numbers, and keep it in a safe place.

- *If you request a new credit card* and it doesn't arrive in an appropriate period of time, call to make sure someone has not filed a change of address for you.

- *Never submit your credit card number* to a website unless it is encrypted on a secured site. Look at the bottom of the screen for a padlock symbol. Do not select to save your information on the site for future transactions.

- *Pay attention to your billing cycles.* Follow up with creditors if bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your credit account and changed your address.

- *Cancel all credit cards* you have not used in the last six months.

- *Order your credit report* at least twice a year from the three major credit bureaus: Equifax (**www.equifax.com**), Experian (**www.experian.com**), and Trans Union (**www.transunion.com**). The Fair Credit Reporting Act allows you to get one free credit report from each of the three major credit bureaus once per year. Visit **www.annualcreditreport.com**.

- *Correct all mistakes on your credit report in writing.* Send a letter to the credit reporting agency identifying the problems item by item, include a copy of the credit report, and send the letter return receipt requested.