



Identity Theft: Your Good Name Gone Bad!

What is Identity Theft?

Identity theft is when someone illegally obtains a person's identifying information, such as name, address, date of birth, social security number or mother's maiden name. Armed with this information, an imposter can open new credit card accounts, drain your bank accounts, purchase automobiles, apply for loans, open utility services and on and on.

No matter how cautious you are, you cannot guarantee that a criminal will not obtain your information. The following steps will tell you what the warning signs are, how to protect yourself, what to do if you become a victim and the resources you will need.

Warning Signs

Often, there are no warning signs that identity theft has occurred. However, some reasons for concern are:

- ◆ Your monthly credit card and bank statements suddenly stop arriving.
- ◆ You are denied credit for no apparent reason.
- ◆ You start getting bills from companies you do not recognize.
- ◆ Credit collection agencies try to collect on debts that do not belong to you.

How To Protect Yourself!

Personal Information

- ◆ Ask your bank, doctor's office, other businesses and your employer how they use and protect your personal information.
- ◆ Never carry your Social Security card, Social Security number, birth certificate or passport unless necessary.
- ◆ Do not put your address, telephone number or driver's license number on a credit card sales receipt.
- ◆ Social Security numbers or phone numbers should not be put on checks.
- ◆ Identifying information should not be given over the phone or the Internet to someone you do not know or on a cellular or cordless phone.
- ◆ Shred all personal documents before placing them in the trash!
- ◆ If your state uses your Social Security number as your driver's license number, ask for another number.

Financial Information

- ◆ Get a copy of your credit report every year.
- ◆ Keep your financial records out of sight. Burglars are just as interested in credit cards, bank accounts and investment statements as they are in your jewelry and other valuables.
- ◆ Check monthly credit card statements for charges you did not make. If monthly statements do not arrive in the mail call the lender immediately.
- ◆ Keep a list, in a safe place, of all credit cards and bank accounts including the account numbers, phone numbers and expiration dates. Only use your credit card on the Internet if it will be encrypted.
- ◆ Shred financial or confidential information such as credit card pre-approvals, credit card receipts, etc.
- ◆ If you have credit cards you do not use, store them in a safe place. Cancel the accounts if you will not use them again. Cut up old credit cards before discarding.
- ◆ Carry only the credit cards you plan to use.
- ◆ When you have applied for a new credit card, keep your eye on the mail and the calendar. If the card does not arrive within the appropriate time, call the credit card company.
- ◆ Do not use your mother's maiden name as a password for accounts. Make one up.
- ◆ Unless your mailbox is secure, mail payments at the post office and pick up new checks at your bank.
- ◆ If you are not interested in pre-approved credit offers, opt-out using the telephone number in our resource section.

What to do if you have become a victim

Despite your best efforts to protect yourself, you have become a victim. Now what? The following steps should be taken immediately and at the same time to best insure your protection.

Record Keeping

In the process of resolving the theft of your identity, be sure to keep records of all correspondence with the creditors and government agencies you contact. Include the date and name of contact. Follow up all telephone contacts with a letter and keep a copy.

Creditors

Notify all creditors and financial institutions in writing and by phone that your name and accounts have been used without your permission. If an existing account has been stolen, ask the creditor or bank to issue you new cards, checks and account numbers. Carefully monitor your account activity on your statements. Report fraudulent activity to the issuing company immediately. The Fair Credit Billing Act (FCBA) is a federal law that limits a consumer's responsibility for fraudulent charges to \$50.

Local Law Enforcement

Immediately report the crime to local police. Provide them with as much documentation as possible. Make sure that the accounts are listed on the police report. Also, get a copy of the

police report. Credit card companies, banks and credit reporting agencies may require you to show a police report to support your claim that a crime was committed.

Federal Law Enforcement

Report the crime to the Federal Trade Commission (FTC). The FTC collects complaints about identity theft from consumers and stores them in a secure online database called the Consumer Sentinel that is available to law enforcement agencies worldwide. The FTC provides information on ways to resolve problems resulting from identity theft and refers individuals to various private and government agencies for further action.

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue, N.W.
Washington, DC 20580
1-877-IDTHEFT
www.consumer.gov/idtheft/

The Credit Reporting Agencies

Contact the fraud units of the three credit reporting agencies: Equifax, Experian and Trans Union. Ask them to place a fraud alert on your credit report to help prevent new fraudulent accounts from being opened. Keep track of when it expires so you can ask for another one if necessary. However, not all creditors check your credit report before issuing a new account.

As an ID fraud victim, you are entitled to a free copy of your credit report. Also, ask the agencies for a copy of your credit report every three months once you have become a victim. This can help determine how many and which accounts listed are fraudulent. You can also identify the existing accounts that have been stolen.

Equifax 1-800-685-1111
www.equifax.com

Experian 1-888-397-3742
www.experian.com

Trans Union 1-800-916-8800
www.transunion.com

To opt-out of receiving pre-approved credit card offers, call 1-888-5-opt-out.

Utility Companies

Ask utility companies (local and long distance telephone service providers, gas, electric and water companies) to watch out for anyone ordering services in your name. If someone has

ordered services in your name, cancel those accounts. If you are having trouble with falsified accounts, contact your state Public Utility Commission.

Other Resources

United States Postal Inspection Service (USPIS)

The USPIS is a federal law enforcement agency that investigates cases of identity theft. The agency has primary jurisdiction in matters involving the integrity of the U.S. mail.

U.S. Postal Inspection Service

475 L'Enfant Plaza
Washington, DC 20260
202-268-2284
www.usps.gov/websites/depart/inspect/

United States Secret Service (USSS)

The USSS is a federal agency that investigates financial crimes. Generally, the USSS will intervene only when the dollar amount of the crime is high. However, they should still be notified in case it is part of a larger fraud ring.

U.S. Secret Service

Contact your local field office.
www.ustreas.gov/uss

Social Security Administration (SSA)

If you detect fraudulent use of your social security number, report it to the SSA. The SSA does not generally take action unless there is a high dollar amount, workplace impersonation or crimes committed in your name. They will only change your SSN if you fit their fraud victim criteria.

Social Security Administration

6401 Security Boulevard
Baltimore, MD 21235
1-800-269-0271 (fraud hotline)
www.ssa.gov/

Call For Action, Inc.

Call For Action, Inc. is an international network of consumer hotlines. CFA volunteers provide assistance and mediate cases on behalf of consumers and small businesses. For the office nearest you, refer to the back of the brochure. For more information on identity theft visit www.callforaction.org.

Additional steps to take:

- ◆ If your bank accounts have been tampered with close those accounts, destroy any checks and cut up any ATM cards. Ask for password protection when opening new accounts.
- ◆ If your checks have been stolen or misused, stop payment on all checks. Open a new account and reissue checks to legitimate creditors. Also, ask your bank to notify its check verification company to stop giving approval for any of the stolen checks.
- ◆ If you believe your investments or brokerage accounts have been tampered with, report it to your account manager and the Securities and Exchange Commission.
- ◆ Even if you think a problem is resolved, check your credit report every six months for several years after your identity was stolen.
- ◆ If you suspect your name and SSN are being used by an identity thief to get a driver's license or non-driver's ID card in your name, contact your Department of Motor Vehicles.