



IDENTITY THEFT PREVENTION TIPS:

- Safeguard your personal information.
- Do not share personal information with unknown persons or companies.
- Carry with you only the information you need.
- Order and review a copy of your credit report at least once a year.
- Shred documents containing sensitive information before discarding.

IF YOU BECOME A VICTIM:

- Contact the credit bureau fraud departments.
- Contact all the creditors involved.
- File a police report.
- Contact the Federal Trade Commission.
- Keep a record of your contacts.

IDENTITY THEFT CONTACT INFORMATION

EQUIFAX

Order Credit Report: 800-685-1111
Report Fraud: 800-525-6285
www.equifax.com

EXPERIAN

Order Credit Report: 888-397-3742
Report Fraud: 888-397-3742
www.experian.com

TRANS UNION

Order Credit Report: 800-888-4213
Report Fraud: 800-680-7289
www.tuc.com

FEDERAL TRADE COMMISSION

ID Theft Hotline: 1-877-IDTHEFT
www.consumer.gov/idtheft

PRIVACY RIGHTS CLEARINGHOUSE

619-298-3396
www.privacyrights.org

IDENTITY THEFT RESOURCE CENTER

Email: voices123@att.net
www.idtheftcenter.org



IDENTITY THEFT

Reduce Your Risk

WHAT IS IDENTITY THEFT?

Identity theft occurs when someone uses your name or personal information, such as your Social Security number, driver's license number, credit card number, telephone number or other account numbers, without your permission. Identity thieves use this information to open credit accounts, bank accounts, telephone service accounts, and make major purchases — all in your name. Information can be used to take over your existing accounts, or to open new accounts. Identity theft can result in damage to your credit rating and denials of credit and job offers.



HOW DOES IDENTITY THEFT HAPPEN?

Identity theft commonly begins with the loss or theft of a wallet or purse. But there are many other ways that criminals can get and use your personal information in order to commit identity theft. The following are some examples:

EXAMPLE #1

One evening, you sit down to pay your monthly bills. You write the checks, toss the statements in the trash and put the container out on the curb for the morning's trash pick-up. While you sleep, "dumpster-divers" go through your trash looking for the papers you've thrown away. They discover a gold mine of information that can be used for fraudulent purposes — your name, address, phone number, utility service account numbers, credit card numbers, and your Social Security number.

EXAMPLE #2

You receive an email message from what appears to be your Internet Service Provider (ISP). The message requests that you update the information they have on file about you — your name, credit card number, bank account number, etc. — by replying to the email or going to a specific Web site address to provide the information. However, neither the message nor the Web site address is from your ISP. They belong to someone who wants to get your information to steal your identity.

PROTECT YOUR IDENTITY

While there is no guarantee that your identity will never be stolen, there are steps you can take to minimize the risk:

- Do not give out your Social Security number to people or companies that you do not know.
- Before disclosing any personal information, make sure you know why it is required and how it will be used.
- Shred information you no longer need that contains personally identifiable information and account numbers. For example, credit card receipts, billing statements and pre-approved credit offers should be shredded before you discard them.
- Guard your mail from theft. Promptly remove your incoming mail from your mailbox and place outgoing mail in post office collection boxes. Install a locking mailbox if mail theft is a problem in your neighborhood.
- Keep the personal information you have at home and at work in a safe place.
- Do not carry extra credit cards, your birth certificate or passport, or other cards that display your Social Security number in your wallet or purse, except when necessary.
- Create unique passwords and personal identification numbers (PINS) and avoid using easily available information such as mother's maiden name, date of birth, or the last four digits of your Social Security number. Use passwords on your banking and brokerage accounts.
- Get a copy of your credit report from each of the three major credit reporting agencies at least once a year. Review the reports to be sure no one else is using your identity to open new accounts or to use your existing accounts.

IF YOU'RE A VICTIM

- **Contact the fraud departments of the three major credit bureaus.**

Request that a "fraud alert" be placed on your file and include a statement that creditors must get your permission before any new accounts are opened in your name. Get a copy of your credit report from each credit bureau so that you can dispute any inaccurate information. Check your reports at least every six months.

THE THREE MAJOR CREDIT BUREAUS ARE:

EQUIFAX

Order Credit Report: 800-685-1111
Report Fraud: 800-525-6285
www.equifax.com

EXPERIAN

Order Credit Report: 888-397-3742
Report Fraud: 888-397-3742
www.experian.com

TRANS UNION

Order Credit Report: 800-888-4213
Report Fraud: 800-680-7289
www.tuc.com

- **Contact all the creditors involved.**

Let them know that your accounts may have been used without your permission, or that new accounts have been opened in your name. If your accounts have been used fraudulently, ask that new cards and account numbers be issued to you. Check your billing statements carefully and report any fraudulent activity immediately. Many banks and creditors will accept the "ID Theft Affidavit" available at www.consumer.gov/idtheft, to dispute the fraudulent charges.

- **File a police report.**

Get a copy of the report to submit to your creditors and others that may require proof of a crime.

- **Contact the Federal Trade Commission.**

The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); by mail, Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington DC 20580; or online at www.consumer.gov/idtheft. Also request a copy of the publication, ID Theft, When Bad Things Happen to Your Good Name.

- **Keep a record of your contacts.**

Start a file with copies of your credit reports, the police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties. Follow up all phone calls in writing and send all correspondence certified, return receipt requested.

ADDITIONAL RESOURCES NON-PROFIT ORGANIZATIONS

PRIVACY RIGHTS CLEARINGHOUSE

3100 5th Avenue, Suite B
San Diego, CA 92103
Phone: 619-298-3396
Email: prc@privacyrights.org
www.privacyrights.org

IDENTITY THEFT RESOURCE CENTER

P.O. Box 26833
San Diego, CA 92196
Email: voices123@att.net
www.idtheftcenter.org

FEDERAL GOVERNMENT AGENCIES

FEDERAL BUREAU OF INVESTIGATION

www.fbi.gov/contact/fo/norfolk/ident.htm
FBI Internet Fraud Complaint Center
www.ifccfbi.gov

FEDERAL TRADE COMMISSION

Identity Theft Clearinghouse
600 Pennsylvania Avenue, N.W.
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.consumer.gov/idtheft

SOCIAL SECURITY ADMINISTRATION

SSA Fraud Hotline
P.O. Box 17768
Baltimore, MD 21235
1-800-269-0271
email: oig.hotline@ssa.gov

U.S. POSTAL INSPECTION SERVICE

www.usps.gov/websites/depart/inspect

STATE AND LOCAL GOVERNMENT AGENCIES

Contact your State Attorney General's office or local consumer protection agency to find out whether your state has laws related to identity theft.



Published by American Express in cooperation with the Privacy Rights Clearinghouse and the Identity Theft Resource Center. Information was prepared with the assistance of the Federal Trade Commission. This document may be reproduced for non-profit educational purposes.

© 2002, American Express Company
Consumer Affairs Office, 801 Pennsylvania Avenue
N.W., Washington, D.C. 20004