What is Identity Theft?

When someone else uses your personally identifying information without your knowledge or permission to:

- Obtain Credit Cards
- Empty Bank accounts
- Get Wireless or phone products, services
- Get Loans and Mortgages
- Obtain Employment
- Avoid Criminal Penalties
- Commit Other Frauds or Crimes

How can you tell if you are the victim of identity theft?

According to the Federal Trade Commission, important indications of identity theft include.

- Failing to receive bills or other mail signaling an address change by the identity thief.
- Receiving credit cards for which you did not apply.
- Receiving calls from debt collectors or companies about merchandise or services you never bought.
- Denial of credit for no apparent reason.

You may not realize you are a victim of identity theft until you try to obtain additional credit in your name, which usually requires a check of your credit report, or until a few months of non-payment on accounts that thieves have opened assuming your identity.

Reviewing your credit report can help you detect fraudulent activity early, allowing to take effective steps to limit the headaches you may encounter if you are a victim of ID theft.

Knowing what's in your report before you apply for a loan or a job may also be helpful.

BEFORE YOU ORDER:

- The three CRAs have established a single service to use when ordering free credit reports. Don't attempt to order directly through the CRAs.
- You will be asked to provide sensitive information.
- Request that no more than the last 4 digits of your social security number appear.

How to avoid becoming a victim of identity theft?

Experts tell us that to reduce or minimize the risk of becoming a victim of identity theft or fraud, you should do the following.

- Be "stingy" with personal information to others unless you have reason to trust them. Start by guarding your personal data and adopting a "need to know" approach to sharing such information.
- Don't be a "phish." Identity thieves, assuming the identity of major corporations or on-line retail businesses, send out mass e-mails that appear to come from companies you know and respect. This technique is commonly known as "phishing." NEVER click on a hot link in such an e-mail and never respond with any personal information. Reputable companies, especially financial services institutions, make it a policy never to seek personal information via internet.
- The more information that you have printed on your personal bank checks, such as your social security number or home telephone number—the more personal data you are routinely providing to people who probably don't need that information.
- Never throw away receipts or statements that contain personal information. The trash is the greatest repository of information for identity thieves. Invest in an inexpensive shredder to eliminate any personal information, like bank account numbers, social security numbers, etc.
- If someone you don't know calls you and offers the chance to receive a "major" credit card, a prize or other valuable item, but asks you for personal data—such as your social security number, credit card number and expiration date or mother's maiden name—ask them to send you a written application form.
- Don't leave your mail or newspaper out overnight. If you will be away from home for any period, have your home mail delivery stopped. Make sure your home looks as if it is occupied while you are gone.
- Write "Check ID" on the back of your debit or credit cards next to your signature. That way, when a retail store checks your signature on your card, they will verify that the card is being used by the proper individual.
- Be aware of people standing too close to you and "shoulder surfing" for your PIN number while you conduct ATM transactions.
- If you have to call someone while you're traveling, and need to pass on personal financial information to the person your calling, don't do it at an open telephone booth where a passerby can listen to what you're saying. Use a telephone booth where you can close the door, or wait until you're at a less public location to make the call.

Identity Theft Checklist

- File a complaint with your local law enforcement agency immediately. Obtain a copy of the police report. Most likely your bank, credit card company or other financial institution will require proof that a crime has been committed.
- Request or download an ID Theft Affidavit from the Federal Trade Commission to report an identity theft crime. It is accepted by all three credit bureaus and over 25 major creditors, thereby eliminating the need to file separate hand-written forms with many different companies.
- Call at least one of the "big three" credit reporting agencies. Place a fraud alert on your file. Consider a "freeze" on your credit information.
- Request a current credit report from each credit reporting agency. You should also add a "victim's statement" to your credit file that describes the theft of your identity and requests that creditors contact you before opening new accounts or altering accounts in your name. Review your credit reports every few months to verify that the corrections were made and to look for evidence of new fraudulent activity.
- Send a registered letter to all creditors with whom fraudulent accounts have been opened. Include a copy of the police report to substantiate the claim. Request a letter from each creditor acknowledging that the fraud took place and releasing you from liability for fraudulent charges. Also, request that creditors report that your previous accounts were closed "at customer requests."
- Contact and notify utilities and other service providers to alert them that you have been a victim of identity theft and request that new unique identifiers be established for your accounts.
- Report the loss of an ATM card, debit card, or checkbook to your bank, as well as any other account numbers that may have been stolen. Close existing bank checking and savings accounts and open new ones with new account numbers. Get a new ATM card with a new PIN number.
- Remember that changing bank account numbers will probably also require changing paycheck direct deposit arrangements, pre-authorized account withdrawals, and other types of automated deposits or bill paying services.
- Report a lost or stolen driver's license to the state Division of Motor Vehicles and request a new license with a new number (not your Social Security numbers).
- Report the theft of your mail to commit identity theft, or suspicions about falsified change-of-address forms, to your local post office inspector.
- If identity thieves have made unauthorized phone calls in your name, contact your service provider immediately to dispute the charges and establish new accounts.
- Keep copies of all correspondence with creditors and records of telephone calls (date, time, name of company, contact person, etc.) to document your efforts to correct credit problems.
- Visit www.consumer.gov/idtheft for tips on resolving identity theft problems. Download the booklet *ID Theft: When Bad Things Happen To Your Good Name* or request it by phone from the Federal Trade Commission (FTC). Also, visit the Privacy Rights Clearinghouse web site: www.privacyrights.org.

Contact Information

Check Verification Agencies

Global Payments	(800) 638-4600
Chex Systems	(800) 428-9623
CrossCheck	(707) 586-0551
International Check Service	(800) 526-5380
SCAN	(800) 526-5380
TeleCheck	(800) 710-9898

Credit Card Issuers

Visa	(800) 847-2911
Master Card	(800) MC-ASSIST
American Express	(800) 554-AMEX

Credit Reporting Agencies

TransUnion
Fraud Victim Assistance Department
PO Box 6790
Fullerton, CA 92834
Phone: (800) 680-7289

Equifax Credit Information Services, Inc.
Consumer Fraud Division
PO Box 740250
Atlanta, GA 30374
Phone: (800) 525-6285

Experian
National Consumer Assistance
PO Box 1017
Allen, TX
Phone: (888) 397-3742

Post Office (Postal Inspection Service Offices)

New Haven	(203) 782-7018
Wallingford	(203) 294-6760
Hartford	(860) 524-6454

Other Agencies

Internal Revenue Service	(800) 829-0433
Federal Trade Commission	(877) 438-4338
Social Security Administration	(800) 269-0271

Notes....

Office of the Victim Advocate

505 Hudson Street, 5th Floor
Hartford, CT 06106
Phone: 860-550-6632
Fax: 860-566-3542
Website: www.ova.state.ct.us

Quick Reference Guide

Identity Theft

State of Connecticut
Office of the Victim Advocate

505 Hudson Street
Hartford, CT 06106
Phone (860) 550-6632
Toll Free 1-888-771-3126
Fax (860) 566-3542