

Identity Theft

Your Good Name Gone Bad!

Identity theft is when someone obtains, and illegally uses, your identifying information, such as name, address, date of birth, social security number or mother's maiden name. 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.



Warning Signs

Often, there are no warning signs that identity theft has occurred. 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

Get a copy of your credit report every year. Check for accounts that may have been opened without your knowledge.

Keep a list, in a safe place, of all credit cards and bank accounts including the account numbers, phone numbers and expiration dates. Limit the number of cards you carry. Cancel inactive credit card accounts.

Do not use your mother's maiden name as a password for accounts. Make one up. Check if your online purchase is processed on a secure server.

Do not put your address, telephone number or driver's license number on a credit card sales receipt.

Do not list your Social Security Number on checks or any other documents in your wallet.

Before tossing "junk mail," shred any items that may include identifying information. Shred old statements and receipts before throwing them away.

Contact the post office if you think you are not receiving all of your mail. And don't leave envelopes with checks in your mailbox for postal pickup.

Be aware of others nearby when entering your Personal Identification Number (PIN). Don't carry PINs or passwords with you.

Be sure to pick up all card and ATM receipts.

Don't give out account numbers, SSN, or bank account details over the phone or on the Internet unless you initiated the contact and know the business is reputable.

Beware of "**phishing**" scams—e-mails, from what appear to be legitimate addresses or companies, that ask for personal and/or financial information. Do not respond to these e-mails. Delete them. **Legitimate institutions will not ask for this information via e-mail.**



If You Are 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.

Keep accurate records of all calls and letters regarding the theft. Follow up all telephone contacts with a letter and keep a copy.

Notify all creditors and financial institutions by phone and in writing 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.*

Immediately report the crime to local police. Make sure that the accounts are listed on the police report, and 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.

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.

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. *Keep in mind that 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. 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.

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 you are having trouble with falsified accounts, contact your state Public Utility Commission.

The Fair Credit Billing Act (FCBA) is a federal law that limits a consumer's responsibility for fraudulent charges to \$50.

Resources

■ CREDIT BUREAUS

Equifax 1-800-525-6285
www.equifax.com

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

Trans Union 1-800-680-7289
www.transunion.com

■ OPT-OUT OF RECEIVING CREDIT CARD OFFERS:

Call 888-5-opt-out (888-567-8688)

■ FEDERAL TRADE COMMISSION

Consumer Response Center
600 Pennsylvania Avenue, N.W.
Washington, DC 20580
877-IDTHEFT (877-438-4338)
www.consumer.gov/idtheft/

■ UNITED STATES POSTAL INSPECTION SERVICE (USPIS)

The USPIS is a federal law enforcement agency that investigates cases of identity theft.

475 L'Enfant Plaza
Washington, DC 20260
202-268-2284

202-268-2284

www.usps.com/websites/depart/inspect/

■ SOCIAL SECURITY ADMINISTRATION (SSA)

6401 Security Boulevard
Baltimore, MD 21235

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, visit www.callforaction.org/offices/.