



What is Identity Theft?

Identity theft is a crime in which someone obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, the thief might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen. It can destroy your credit and ruin your good name.

Identity theft is categorized in two ways: true name and account takeover. True name identity theft means that the thief uses personal information to open new accounts. The thief might open a new credit card account, establish cellular phone service, or open a new checking account in order to obtain blank checks. Account takeover identity theft means the imposter uses personal information to gain access to the person's existing accounts. Typically, the thief will change the mailing address on an account and run up a huge bill before the person whose identity has been stolen realizes there is a problem. The Internet has made it easier for an identity thief to use the information they've stolen because transactions can be made without any personal interaction.

(definition: SearchSecurity.com)

How does this happen?

Some of the common ways identity thieves steal your personal information include:

1. Dumpster Diving—yes, actually rummaging through trash looking for bills or other papers with your personal information on it.
2. Skimming—stealing credit/debit card numbers by storing the numbers when processing your card
3. Phishing—pretending to be financial institutions or other legitimate businesses sending you email or spam or pop-up messages to get you to reveal your personal information
4. Changing Your Address—diverting your billing statements to another location by completing a “change of address” form
5. Good Old Fashioned Stealing—stealing purses, wallets, mail (bank/credit card statements, preapproved credit offers, new checks), and tax information. Thieves may also steal personnel records from their employers or bribe employees with access to this information.

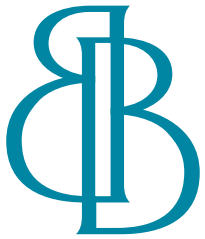
(source: www.ftc.gov/idtheft)



What are Some Simple Steps to Safeguard Your Identity?

You can deter thieves by following some simple, commonsense precautions:

1. Shred financial documents, statements, receipts, credit card offers, expired credit cards—anything that has personal information about you. Don't just throw mail away in the trash or recycling without shredding or ripping up items. It may have more information about you than you realize. You can also choose to "opt out" of pre-approved direct mailings by contacting a hotline sponsored by the credit bureaus at 1-888-5OPT OUT.
2. Only put your name and address on checks. If you put an account number in the memo section, try to only include the last four numbers—the bank should know the rest. NEVER print your Social Security or Driver's License number on checks. When you order checks, ask when to expect delivery, or consider picking up your new checks at the bank instead of having them in your mailbox.
3. Never carry a password or PIN in your wallet or purse. Memorize them. Use an unobvious combination of letters and numbers for your password. And, shield the keyboard at the ATM or point of purchase machines so others cannot see you entering your password.
4. Don't carry your Social Security card, passport or birth certificate in your wallet or purse on a regular basis. And don't give out your Social Security number unless it's absolutely necessary or you are sure your privacy is protected. Ask if another number can be substituted.
5. It's a good idea to photocopy everything in your wallet in case it is lost or stolen. It makes it easier to remember what was taken and to alert credit card companies and others that the cards have been stolen. Make sure to keep the copies in a safe place—locked in a file cabinet or in a safety deposit box.
6. NEVER give out personal information over the phone if you DID NOT initiate the call. Often scam artists call unsuspecting victims and pretend to be a legitimate financial company or bank and explain that they urgently need your information. Ask for the name, phone number and address of the company and offer to call them back. This may end the call right there if it is a scam. Or get the number off of a statement you received and call the company back. Chances are, you will then alert the company that someone is out there using their name illegally and they can then inform other customers.
7. Review your credit report regularly—at the very least annually. Check to make sure there are not accounts on it that you haven't opened and also check on any inquiries by people you don't recognize.
8. Carefully review every credit card and bank statement you receive and immediately contact the company to report any charges you did not make. And, ask specifically for monthly statements. Thieves will often use a change of address form to allow a few extra weeks of purchasing without your knowledge.
9. Do not mail bills or other items with personal data (checks, tax forms) from your home mailbox. Take them directly to the post office or an official postal drop box. It's very easy for criminals to remove the mail from your street box, use special chemicals to remove the ink from checks and then write them to themselves.
10. Guard deposit slips as closely as you do checks. Criminals can get your name, address and account number off these slips; then make deposits of bad checks and withdraw your money using the "less cash received" line tuition and other creditors to make them aware of the situation.



What are Some Simple Steps to Safeguard Your Identity? (cont.)

11. If you are ever denied credit, ask why. This may be the first indication that someone has stolen your identity and opened accounts or made excessive charges in your name.
12. Also, if one of your credit card companies calls you to report a possible fraudulent purchase, react quickly. Chances are the credit card company will handle that transaction, but this too could be an indication that your identity has been stolen. So, check your credit report immediately and possibly contact your financial insti
13. Many insurance and credit card companies now offer identity theft insurance and identity monitors. Though not a sure guarantee, this often lessens your chances of becoming a victim and will also help cover the time and expense that can be incurred if your identity is stolen.



Just how safe is the Internet?

Buying products and services online has become more and more commonplace. Let's face it, it's convenient, quick and allows for easy price and features comparisons. But is it safe? There are some safer options out there, plus some tips to watch for to help ensure you don't become a victim of Internet fraud or stolen identity.

1. Some newer purchase methods are safer options for consumers purchasing over the Internet. These include: stored-value cards (directly from the merchant or credit card companies); smart cards; Point of sale devices (mobile phones or PDAs that are linked directly to you); Digital cash; e-wallets and online payment services such as Paypal.
2. If you are paying by credit card, make sure the site is secured. Look for: independent services that offer site security, such as Verisign; a small symbol of a lock in one of the corners of your screen; a pop-up message telling you that you are now entering a secured site as you begin your purchase; or the site address will change to https:// as you enter the purchase area of the site.
3. Use the most recent version of your Internet browser (don't just ignore those update messages you often get when you log on!). Browsers are updated regularly and the software provides the latest built-in encryption capabilities that scramble your information as it passes from one server to another.
4. Check the web site's privacy policy. Make sure your information is kept confidential and not sold to others.
5. Use only one credit card for your online purchases. Makes purchases easier to track. And, review your monthly statements carefully.
6. NEVER give out login names or passwords on line—this includes emails. The latest scams are emails that look like they are from legitimate companies requesting this information. When in doubt, call the company directly and ask about the email.
7. Once you've made a purchase, most online merchants then follow up with a confirmation email to you. Review this information quickly and carefully. If there is a problem, call the company immediately.
8. Don't open email or any attachments from unknown sources. And make sure your virus protection is up to date on your email account. On-line hackers can often get information from computers through viruses.



What do I do if my information or identity is stolen?

If you determine that your identity has been stolen:

1. **The first thing to do is to contact the police.** The police should then generate a report or case number. You will need this number as some credit card companies may ask for it as verification that a crime has occurred.
2. **Then, immediately contact your credit card issuers and financial institutions.**
 - a. Close all existing accounts and open new accounts. Make sure the issuer notes on your old account that the “account was closed at consumer request.”
 - b. Follow up in writing to verify the date you initially contacted the credit card company and/or financial institution, and to confirm your request to close the existing account.
 - c. Close any other accounts that you know the thief has opened in your name.
 - d. Be sure to change any passwords associated with the old and new accounts. **DON'T** use anything obvious (mother's maiden name, last four digits of social security number, a birthday, etc.). Use a combination of letters and numbers in your passwords.
 - e. Next, call the fraud units at all three credit bureaus and report the theft. Request that your file be tagged with a “fraud alert” or a “victim's statement” which means anytime someone tries to open a new account in your name, it must be verified by the creditor by calling you at home. Confirm with the bureau representative that this will occur and provide the phone number where you would like to be reached. Keep in mind that this means you will not be able to obtain “instant credit” at a merchant, but this is the best way to prevent unauthorized account being opened.

The Credit Bureaus:

Equifax Credit Information Services
Consumer Fraud Division
P.O. Box 105496
Atlanta, GA 30348-5496
1-800-997-2493
www.equifax.com

Experian
P.O. Box 2104
Allen, TX 75013-2104
1-888-397-3742
www.experian.com

TransUnion
Fraud Victims Assistance Dept.
P.O. Box 390
Springfield, PA 19064-0390
1-800-680-7289
www.transunion.com

3. Make sure to document all conversations with authorities and financial companies. Keep a call log and copies of all correspondence and emails.
4. If your Social Security Number has been stolen, notify the Social Security Administration's Office of Inspector General:

http://www.ssa.gov/oig/public_fraud_reporting/index.htm
1-800-269-0271 from 10:00 a.m. to 4:00 p.m. Eastern Standard Time
410-597-0118 Fax
1-866-501-2101 TTY for the deaf or hard of hearing.

U.S. Mail:
Social Security Fraud Hotline
P.O. Box 17768
Baltimore, Maryland 21235



What do I do if my information or identity is stolen? (cont.)

5. Finally, file a report with the Federal Trade Commission (FTC) by contacting the FTC's Consumer Response Center. The FTC is the federal clearinghouse for victims of identity theft. The agency cannot prosecute, but does assist victims by providing resources and information to help them resolve the problems that result from the theft. The FTC can also refer victims to other government and private agencies for more help . To contact the FTC:

Consumer Response Center
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
1-877-382-4357
www.ftc.gov/ftc/consumer.htm

(Sources: American Bankers' Association; www.howstuffworks.com; Federal Trade Commission)