IDENTITY THEFT PROTECTION GUIDE

By Dana Altman, USLegalForms.com Staff Attorney

Introduction

Identity theft is a pervasive and fast-growing crime that affects millions of Americans each year. The Federal Trade Commission (FTC) reported that 43 percent of all complaints received in 2002 were based on identity theft. Identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes. Identity thieves steal your personal information to access your financial resources, obtain your identification documents, or obtain your benefits. A person also commits identity theft by obtaining goods or services through the use of your identifying information, and by obtaining identification documents in your name. Victims of identity theft may lose job opportunities, be refused loans for education, housing, or cars, and even get arrested for crimes they didn't commit.

Victims of identity theft are often faced with costly and time-consuming efforts to remedy the effects of identity theft and clear their name. Federal legislation exists to help victims of identity theft and, as well as many state laws, which vary by state.

In the fall of 1998, for example, Congress passed the Identity Theft and Assumption Deterrence Act. This legislation created a new offense of identity theft, which prohibits knowingly transferring or using, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law (18 U.S.C. § 1028(a)(7)). This offense, in most circumstances, carries a maximum term of 15 years' imprisonment, a fine, and criminal forfeiture of any personal property used or intended to be used to commit the offense.

Acts committed in connection with identity theft or fraud may also involve violations of other statutes such as identification fraud (18 U.S.C. § 1028), credit card fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C. § 1030), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), or financial institution fraud (18 U.S.C. § 1344). These federal offenses are felonies that carry substantial penalties in some cases, as high as 30 years' imprisonment, fines, and criminal forfeiture.

How Criminals Steal Your Identity

Some of the more common methods criminals you to obtain your personal information for illegal purposes include:

1. Using their position as an employee of a business or other institutions to steal records or information while they're on the job, bribing an employee who has access to these records, hacking these records, or conning information out of employees.

2. Stealing your mail, including bank and credit card statements, credit card offers, new checks, and tax information. They may also complete a change of address form to have your mail diverted to another address.

3. Rummaging through your trash, the trash of businesses, or public trash dumps to recover discarded documents containing personal information. This practice is known as "dumpster diving."

4. Abusing their employer's authorized access to get your credit report, or posing as a landlord, employer, or someone else who may have a legal right to access your report.

5. Stealing your credit or debit card numbers by capturing the information in a data storage device. They may swipe your card for an actual purchase, or attach the device to an ATM machine where you may enter or swipe your card. This is a practice known as "skimming."

6. Stealing your wallet or purse.

7. Stealing personal information from your home.

8. Posing as legitimate companies and claiming that you have a problem with your account to steal personal information from you through email or phone. This practice is known as "phishing" online, or pretexting by phone. A recently reported scam involves a person posing as a court official (jury coordinator) calling to report that a warrant has been issued for the victim’s arrest for failure to appear for jury duty. When the victim protests that he or she never received a summons for jury duty, the person asks for the victim’s social security number and date of birth to verify the information and cancel the arrest warrant.

Some Signs That You May Be the Victim of Identity Theft

1. Your application for a credit card is turned down because of a low credit score, yet you know that you’ve always paid your accounts on time, or your credit is accepted on less favorable terms.

2. You receive a call from a debt collector demanding payment on an overdue account for a credit card you have never had.

3. You receive a credit card in the mail that you've never applied for.

4. You receive phone calls or letters from debt collectors or businesses regarding products or services that you did not purchase.

Initial Steps to Take if You Are a Victim of Identity Theft

1. File a report with your local police or the police in the community where the identity theft took place. Get a copy of the report or, at the very least, the number of the report, to submit to your creditors and others that may require proof of the crime. Provide as much documented evidence as possible and make sure the police report lists the fraudulent accounts. Make a note of the phone number of your investigator so you'll be able to give it to creditors and others who require verification of your case.

2. File an identity theft complaint with the FTC. The FTC is a clearinghouse for identity theft information. They maintain a database of identity theft cases that they share with law enforcement agencies for investigations. The FTC can also refer complaints to other government agencies and companies to locate identity thieves. You may call the FTC identity theft hotline at 1-877-438-4338, use its online identity theft complaint form, www.consumer.gov/idtheft, or write: FTC Identity Theft Clearinghouse, 600 Pennsylvania Ave. N.W., Washington, DC 20580.

3. Create new Personal Identification Numbers (PINs) and passwords for any new accounts you open. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.

4. If the identity thief has made charges or debits on your accounts, or on fraudulently opened accounts, ask the company for the instructions to dispute those transactions. You should immediately close any accounts that you know or believe have been tampered with or opened fraudulently. Use the ID Theft Affidavit, available on the USLegalForms.com site at http://www.uslegalforms.com/identity-theft-forms.htm, when disputing new unauthorized accounts.

5. If your own checks are rejected at stores where you shop, contact the check verification company that the merchant uses. The major ones are:

Fidelity National Information Services
(was Certegy)
(800) 437-5120
www.fidelityinfoservices.com
SCAN

(800) 262-7771
www.consumerdebit.com

TeleCheck
For annual file disclosure
Fraud, id theft department
(800) 366-2425
(800) 835-3243
(800) 710-9898
.
International Check Services
(800) 526-5380
.
CrossCheck
(800) 843-0760
www.cross-check.com

6. Contact your state's Attorney General's office for information about identity theft assistance and laws in your state.

7. Contact your local Department of Motor Vehicles (DMV) to determine if another license has been issued in your name. Ask the DMV what procedures exist to prevent misuse of your identification. Some states offer a fraud alert will prevent another person from getting a license or identification card in your name. You will need to provide identification and copies of the police report, bills and other documents as evidence of your fraud claim. You may need to change your driver's license number if yours is being used as identification on bad checks or for other fraudulent reasons. Request that your social security number be removed from appearing on your license or that a substitute identification be used as your driver's license number.

When you contact the various entities to dispute charges and prove your identity has been used fraudulently, it's best to follow up phone calls with a dated written letter. Sending correspondence by certified mail with return receipt requested is preferred and always keep a copy of the letter you send. When sending dispute letters, include copies (NOT originals) of your police report or other documents that support your position.

Correcting Credit Abuse and Credit Reporting

Contact the fraud departments of any one of the three consumer reporting companies to place a fraud alert on your credit report. The fraud alert instructs creditors to contact you before opening any new accounts or making any changes to your existing accounts. You only need to contact one of the three companies to place an alert. The company you call

is required to contact the other two, which will place an alert on their versions of your report, too.

Under new provisions of the Fair Credit Reporting Act (FCRA, §605A) you can place an initial fraud alert for only 90 days. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. After placing the fraud alert in your file, you're entitled to one free credit report within twelve months from each of the three nationwide consumer reporting companies. You may also request that only the last four digits of your Social Security number will appear on your credit reports.

You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an "identity theft report." FTC regulations define an "identity theft report" to include a report made to a local, state, or federal law enforcement agency. If your local police department refuses to file a report and your situation involves fraudulent use of the U.S. mail, you can obtain an identity theft report from the U.S. Postal Inspector. If your case involves fraudulent use of a driver's license in your name, you might be able to obtain a report from your state's Department of Motor Vehicles. The FTC has more information on identity theft reports at www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#Identity

An extended alert stays on your credit report for seven years. You must have evidence of attempts to open fraudulent accounts and an identity theft report to establish the seven-year alert. When you place an extended alert on your credit report, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies. The consumer reporting companies will also remove your name from marketing lists for pre-screened credit offers for five years unless you request to be put back on the list before then.

Members of the military who are away from their usual duty station may place an active duty alert on your credit reports to help minimize the risk of identity theft while you are deployed. Active duty alerts remain on your report for one year. If your deployment lasts longer, you can place another alert on your credit report. By placing an active duty alert, you'll also be removed from the credit reporting companies' marketing list for pre-screened credit card offers for two years unless you request to be put back on the list before then.

Under federal law, you're entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance, or employment, and you request your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; you're on welfare; or your report is inaccurate because of fraud. Otherwise, a consumer reporting company may charge you up to $9.50 for another copy of your report within a 12-month period.

In addition to the free reports you're entitled to by activating a fraud alert, the federal Fair and Accurate Credit Transaction Act (FACTA) law enables you to receive a free credit report per year from each of the three credit bureaus (FCRA §612). It is recommended you make a follow up check of your report by requesting this free copy a few months after receiving the free report you received by placing the fraud alert. To order this free annual report from one or all the national consumer reporting companies, you must contact the Annual Credit Report Request Service, which is the centralized source for consumers to request this annual credit report. To contact the Annual Credit Report Request Service on-line, visit www.annualcreditreport.com. You can also contact the Annual Credit Report Request Service to obtain this free annual disclosure by calling toll free (877) FACTACT (322-8228) or by using the mail request form available at the central source website at www.annualcreditreport.com.

Once you have received your credit reports, examine each one carefully. If your credit report shows that the imposter has opened new accounts in your name, contact those creditors immediately by telephone and in writing. Report fraudulent accounts and erroneous information in writing to both the credit bureaus and the credit issuers by following the instructions provided with the credit reports. After you notify the credit bureaus about fraudulent accounts, the bureau is required to block that information from future reports. USLegalForms.com provides a sample letter at http://www.uslegalforms.com/identity-theft-forms.htm to send to the credit bureaus requesting that fraudulent accounts be blocked. The consumer reporting company has four business days to block the fraudulent information after accepting your identity theft report. It also must tell the information provider that it has blocked the information. The consumer reporting company may refuse to block the information or remove the block in some cases, such as false claims of identity theft. The consumer reporting company must inform you if it removes the block or refuses to place the block.

The bureau must also notify the person or entity who extended credit about the fraudulent account (FCRA, §605B). If the credit report doesn't include the names and phone numbers of those with whom fraudulent accounts have been opened, request this information from the credit reporting bureau. Ask the credit grantors in writing to furnish you and your investigating law enforcement agency with copies of the documentation, such as the fraudulent application and transaction records. Federal law (FCRA § 609(e)) and some state laws give you the right to obtain these documents. The business must provide copies of these records to the victim within 30 days of the victim's request at no charge. The law also allows the victim to authorize a law enforcement investigator to get access to these records.

Creditors will often ask you to fill out fraud affidavits. USLegalForms.com offers an affidavit form at http://www.uslegalforms.com/identity-theft-forms.htm. No law requires affidavits to be notarized at your own expense. You may choose to substitute witness signatures for notarization if creditors require verification of your signature. A victim of identity theft must provide a copy of the fraud affidavit, plus government-issued identification, and a copy of an identity theft report in order to obtain the documents created by the imposter. After the matter involving the fraudulent account is resolved

with the creditor, ask for a letter stating that the company has closed the disputed account and has discharged the debts. Keep this letter in your files.

In addition, instruct the credit bureaus in writing to remove inquiries that have been generated due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months (two years for employers) to alert them to the disputed and erroneous information.

In all communications with the credit bureaus, you will want to refer to the unique number assigned to your credit report and use certified, return receipt mail. Be sure to save all credit reports as part of your fraud documentation file.

Laws in several states give individuals additional opportunities to obtain free credit reports. Some states, such as California, have enacted legislation that allows individuals to place a "security freeze" on their credit reports. This is stronger protection than a fraud alert because it prevents anyone from accessing your credit file for any reason unless you instruct the credit bureaus to unfreeze your report. If you live in a state that offers the security freeze, you may want to consider using a security freeze if your identity thief is persistent and doesn't cease to use your identity to obtain credit. A list of the states where a security freeze is available may be viewed at www.consumersunion.org/campaigns//learn_more/003484indiv.html

Most states offer the security freeze free to victims of identity theft. Non-victims who wish to activate the security freeze as a precaution must pay a fee in most states. Some states make the security freeze available only to identity theft victims.

To place a fraud alert on your credit report, you may contact any of the following credit reporting agencies:

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Tax Information

If you think your identity has been stolen and used inappropriately for tax purposes, call the Internal Revenue Service (IRS) at 1-800-829-1040. If you have an unresolved issue related to identity theft, or you have suffered or are about to suffer a significant hardship due to enforcement of the tax laws, visit the IRS Taxpayer Advocate Service website www.irs.gov/advocate/ or call toll-free: 1-877-777-4778.

Bank and Brokerage Account Withdrawals

State laws govern fraud committed by a thief using paper documents, like stolen or counterfeit checks. However, federal law applies if the thief used an electronic fund transfer.

The federal Electronic Fund Transfer Act (EFTA) provides consumer protections for transactions involving an ATM or debit card, or another electronic method to debit or credit an account. It also limits your liability for unauthorized electronic fund transfers.

You have 60 days from the date your bank account statement is sent to you to report in writing any money withdrawn from your account without your permission. This includes instances when your ATM or debit card is "skimmed" that is, when a thief captures your account number and PIN without your card having been lost or stolen.

How much you can be liable to pay if your ATM or debit card is lost or stolen depends on how quickly you report it, so you should report the loss immediately.

- If you report the loss or theft within two business days of discovery, your losses are limited to $50.
- If you report the loss or theft after two business days, but within 60 days after the unauthorized electronic fund transfer appears on your statement, you could lose up to $500.
- If you wait more than 60 days to report the loss or theft, you could lose all the money that was taken from your account.

Note: VISA and MasterCard voluntarily have agreed to limit consumers' liability for unauthorized use of their debit cards in most instances to $50 per card, regardless of the time between the discovery of the loss or theft of the card and the time you report it.

The institution generally has 10 business days to investigate after receiving your notice of an error on your statement. After the investigation is completed, the institution must inform you of the results within three business days and must correct an error within one business day after determining that it occurred. If the institution needs more time, it may take up to 45 days to complete the investigation, but only if the amount in dispute is returned to your account and you are notified promptly of the credit. If the investigation determines that no error occurred, the institution may take the money back if it sends you a written explanation.

Chex Systems, Inc., produces consumer reports specifically about checking accounts, and as a consumer reporting company, must comply with the Fair Credit Reporting Act. Many banks use Chex Systems to find out negative banking information, such as bounced checks, which may prevent you from opening an account. You can request a free copy of

your consumer report by contacting Chex Systems, Inc. if you find inaccurate information on your consumer report.
Chex Systems, Inc.: 1-800-428-9623; www.chexhelp.com
Fax: 602-659-2197
Chex Systems, Inc.
Attn: Consumer Relations
7805 Hudson Road, Suite 100
Woodbury, MN 55125

To find out if the identity thief has been passing bad checks in your name, you may also call SCAN at 1-800-262-7771.

Bank procedures for protecting your account against unauthorized transactions vary by institution. For example, they may place a freeze on your accounts, but this can prevent you from making ATM transactions, conducting transactions online, and other services. If you are a victim of identity theft and your institution offers online access to your account, you should use it to monitor to your account daily for unauthorized transactions.

The above protections do not apply to brokerage accounts. If an identity thief tampers with your brokerage account, refer to your account agreement for information on what to do. Read the account agreement to determine if you are responsible for securing your own account information and know the steps you should take if your information has been compromised. Immediately report the incident to the brokerage company and notify the Securities and Exchange Commission at www.sec.gov as well as the National Association of Securities Dealers at www.nasd.org.

Bankruptcy

If you believe someone has filed for bankruptcy in your name, send written notification to the U.S. Trustee in the region where the bankruptcy was filed. A list of the U.S. Trustee Programs' Regional Offices is available on the UST website, or check the Blue Pages of your phone book under U.S. Government Bankruptcy Administration.

Your correspondence should include the facts of your case and provide proof of your identity. If you provide enough documented evidence of your claim, the U.S. Trustee will make a criminal referral to law enforcement authorities. You also may want to file a complaint with the U.S. Attorney and/or the FBI in the city where the bankruptcy was filed. You may need to hire an attorney to help prove your filing was fraudulent, since the U.S. Trustee does not offer free legal help or court documents. Copies of court documents may be obtained from the bankruptcy clerk's office for a fee.

False Criminal Charges

If you are falsely charged with a crime or traffic violation, file an impersonation report with the police/sheriff's department or the court, and confirm your identity. Have the police department take a full set of your fingerprints, photograph you, and make a copies of your photo identification documents, such as your driver's license, passport, or travel visa. You can request the police to establish your innocence by comparing the prints and photographs with those of the imposter.

If the arrest warrant is not issued from the state or county where you live, ask your local police department to forward the impersonation report to the police department in the jurisdiction where the arrest warrant, traffic citation, or criminal conviction originated.

Once your name is cleared, the law enforcement agency should recall any warrants and issue a "clearance letter" or "certificate of release". To prevent being falsely arrested again, you need to keep this document on your person at all times. Ask the law enforcement agency to file the record of the follow-up investigation establishing your innocence with the district attorney's (D.A.) office and/or court in the jurisdiction where the crime occurred, so that an amended criminal complaint can be filed. It is difficult o completely remove your name from a criminal database once it is entered, but you should request that the "key name" or "primary name" be changed from your name to the imposter's name (or to "John Doe" if the imposter's true identity is not known), with your name noted as an alias.

State laws on clearing your name is court records vary by state. You may contact the D.A.'s office in the county where the case was originally prosecuted for assistance, but may also need to hire a criminal defense attorney to help you clear your name.

If the identity thief is apprehended by law enforcement and goes to trial and/or is sentenced, write a victim impact letter to the judge assigned to the case. Contact the victim-witness assistance program in your area for advice on how to effectively impact the legal proceedings.

Debt Collectors

You may stop a debt collector from contacting you by writing a letter to the collection agency telling them to stop. After receiving you letter, the debt collector may only contact you further to tell you there will be no further contact, or to inform you that the debt collector or the creditor intends to take some specific action.

You may also send a letter to the collection agency, within 30 days after you received written notice of the debt, stating that you do not owe the money. Include copies of documents that support your claim, and also include a copy (NOT original) of your police report. After receiving your letter, a collector must send you proof of the debt in order to renew collection activities.

Passport Fraud

If you've lost your passport, or believe it was stolen or is being used fraudulently, contact the United States Department of State (USDS) through their website at www.travel.state.gov/passport/passport_1738.html, or call a local USDS field office. Local field offices are listed in the Blue Pages of your telephone directory. Even if you do not have a current passport, you should notify them of your identity theft to alert them to anyone ordering a passport fraudulently.

Phone Fraud

If an identity thief has established phone service in your name, is making unauthorized calls that seem to come from and are billed to your cellular phone, or is using your calling card and PIN, contact your service provider immediately to cancel the account and/or calling card. Open new accounts and choose new PINs. For assistance with difficulties in removing fraudulent phone charges from your account or getting an unauthorized account closed, contact the appropriate agency below:

- Contact your state Public Utility Commission for disputed local call charges.
- Contact the Federal Communications Commission (FCC) for disputed cellular or long distance charges. The FCC regulates interstate and international communications by radio, television, wire, satellite, and cable. Call: 1-888-CALL-FCC; TTY: 1-888-TELL-FCC; or write: Federal Communications Commission, Consumer Information Bureau, 445 12th Street, SW, Room 5A863, Washington, DC 20554. You can file complaints online at www.fcc.gov, or e-mail your questions to fccinfo@fcc.gov.

Social Security Number Misuse

The SSA Office of the Inspector General should be notified of information regarding specific instances of SSN misuse that involves the buying or selling of Social Security cards, may be related to terrorist activity, or is designed to obtain Social Security benefits. You may file a complaint online at www.socialsecurity.gov/oig, call toll-free: 1-800-269-0271, fax: 410-597-0118, or write: SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235. You may request a replacement Social Security Number card if yours has been stolen and, in very serious identity theft cases, you may attempt to change your Social Security Number.

You also may call SSA toll-free at 1-800-772-1213 to verify the accuracy of the earnings reported on your SSN, request a copy of your Social Security Statement, or get a replacement SSN card if yours is lost or stolen. Be sure to follow up with written correspondence and keep a copy for your files. You may also request a Social Security Statement (Form 7004) at www.ssa.gov/online/ssa-7004.html.

Student Loans

You should close the loan account by contacting the school or program that opened the student loan. Also report the fraudulent loan to the U.S. Department of Education. Call the Inspector General's Hotline toll-free at 1-800-MIS-USED; visit www.ed.gov/about/offices/list/oig/hotline.html?src=rt; or write: Office of Inspector General, U.S. Department of Education, 400 Maryland Avenue, SW, Washington, DC 20202-1510.

Medical Identity Theft

An identity thief may use a victim's identifying information to obtain medical treatment or medical supplies, or to submit false claims to Medicare/Medicaid or to a victim's health insurance plan. Medical identity theft is on the rise among large crime rings and among insiders or employees who work in the health care profession and have access to patient records. According to the World Privacy Forum, as many as 250,000 to 500,000 Americans have become victims of this type of identity theft. For further details on medical identity theft and help for consumers and victims, see the World Privacy Forum's report at www.worldprivacyforum.org/medicalidentitytheft.html.

Preventative Measures

1. If someone contacts you by phone, mail, or Internet, don't give out personal information unless you requested to be contacted or are sure you know who you're dealing with. Identity thieves often impersonate corporate agents, government officials, and others to obtain your SSN, mother's maiden name, account numbers, and other identifying information. If you are asked for any type of personal information, ask the caller for his/her name and telephone number and the organization he/she is representing. Hang up and then call the company using the customer assistance number the company provides with your account statement or bill (not the number you were given by the caller). If the call was legitimate, they can connect you to the proper extension. Check an organization's website by typing its URL in the address line, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly.
2. Invest in a paper shredder (they can be purchased inexpensively for $15-20). Shred any mail or other documents containing personal information before discarding in the trash, especially charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers.
3. Don’t leave mail in your mailbox for pickup. Deposit your outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold.

The Postal Service will hold your mail at your local post office until you can pick it up or are home to receive it.

4. Remove your name from mailing lists for credit offers by calling 1-888-5-OPTOUT (1-888-567-8688).
5. Memorize your SSN and don't carry your SSN card. Store it in a secure place.
6. Only give out your SSN only when absolutely necessary, and request other types of identifiers whenever possible, such as on a driver's license or insurance policy number.
7. Carry only the identification information and the credit and debit cards that you'll actually need when you go out.
8. Beware of phony promotional offers which identity thieves use to get your personal information
9. Safeguard your purse or wallet and forms with sensitive information in a safe place at work.
10. When ordering new checks, pick them up from the bank instead of having them mailed to your home mailbox.
11. Don't put any personal information in a web page on the Internet unless it is submitted over a secure connection, as indicated by a closed lock icon in the bottom of your browser window, as well as "https" in the browser window address bar.
12. Never leave receipts at bank machines, bank counters, trash receptacles or unattended gasoline pumps.
13. Memorize your passwords. Do not record them on any cards or on anything in your wallet or purse. Decline when prompted by your computer to store passwords for you.
14. Contact your creditor or service provider if expected bills don't arrive.
15. Never put your credit card or any other financial account number on a postcard or on the outside of an envelope.
16. Destroy all checks immediately when you close a checking account. Destroy or keep in a secure place, any courtesy checks that your bank or credit card company may mail you.
17. Promptly examine and reconcile your check and credit card statements and reports. Immediately dispute any purchases you did not make.
18. Limit the number of credit cards you have, and cancel inactive accounts.
19. Remove your name from mail marketing lists. You may contact Direct Marketing Association by writing to: Mail Preference Service, P.O. Box 282, Carmel, NY 10512 and include a processing fee of $1.00 in the form of a check or money order. You may also opt-out online for a fee of $1.00 at www.dmaconsumers.org.
20. Remove your phone number(s) from telemarketing lists by phoning the FTC's Do Not Call Registry at (888) 382-1222 or registering online at www.donotcall.gov. Many states also have their own do not call registry.
21. Order your Personal Earnings and Benefits Estimate Statement from the Social Security Administration by calling (800) 772-1213. The SSA automatically mails it to individuals three months before the birthday each year. A request form is also available at www.ssa.gov/online/ssa-7004.html.

22. Ensure that your PIN numbers cannot be observed by anyone while using an ATM or public telephone.
23. Closely monitor the expiration dates on your credit cards and contact the issuer if you don't receive a replacement prior to the expiration date. Sign the back of your new card immediately upon receipt.

Online Safety Tips

1. Use virus protection software and keep it updated.
2. Make sure the webpage is sending any personal information you type in with encrypted security software. To determine is the information is encrypted and secure, look at the URL of the page you are on when you are asked to give the personal information. An unsecured URL will look like this: http://www.site.com. A secure server will have an "s" either in front of or following the "http", and it will look like this: https:/ www.site.com or shttp://www.site.com. The bottom of the browser window will also display an icon, showing whether the information is “locked” or “unlocked”. If it is locked, a secure site will also have an icon that appears as locked padlock on the bottom of your browser window. An unlocked insecure site will have an unlocked padlock icon in the same area.
3. Install a spyware protection program and firewall.
4. Download free software only from sites you know and trust. Don’t install software without knowing what it is.
5. In your browser, set the security preferences to at least “medium.”
6. Don’t click on links in pop-up windows or in spam e-mail.
7. Don’t open email attachments from unknown senders.
8. Don’t give out personal information in chat rooms or publicly posted messages.
9. If you shop online, consider using a credit card or bank account that you use exclusively for online purchases.
10. Don’t use the "Remember my Password" function on any website that contains personal or financial information.
11. Clear your cache files after browsing the Internet by going to the "Preferences" folder in your browser and clicking on the "Empty Cache" button. Sometimes this option is in the "Advanced" menu of the browser preferences. In Internet Explorer, go to "Internet Options" from the "Tools" menu and click on "Clear History".
12. Completely log out of sites that contain your financial information, such as an online banking website.

Identity Theft Insurance

The value of identity theft insurance is a matter of personal judgment. It may be purchased as part of some homeowner’s and renter’s insurance policies, as standalone policies, or offers through your credit card issuer. Such insurance covers your out-of-

pocket expenses to clear your name, such as phone bills, lost wages, notary, certified mailing costs, and sometimes attorney fees. However, identity theft isn't going to fix your credit or return the money taken from your accounts through fraudulent transactions. On average, these policies cost between $25 and $50 for $15,000 to $25,000 worth of coverage.

Useful Links

American Association of Retired Persons - http://www.aarp.org/money/wise_consumer/scams/a2002-10-03-WiseConsumerIdentityTheft.html

Annual Credit Report Request Service- http://www.annualcreditreport.com

Better Business Bureau - http://www.bbbonline.org/idtheft/complaint.asp

Federal Bureau of Investigation - http://www.fbi.gov/publications/financial/fcs_report052005/fcs_report052005.htm#e1

Federal Deposit Insurance Corporation - http://www.fdic.gov/consumers/consumer/ccc/theft.html

Identity Theft Resource Center - http://www.idtheftcenter.org/index.shtml

National Consumers League - http://www.nclnet.org/privacy/

National Fraud Information Center - http://www.fraud.org/welcome.htm

Privacy Rights Clearinghouse - http://www.privacyrights.org/identity.htm

Social Security Administration Online - http://www.ssa.gov/pubs/idtheft.htm

United States Department of Justice – http://www.usdoj.gov/criminal/fraud/idtheft.html

United States Postal Inspection Service - http://www.usps.com/postalinspectors/idthft_ncpw.htm


USLEGAL
USLEGALFORMS.COM