

IDENTITY THEFT

How to Prevent It

**What to Do If You
Are a Victim**



www.tn.gov/consumer

www.tn.gov/safety

Tennessee Division of Consumer Affairs

Identity theft happens when someone steals your personal information and uses it without your permission. It is a serious crime that can wreak havoc with your finances, credit history, and reputation.

The Department of Commerce & Insurance's Division of Consumer Affairs and the Department of Safety & Homeland Security have developed this guide to educate Tennessee consumers about the threats and dangers of identity theft. This helpful booklet is designed to assist you in preventing identity theft and to direct you about what to do if you are a victim.

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. Identity thieves could file a tax return in your name and get your refund. In some extreme cases, they might even give your name to the police during an arrest.

We invite you to not only read the information in this guide, but to share the information with your friends and family. We also encourage you visit our websites for helpful links that offer other useful material.

www.tn.gov/consumer and <http://www.tn.gov/safety/cididtheft.shtml>



Table of Contents

How to Prevent Identity Theft

Only Make Purchases on Trusted Sites	1
Order Your Credit Report	1
Know How to Spot Phishing	1
Secure Your Network.....	2
Can the Spam.....	2
Don't Store Sensitive Information on Non-Secure Web Sites.....	2
Set Banking Alerts	2
Don't Reuse Passwords	3
Use Optional Security Questions.....	3
Don't Put Private Information on Public Computers	3

What to Do If You Are a Victim

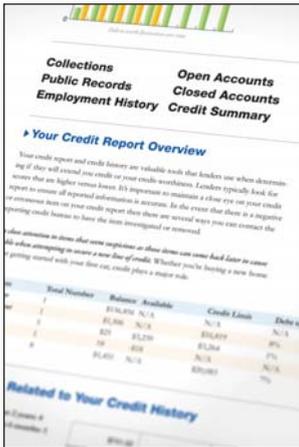
Credit Bureaus	4
Creditors	5
Law Enforcement	5
Stolen Checks	5
ATM Cards	6
Fraudulent Change of Address	6
Social Security Number Misuse	6
Passports	6
Phone Service	6
Driver License Number Misuse.....	6
False Civil and Criminal Judgments.....	7

How to Prevent Identity Theft

Only Make Purchases on Trusted Sites

When deals seem too good to be true, they just may be—you might become a victim of identity theft when you make purchases on Web sites that aren't secure. There are lots of small online retailers that don't have adequately secure payment systems. The best way to make sure that your information doesn't get intercepted is by simply sticking with trusted, well-known online retailers, or smaller sites that use reputable payment processors like PayPal or Google Checkout. Regardless of which site you use, you should always make sure to look for the padlock icon  on the bottom of your browser to verify that the page is safe.

Order Your Credit Report



Your credit report is your window into your ID security. The Fair and Accurate Credit Transactions Act, passed by the Federal government in 2003, mandates that each of the major credit bureaus supply consumers a free copy of their credit report each year. You can get yours at AnnualCreditReport.com (American users only), a Web site run by the credit reporting agencies to comply with this legislation. Your credit report allows you to see whether someone has opened new accounts under your name.

online: AnnualCreditReport.com

phone: 877-322-8228

mail: Annual Credit Report Request Service
P. O. Box 105281
Atlanta, GA 30348-5281

Know How to Spot Phishing

Phishing is a technique used by identity thieves to get your sensitive information by pretending to be a site you trust. Phishing schemes are successful because you believe that you're just signing into your bank or credit card account, when it's really a ploy to get your important information. When



logging into these accounts, make sure that you're not being asked for any information that you usually wouldn't be required to provide to log in. Social security numbers and addresses are often red flags. Also, check the url of the site.

Secure Your Network



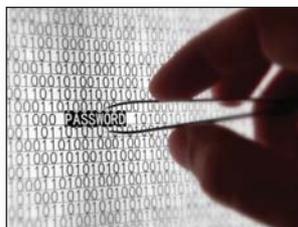
If you have a wireless network at home or work, make sure that you secure it. A hacker can gain access to anything you do over an unsecured network in a matter of seconds. If you look at the documentation for your wireless router, you'll be able to find out how to lock your router and encrypt your information. It won't affect the way you use your wireless network, but it will keep intruders from getting a hold of your information.

Can the Spam

Be very leery of "spam" (or junk e-mail) that works its way into your inbox. Not only are these messages often from phishers, but they can also contain Trojan horses (viruses) that can get into your computer and send your information back to their unsavory creators. If you have the option, install spam-filtering software (or ask your e-mail provider whether it can add spam-filtering to your account). Not only will this cut back on your daily pile of junk e-mail, it can also keep your data safe.

Don't Store Sensitive Information on Non-Secure Web Sites

As more and more useful Web applications start springing up (like Backpack, Facebook and Google Calendars) it's important to make sure that you're not storing sensitive data on non-secure Web sites. While online calendars, to-do lists and organizers are really useful, make sure that your account numbers and passwords don't make their ways onto these sites, which often aren't protected in the same way a banking or brokerage Web site would be.



Set Banking Alerts

Many financial institutions are beginning to offer e-mail and text alerts when your accounts reach certain conditions (being near overdraft, or having

transactions over \$1,000, for example). Setting alerts for your accounts can ensure that you find out about unauthorized access as soon as possible.

Don't Reuse Passwords



As tempting as it may be to reuse passwords, it's a really good practice to use a different password for every account you access online. This way, if someone discovers the password to your credit card account, they will not be able to also access your checking, brokerage and email accounts. It may take a little more organization to use different passwords for each site, but it can help marginalize the effects of unauthorized access to your accounts.

Use Optional Security Questions

As with using different passwords for each account, it's a good idea to set up optional security questions to log into your accounts. Many financial institutions ask security questions that a third party wouldn't know, but you can often set up multiple optional questions that can increase the security of your account. Remember to use questions that don't have answers available by public record. For example, choose questions such as "What was the color of your first car?" over "What city were you born in?"

Don't Put Private Information on Public Computers

If you're away from home, make sure not to save private information onto a computer used by the public. If you're accessing a private account at the library or cyber cafe, make sure to log out completely from your accounts, and never choose to save login information (like your username or password) on these computers.

These days, identity theft has become commonplace, and people are even afraid to use their own personal computers to access any financial information or purchases online. You can do those things without being taken advantage of by making sure that you keep yourself safe online.



What to Do If You Are a Victim

This guide provides victims of identity theft with the major resources to contact. Victims themselves have the ability to assist greatly with resolving their case. It is important to act quickly and assertively to minimize the damage.

In dealing with the authorities and financial institutions:

- Keep a log of all conversations, including dates, times, names, and phone numbers.
- Note the time spent and any expenses incurred.
- Confirm conversations in writing.
- Send correspondence by certified mail (return receipt requested).
- Keep copies of all letters and documents.



Once you discover you are a victim of identity theft you should notify the following:

Credit Bureaus — Immediately call the fraud units of the three credit reporting companies - Experian, Equifax, and Trans Union. Report the theft of your credit cards or numbers. The phone numbers are provided at the end of this brochure. Ask that your account be flagged. Also, add a victim's statement to your report, up to 100 words. ("My ID has been used to apply for credit fraudulently. Contact me at (your telephone number) to verify all applications.") Be sure to ask how long the fraud alert is posted on your account, and how you can extend it if necessary.

Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter. Ask the credit bureaus in writing to provide you with a free copy every few months so you can monitor your credit report.

Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been

opened. Ask the credit bureaus to remove the 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) in order to alert them to the disputed and erroneous information.



Creditors — Contact all creditors immediately with whom your name has been used fraudulently by phone and in writing. Get replacement cards with new account numbers for your own accounts that have been used fraudulently. Ask that old accounts be processed as “account closed at consumer’s request.” (This is better than “card lost or stolen” when this statement is reported to credit bureaus, it can be interpreted as blaming you for the loss.) Carefully monitor your mail and credit card bills for evidence of new fraudulent activity. Report it immediately to credit grantors.

Creditors are required to report fraud. You may be asked by banks and credit grantors to fill out and notarize fraud affidavits, which could become costly. The law does not require that a notarized affidavit be provided to creditors. A written statement and supporting documentation should be enough (unless the creditor offers to pay for the notary.)



Law Enforcement — Report the crime to the law enforcement agency with jurisdiction in your case. Give them as much documentary evidence as possible. Get a copy of your police report. Keep the report number of your police report handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report to verify the crime. Some police departments

have been known to resist writing reports on such crimes. Prior to January 1, 1998, the creditors (credit card companies, banks, etc.) were the only “legal” victims of Credit Fraud/Identity Theft. California Penal Code Section 530.5 went into effect on January 1, 1998, thus giving legal standing to individual victims. Some police departments have not yet received training in the new laws of Identity Theft. Be persistent!

Stolen Checks — If you have had checks stolen or bank accounts set up fraudulently, report it to the check verification companies. Put stop payments on any outstanding checks that you are unsure of.



Cancel your checking and savings accounts and obtain new account numbers. Give the bank a secret password for your account (not your mother’s maiden name).



ATM Cards — If your ATM card has been stolen or is compromised, get a new card, account number, and password. Do not use your old password. When creating a password, don’t use common numbers like the last four digits of your social security number or your birth date.

Fraudulent Change of Address — Notify the local Postal Inspector if you suspect an identity thief has filed a change of address with the post office or has used the mail to commit credit or bank fraud. Find out where the fraudulent credit cards were sent. Notify the local Postmaster for the address to forward all mail in your name to your own address. You may also need to talk to the mail carrier.

Social Security Number Misuse — Call the Social Security Administration to report fraudulent use of your social security number. As a last resort you might want to change the number. The SSA will only change it if you fit their fraud victim criteria. Also order a copy of your Earnings and Benefits Statement and check it for accuracy.

Passports — If you have a passport, notify the passport office in writing to be on the lookout for anyone ordering a new passport fraudulently.



Phone Service — If your long distance calling card has been stolen or you discover fraudulent charges on your bill, cancel the account and open a new one. Provide a password that must be used anytime the account is changed.



Driver License Number Misuse — You may need to change your driver license number if someone is using yours as identification on bad checks. Call the state office of the Department of Safety’s Driver License Division to see if another license was issued in your name. Put a fraud alert on your license. Go to the nearest local Driver License Station to request a new number. Also, fill out the driver license complaint form to begin the fraud investigation process. Send

supporting documents with the complaint form to the Criminal Investigation Division of the Department of Safety.

False Civil and Criminal Judgments — Sometimes victims of identity theft are wrongfully accused of crimes committed by the imposter. If a civil judgment has been entered in your name for actions taken by your imposter, contact the court where the judgment was entered and report that you are a victim of identity theft. If you are wrongfully prosecuted for criminal charges, contact the state Department of Justice and the FBI. Ask how to clear your name.





Tennessee Division of Consumer Affairs

500 James Robertson Parkway, 12th Floor
Davy Crockett Tower
Nashville, TN 37243
615-741-4737

www.tn.gov/consumer



Complaint Form



Contact Us



Department of Commerce and Insurance, Authorization No. 335410, 7,500 copies, May 2013. This public document was promulgated at a cost of \$.54 per copy.

The cost for this publication came from a reserve fund at no cost to Tennessee taxpayers.