

Act immediately...

1. If you think an identity thief is using your SSN, call the Social Security Fraud Hotline at 1-800-269-0271.
2. Call the three national credit reporting organizations immediately after the theft of a purse or wallet to place a fraud alert on your name and SSN. The alert means any company that checks your credit knows your information was stolen and they have to contact you by phone to authorize new credit.
 - Equifax 1-800-525-6285
 - Experian 1-800-397-3742
 - Trans Union 1-800-680-7289

And if it happens...

If you are the victim of identity theft, you can find many resources for help. One CSU employee found the following book particularly helpful when she faced identity theft...

From Victim to Victor: A step-by-step guide for ending the nightmare of identity theft, Second Edition with CD by Mari J. Frank, ISBN: 1-892126-04-4

Information provided by the following brochures: *Protect Yourself Against Identity Theft* by the Ohio Attorney General's Office, *10 Tips for Identity Theft Prevention* from the Office of Privacy Protection of the California Department of Consumer Affairs, and a generally-distributed email with the subject of *Good Advice from an Attorney*.

Identity Theft Statistics...

Approximately 7 million people became victims of identity theft in the prior 12 months. That equals 19,178 per day, 799 per hour, 13.3 per minute.

Victims now spend an average of 600 hours recovering from this crime, often over a period of years.

Even after the thief stops using the information, victims struggle with the impact of identity theft. That might include increased insurance or credit card fees, inability to find a job, higher interest rates and battling collection agencies and issuers who refuse to clear records despite substantiating evidence of the crime.

Today victims spend an average of \$1,400 in out-of-pocket expenses, an increase of 85% from years past.

Approximately 85% of victims found out about the crime due to an adverse situation – denied credit or employment, notification by police or collection agencies, receipt of credit cards or bills for merchandise never ordered, etc. Only 15% found out through a positive action taken by a business group that verified a submitted application or a reported change of address.

The emotional impact on victims is likened to that felt by victims of more violent crime, including rape, violent assault and repeated battering. Some victims feel dirty, defiled, ashamed and embarrassed, and undeserving of assistance. Others report a split with a significant other or spouse and of being unsupported by family members.

Above statistics are from: Identity Theft Resource Center, a national non-profit organization that focuses exclusively on identity theft – www.idtheftcenter.org

CSU is an Affirmative Action/Equal Opportunity Institution
Rev. 05/14

STUDENTS, FACULTY & STAFF

Identity Theft

*Protect Yourself
Protect Your Future*

engaged
learning™

Cleveland State
University
Information Services and Technology



A TOO COMMON STORY...

Charlene's wallet had been stolen out of her purse. "Where could it have happened?" she thought. "Work? Grocery shopping? Getting gas?" However it happened, it was gone.

Before she had a chance to cancel her credit cards, the thief had used them to order an expensive monthly cell phone package, applied for a VISA credit card, had a credit line approved to buy a Gateway computer, received a PIN number from the BMV to change her driving record online, and more. It took Charlene a lot of time and work to straighten out the mess and get her credit rating fixed.

Can this happen to you? Sure. In fact, it's probably happened to some people reading this article.

So what can you do to better protect yourself from these kinds of problems? Here's a shopping list, in no particular order, of things you can do to protect your identity from being stolen and minimize the damage if it has been.

When you are out...

1. Don't carry you SSN card with you.
2. Reduce the number of credit cards you actively use. Carry only one or two credit cards.
3. Always take credit card and ATM receipts with you. Never toss them in a public trash container.
4. File a police report immediately in the jurisdiction where your purse or wallet was stolen; this proves to credit providers that you were diligent and is a first step toward an investigation (if there ever is one).
5. Shield your hand when using your PIN at a bank ATM or when making long-distance phone calls with your phone card to prevent others from seeing your code.

Protect your PC use...

1. Protect your personal information on your home computer. Use strong passwords with at least eight characters, including a combination of letters, numbers, and symbols that are easy for you to remember but difficult for others to guess.

2. Protect yourself from spyware; download free software only from sites you know and trust.
3. Don't install software without knowing what it is.
4. Set Internet Explorer browser security to at least "medium".
5. Don't click on links in pop-up windows or in spam e-mail.
6. When shopping online, check out a website before entering your credit card number or other personal information. Read the privacy policy and look for opportunities to opt out of information sharing. If there is no privacy policy posted, beware! Shop elsewhere.
7. Only enter personal information on secure web pages with "https" in the address bar and a padlock symbol at the bottom of the browser window. These are signs that your information will be encrypted during transmission, protecting it from hackers and thieves.

When asked for personal info...

1. Don't give out your personal information unless YOU make the contact. Scam artists "phish" for victims by pretending to be banks, stores or government agencies. They do this over the phone, in emails, and in regular mail.
2. Don't respond to a request to verify your account number or password. Legitimate companies will not request this kind of information in this way.
3. Ask questions whenever you are asked for personal information that seems inappropriate for the transaction. Ask how the information will be used and if it will be shared. Ask how it will be protected. Explain that you're concerned about identity theft. If you're not satisfied with the answers, consider going somewhere else.

Prepare yourself...

1. The next time you order checks, have only your first initial and last name printed on them. Anyone stealing your checkbook will not know if you sign your checks with just your initials or your first name, but your bank will know how you sign your checks.
2. Put your work phone number on your checks instead of your home phone. If you have a PO Box, use that instead of your home address. Never have your SSN printed on your checks!

3. When writing checks to pay on your credit card accounts, DO NOT put the complete account number on the "For" or "Memo" line. Instead, just put the last four digits. The credit card company knows the rest of your number and anyone who might be handling your check as it passes through the check processing channels won't have access to it.
4. Place the contents of your wallet on a photocopy machine and copy both sides of your license, credit cards, etc. You will know what you have in your wallet, all your account numbers, and the toll free phone numbers to call to cancel. It's important that you store the photocopy in a very secure place!
5. Shred your papers with personal information before you throw them away. Shred credit card offers and "convenience checks" that you don't use.
6. Open your bills and bank statements right away. Carefully check for any unauthorized charges or withdrawals and report them immediately. Call if bills don't arrive on time. It may mean that someone has changed contact information to hide fraudulent charges.
7. Cancel all unused credit card accounts. Even though you do not use them, their account numbers are recorded in your credit report, which is full of data that can be used by identity thieves.
8. Request in writing that any of your credit card issuers remove you from receiving convenience checks. These checks are easy for identity thieves to steal and use.
9. Memorize all your passwords and PINS. Do not write them on anything in your wallet or purse.
10. Stop most pre-approved credit card offers. They make a tempting target for identity thieves who steal your mail. Have your name removed from credit bureau marketing lists. Call 1-888-5OPTOUT (888-567-8688).
11. One of the best ways to protect yourself from identity theft is to monitor your credit history. You can get one free credit report every year from each of the three national credit bureaus (see #2 of "Act immediately..." below for the names and phone numbers). You can request all three reports at once, or you can be your own no-cost credit-monitoring service by spreading out your requests, ordering from a different bureau every four months.