Protecting your identity

Though it might not seem like it, your identity is one of the most precious things you possess. Criminals who are able to steal your identifying information can pretend to be you, buying things on accounts that you own or are under your name. This leaves you getting their bills! It can also create problems with your credit reports and scores.

Identifying information is anything that is specifically unique to you, such as your:

- Credit card and bank account numbers
- Driver's license number
- Date, city, and state of birth
- Social security number
- Passwords or PIN numbers

Many people think that identity theft happens primarily online, and if you don't shop online, you are safe. The reality is that most identity thefts take place offline—just the opposite of what many people think. In addition, in over half of the cases of identity theft, the thief is someone that the victim knows. Because of this, it's important to be cautious with your identifying information–both online and in the real world.

✔	**Steps to protect your identity**
Check your credit report	
	Remove your name from all three credit bureaus' (Equifax, Experian, and TransUnion) mailing lists by calling to opt-out at (888) 567-8688 or online at http://www.optoutprescreen.com – choose "forever" removal option. This prevents prescreened offers from falling into other people's hands.

	Check your credit at all three credit agencies each year using the free https://www.annualcreditreport.com. If you see anything that is incorrect or suspicious, contact them immediately. (See *Module 12: Understanding Your Credit Reports and Scores* for more information).
Limit access to your information	
	Don't carry your Social Security card or number in your wallet or purse.
	Remove your name from many direct mail marketers' lists by registering with the *Direct Marketing Association* online form at http://www.dmachoice.org. Removing your name from marketers' lists will create fewer opportunities for thieves to steal your information.
	Remove yourself from most telemarketers' lists by registering your phone number with the *Do Not Call Registry* at (888) 382-1222 or at http://.www.donotcall.gov. Numbers registered after February 2008 remain permanently on the National Do Not Call Registry.
	Never give your personal information to someone who calls you and asks for it, even if they say there are from your financial institution.
	Use a shredder, scissors, or your hands to tear all papers with identifying information or account numbers into tiny pieces before throwing them out.
	Give out your Social Security number only when absolutely necessary. Often when someone asks for it, you are not required to give it to them.
Practice online security	
	Commit all passwords to memory. Never write them down or carry them with you (not even on a post-it by your computer!).
	Make sure passwords include upper- and lower-case letters, numbers, and do not include any words that can be found in a dictionary or names and dates that can be associated with you (your children's names and birthdates, for example). Longer passwords are better. The best practice is to have a different password for each account. If you find it too hard to keep track of so many passwords, have separate, longer, harder-to-guess passwords for your financial accounts than for ordinary uses like your e-mail.
	Don't give out your financial or personal information over the Internet, unless you have initiated the contact or know for certain who you are dealing with.
	Never share identity information online unless the site is ***secure*** with an encryption program so no one can intercept your information. **If secure, the web site address will start with https, not http**. There will also be a lock icon (🔒) in front of the web address.

	Do not reply to emails asking for personal banking information, **even if they have a bank or PayPal logo! Financial Institutions will never ask for personal information via email.**

According to the Federal Trade Commission (FTC), identity protection means treating your personal information like cash or a valuable commodity—being careful not to leave it around, and being thoughtful about who is asking for it, why they need it, and how they're going to safeguard it for you.

This is the FTC's list of common red flags that your identity has been stolen:

- There are mistakes on your bank, credit card, or other account statements.
- There are mistakes on the explanation of medical benefits from your health plan.
- Your regular bills and account statements don't arrive on time.
- You get bills or collection notices for products or services you never received.
- You receive calls from debt collectors about debts that don't belong to you.
- You get a notice from the IRS that someone used your Social Security number.
- You receive mail, email, or calls about accounts or jobs in your minor child's name.
- You receive unwarranted collection notices on your credit report.
- Businesses turn down your checks.
- You are turned down unexpectedly for a loan or job.

If you determine your identity has been stolen, the FTC recommends the following steps:

1. Place a fraud alert on your credit file

Call one of the nationwide credit reporting agencies, and ask for a fraud alert on your credit report. The company you call must contact the other two so they can put fraud alerts on your files. An initial fraud alert is good for 90 days. If you want to place an extended alert on your credit report after your identity has been stolen, you must file either a police report or a report with a government agency such as the FTC, known as an "identity theft report." An extended alert is good for seven years. An extended alert requires that the creditor contact you in person

or through the telephone number or other contact method you designate to verify whether you are the person making the credit request.

- **Equifax:** (800) 525-6285
- **Experian:** (888) 397-3742
- **TransUnion:** (800) 680-7289

2. Consider a security freeze

You can also place a "freeze" on your credit report. A security freeze means that potential new creditors cannot access your credit report. Only a limited number of entities can see your file while a freeze is in place, including existing creditors, certain government entities like child support agencies, and companies that monitor your credit file at your direction to prevent fraud. Because most businesses will not open credit accounts without checking your credit report, a freeze can deter identity thieves from opening new accounts in your name. Be mindful that a freeze does not prevent identity thieves taking over existing accounts. Credit reporting agencies may charge for this service. In some states, identity theft victims are not charged to place a security freeze.

3. Order your credit reports

Each company's credit report about you is slightly different, so order a report from each company. When you order, you must answer some questions to prove your identity. Read your reports carefully to see if the information is correct. If you see mistakes or signs of fraud, contact the credit reporting company.

4. Create an identity theft report

An Identity Theft Report can help you get fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name. To create an Identity Theft Report, first file a complaint with the FTC at ftc.gov/complaint or (877) 438-4338; TTY: (866) 653-4261. Your completed complaint is called an FTC Identity Theft Affidavit. Next, you can take your FTC Affidavit to your local police, or to the police where the theft occurred, and file a police report. Get a copy of the police report. The two documents comprise an Identity Theft Report.

For more information from the Federal Trade Commission, visit:
http://www.consumer.ftc.gov/features/feature-0015-identity-theft-resources.