GREENPATH FINANCIAL WELLNESS SERIES

IDENTITY THEFT

"Through financial knowledge and expertise, we provide high-quality products and services that enable people to enjoy a better quality of life."

Family First
CREDIT UNION
Your Trusted Financial Partner

GreenPath
debt solutions

> “Smart financial planning — such as budgeting, saving for emergencies, and preparing for retirement — can help households enjoy better lives while weathering financial shocks. Financial education can play a key role in getting to these outcomes.”
>
> – *Ben Bernanke, an American economist and currently chairman of the Federal Reserve, the central bank of the United States*

TABLE OF CONTENTS

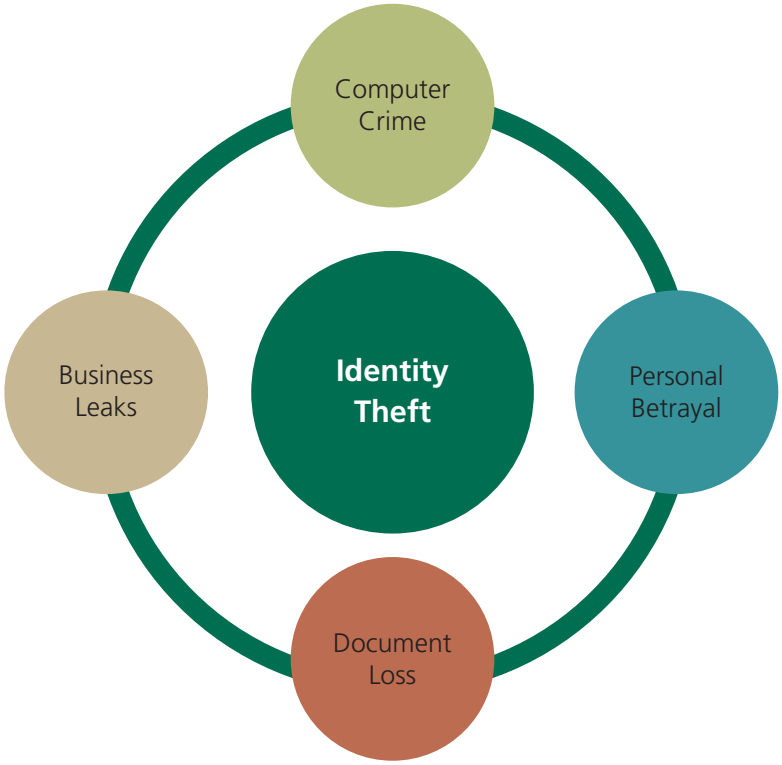
CHECK YOUR KNOWLEDGE

Look for this icon throughout the workbook for important information.

WHAT IS IDENTITY THEFT?

Unfortunately, most people don't consider this question until after they have been a victim of identity theft. Identity theft is a serious and growing crime. An identity thief takes some piece of your personal or financial information and uses it by posing as you and stealing from you by performing financial transactions in your name without your knowledge. A thief may charge items to your existing account and/or open new accounts, credit cards or other fraudulent accounts in your name. Each year, millions of Americans are affected and it can occur in many different forms:

- Computer crime – This occurs when data is stolen from you during your online activities.
- Personal betrayal – This occurs when a friend, relative, employee or stranger steals your data.
- Document loss – This occurs when you lose your wallet, checkbook or credit cards or your mail or trash is stolen.
- Business leaks – This occurs when your personal files are stolen and exploited from a place where you have conducted business.

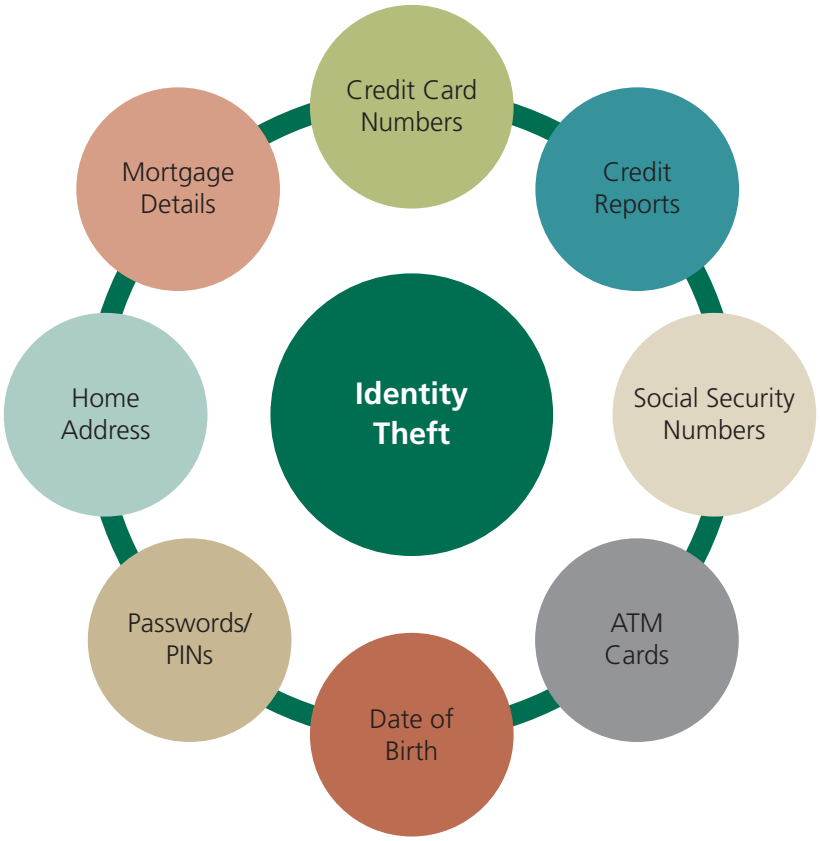


As much as we want to trust that our personal information is safe, it is not wise to assume that it is. There are steps that you can take to safeguard your identity.

A criminal will purchase merchandise online with stolen credentials and have it delivered to a motel. The criminal tracks the delivery status online and meets the driver in the parking lot of the hotel when the driver arrives so the delivery cannot be tracked to a room number or person. The thief then sells the merchandise immediately.

HOW IDENTITY THEFT OCCURS

An identity thief obtains some piece of your personal information without your knowledge and uses it to commit fraud or theft. Some examples of information that thieves want:

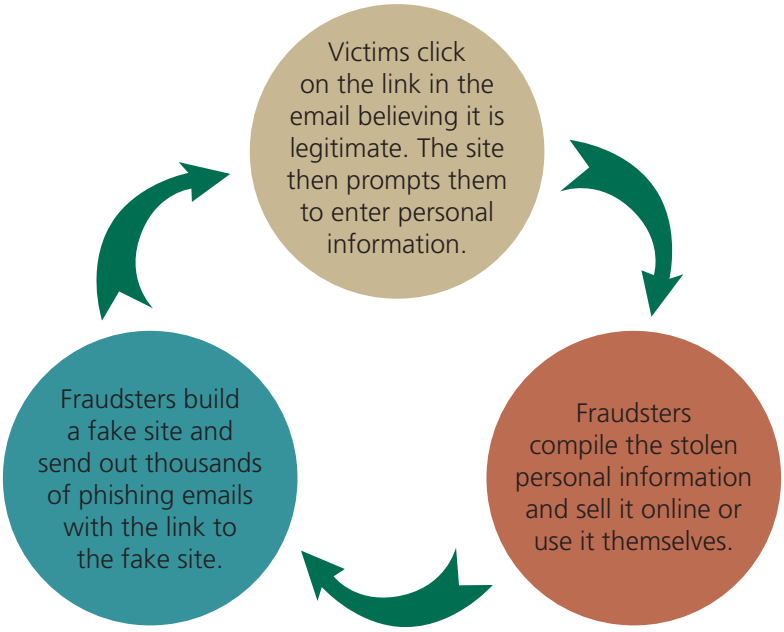


Identity thieves will steal your personal information in a variety of ways. Thieves will:

- Steal wallets, backpacks, briefcases, purses and smartphones.
- Steal your mail, both incoming and outgoing.
- "Dumpster Dive," which occurs when the trash at your house or at work is rummaged through for personal information.
- Steal your vehicle that contains your registration and insurance card.
- Rob your house or business.
- Scam you through email by posing as legitimate companies, government agencies or people in need.
- Lurk at ATMS to pick off PINs. Also called "shoulder surfing."
- Steal your credit card numbers through "skimming" which occurs as your card is processed using a small information storage device that can read the magnetic strip on the back of credit cards.

Another way to verify that you are on a secure website is to look for a padlock on the bottom of your browser or task bar. A locked padlock indicates that the site is secure and that there is an encrypted connection. If the padlock is open, or unlocked, it indicates that the connection is unsecure and you should not enter any personal information.

PHARMING	
What is it:	Pharming is a process that steals information from unsuspecting internet users.
Two major components:	1. Pharmers direct users to fraudulent commercial web sites and capture personal data entered by users. 2. Pharming is more dangerous than phishing because criminals can steal personal information from internet users who are completely unaware of their vulnerability.
What you can do:	1. Delete unknown email messages and don't download attachments or click on links included in the email. 2. Don't send personal or financial information via email. 3. Make sure you are on a secure, encrypted website. A secure site is usually designated by the URL beginning with "https" where the "s" stands for secure.



PHISHING	
What is it:	Phishing is a practice that online fraudsters use to "fish" for confidential passwords and financial data from the "sea" of internet users using email.
Two major components:	1. Spoofing occurs when thieves create a near exact replica of an existing website. 2. Spamming occurs when you receive unsolicited email also known as junk email.
What you can do:	1. Be aware of where you are on the internet. Are you on the site you thought you were? 2. Don't be complacent about security. 3. Don't allow convenience to get in the way of security.

Use caution when clicking on a link to get to a website. You will always want to verify the address after you arrive on the site, or before clicking on the hyperlink. For example — if someone were spoofing a site, such as "www.google.com" it may show as "www.lygoogle.com" in the address bar once you click on the link. The idea is to replicate the site so just by looking at the content on the screen you wouldn't be able to tell it is fake. The best way to avoid this is to directly type the website into the address bar, rather than clicking on any links that could potentially be stealing information from you.

HOW IDENTITY THIEVES USE YOUR INFORMATION

Identity thieves will use your personal information in a number of ways. Thieves will:

- Use your existing credit and debit card account numbers to buy merchandise that they can re-sell easily.
- Open new credit accounts. They will use the accounts and won't pay the bills, while the delinquent accounts appear on your credit report.
- Establish phone or wireless service in your name.
- Open bank accounts and write bad checks.
- Take out loans and buy consumer goods, such as a vehicle in your name.

HOW TO PROTECT YOURSELF

Nearly everyone is vulnerable to identity theft because there is so much personal information out there. If you have ever applied for a credit card, credit line or loan, attended college or had a job, had a savings account or checking account, or had medical insurance with an employer, you are at risk.

You can minimize your risk by aggressively managing your personal information and through continual awareness of the problem. There are many ways in which you can protect yourself against identity theft:

Your Social Security Number – The Key to Your Castle

- Do not carry your SSN with you
- Keep your Social Security card in a secure location like a safe at home
- Give your SSN only when it is absolutely necessary (i.e. your employer will need it for wage and tax reporting)
- Check your Social Security earnings and benefit statement each year for fraud
- Never put your SSN on your checks
- Ask the following questions if someone asks you for your SSN: (the answers you receive will help to determine if you want to continue doing business with them)
  - Why do you need it?
  - How will it be used?
  - How do you protect it from being stolen?
  - What will happen if I don't give it to you?
  - What law requires me to give you my SSN?

Passwords – As Good As Gold

- Be smart about choosing a password. Do not use easily identifiable information such as; mother's maiden name, address, date of birth or your telephone number. Experts say to create a strong password you should use the following criteria:
  - At least eight characters
  - Significantly different from previous passwords
  - Contains a mix of upper and lowercase letters, numbers and characters
  - Does not contain a complete word
  - Does not contain your user name or real name
- Store your passwords in a safe place such as a safe at home
- Don't write them down and carry them with you

Technology – Be on the Lookout

- Pay your bills online. The odds of identity theft are lower when you pay your bills online compared to paying them offline
- Update the virus protection software regularly on your home computer
- Avoid using the automatic log-in feature offered on online services that saves your username and password
- Read privacy policies
- Use a secure browser to guard the privacy of your online transactions
- Don't download files from strangers or click hyperlinks from people you don't know. If you get an email from a friend with just a link, or something seems odd, contact your friend before clicking on anything or entering any personal information into the email as they could have been hacked
- Avoid using the automatic log-in feature offered for online services
- Have a passcode on your smart phone

At Home – Manage Your Personal information

- Buy a crosscut shredder and destroy bills, pre-approved credit offers, and other documents with personal information
- Don't leave personal information in plain view where roommates, relatives or outside help can see it
- Stay on top of your finances, especially bill due dates

- Report any questionable charges on your bills
- Don't put your credit card number or account number on checks when you pay your bills by mail
- Sign and activate new credit cards immediately. Cut up and throw away expired credit cards
- Guard your mail. If you can, take any outgoing mail to the post office or in an official blue postal service collection box
- Guard your trash by keeping your trash cans in a locked area if possible
- Make a copy of all your financial, personal and insurance cards and identification that you carry in your wallet and keep them in a safe place at home
- Order a credit report once a year from each of the three major credit bureaus, Equifax, Experian and TransUnion to verify that the information is accurate
- Review financial statements regularly and close any unused accounts

When You Are Out and About

- Carry only the information that you actually need. Get rid of any identifying information that you don't need in your wallet
- Always secure your Automated Teller Machine (ATM) card, Personal Identification Number (PIN) and ATM receipts

At Work – Practice Security and Question Everything

- If you are a business traveler and you use your laptop when you are in a hotel room, turn off the laptop when you step out of the room
- Affix a privacy screen to your laptop to avoid the snooping eyes of those sitting next to you
- Always shut off the wireless internet on your laptop when you're not using it. This can deter "Evil Twins" which masquerade as hotspots by sending out strong signals to steal passwords and personal information

In summary, make sure you protect what you can control as best you can. The best offense is a good defense. Be aware of identity theft, keep close track of your information and report any suspicious activity immediately.

ARE YOU A VICTIM OF IDENTITY THEFT?

Sometimes you find out that you have been the victim of identity theft at the most inopportune time. For example, a lost job opportunity, a loan denial or even an arrest may be the first clue that you have been a victim.

Some of the most common ways to know if you have been a victim include:

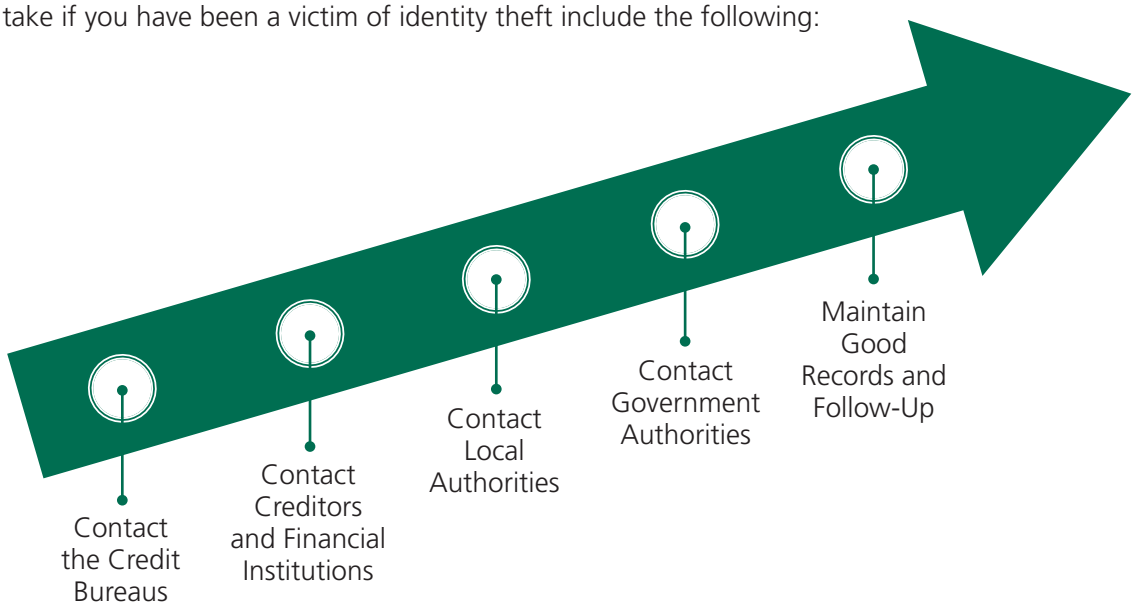
- Unexplained charges or withdrawals on your checking or savings account
- Failing to receive bills or other mail which may indicate a thief did an address change and your mail is now being mailed to the thief's designated address
- Receiving credit cards that you did not order
- Being denied credit for no apparent reason
- Receiving collection calls from creditors and debt collectors for bills that are not yours
- Finding inaccuracies on your credit reports that are not the result of human errors

One thief stole a mortgage loan application from the purse of a consultant who was attending a trade show. The consultant had been working on the application during down time at the trade show and after it was completed, the thief snatched it.

TAKE ACTION IF YOUR IDENTITY IS STOLEN

If you have been a victim of identity theft, you must find out how many of your records have been compromised. Some of the locations of your records are more common than others. The more commonly known databases include: credit bureaus, local and state police and the division of motor vehicles. It's also possible for your personal information to show up on federal watch lists because of criminal activity of the identity thief, fraudulent banking activity lists, and/or unknown addresses affiliated with your SSN.

If you become a victim of identity theft, act quickly to restore your good name. The steps to take if you have been a victim of identity theft include the following:



STEP 1: Contact the Credit Bureaus	• Ask the credit bureaus – Equifax, Experian and TransUnion – to place a fraud alert on your credit report. • Review your credit reports carefully. • Extend the fraud alert beyond the standard 90 days to seven years by writing each of the bureaus and include a copy of the police report that you have filed.
STEP 2: Contact Creditors and Financial Institutions	• Close any accounts that have been tampered with or opened fraudulently. • If you are disputing inaccuracies on your existing accounts, ask the company for their fraud dispute form.

STEP 2: Contact Creditors and Financial Institutions (Continued)	• Stop payment on any outstanding checks if your checks have been stolen or misused. • Create new Personal Identification Numbers (PINs) for your new accounts and place the PINs in a secure location.
STEP 3: Contact Local Authorities	• File a police report with the local police department where the identity theft occurred.
STEP 4: Contact Government Authorities	• The Federal Trade Commission (FTC) – file a complaint by contacting the Identity Theft Hotline: *www.ftc.gov*. • Social Security Administration (SSA) – if it appears that someone is using or has used your Social Security Number. • U.S. Postal Service – If your mail is being tampered with or being stolen. • Contact your state's Department of Motor Vehicles to report a lost driver's license.
STEP 5: Maintain Good Records and Follow-Up	• Document all of your actions including the time and money you spend on straightening out your identity. In some states, any person found guilty of financial identity theft will be ordered to pay restitution to the victim for any financial loss, including lost wages. • Keep copies of correspondence and documents related to the theft and make note of all telephone calls, including the date and time of your call and the name and title of the person who assisted you. • Follow-up all phone calls in writing. • Obtain a copy of your credit report again in a few months to verify that your corrections and changes have been made and to make sure no new fraudulent activity has occurred.

Fortunately, there are steps you can take when your identity has been stolen. If you manage your personal information with caution on a consistent basis, you can guard yourself against identity theft in the future.

A very cautious consumer had his identity stolen and he had no idea how it happened. He always shredded documents before throwing them away. He delivered his outgoing mail to the post office. And yet, when he checked his credit report, he found $15,000 of unauthorized charges on credit cards that he didn't use regularly. This is why it's important to review monthly statements from creditors and your credit reports regularly to check for inaccuracies.

Identity Theft and the Laws that Protect You

Resolving credit problems that occur from identity theft can be time consuming and frustrating. There are protections under federal law for correcting credit reports and billing errors. There is also a federal law that protects you from being contacted by collectors about debts you don't owe. Federal laws have also been passed specifically targeting identity theft.

Fair and Accurate Credit Transactions Act (FACT Act) of 2003

- This act gives every consumer the right to their credit report free of charge every year.
- Requires merchants to leave all but the last five digits of a credit card number off the store receipts.
- Creates and establishes a national system of fraud detection and alerts for consumers.
- Creates a Disposal Rule stating that any person who maintains or otherwise possesses consumer information for a business purpose must properly destroy the information prior to disposal.

Identity Theft and Assumption Deterrence Act of 1998

- This federal law makes it a federal crime when someone transfers or uses another persons' means of identification without a lawful reason to do so and with the intent to commit a crime.

Identity Theft Penalty Enhancement Act

- This law provides greater penalties for identity thieves.
- It creates the crime of "aggravated identity theft" punishable by up to two years in prison when committed in connection with other felonies.

Fair Credit Billing Act

- This act gives you particular rights when dealing with billing errors.

The Electronic Fund Transfer Act

- This act establishes procedures for resolving mistakes on electronic fund transfer account statements.

Fair Credit Reporting Act

- This act is designed to promote the accuracy, fairness and privacy of information in the files of every Consumer Reporting Agency (CRA), the most common of which is a credit bureau.

No federal law limits your losses if someone steals your checks and forges your signature. However, a state law may protect you. Contact your state banking or consumer protection agency for more information.

MONITORING YOUR CREDIT TO PROTECT AGAINST BEING A VICTIM

Monitoring your credit should be a key component in your personal financial plan.

It is important that you understand the information in your credit report, regardless of your financial situation. This information directly impacts your ability to obtain a credit card, buy a car or home, rent an apartment, or even get a new job. Two of the best reasons for reviewing your credit report today are to make sure your credit report is accurate and to protect yourself from fraud or identity theft.

You can create your own free ongoing monitoring system by getting one of your free credit reports every four months.

For example:

1. In January, order your Experian report from *annualcreditreport.com*.
2. Then in May, order your TransUnion report.
3. And finally, in September, order your Equifax report before starting the process again in January.

Since all three bureaus have most of the same information, you will be able to monitor the activity on your credit reports and identify questionable items.

CREDIT BUREAUS				
To order your credit report:	Phone:	Website:	Address:	To report fraud call:
Experian	888-EXPERIAN	www.experian.com	PO Box 9532 Allen, TX 75013	888-EXPERIAN
TransUnion	800-916-8800	www.transunion.com	PO Box 1000 Chester, PA 19022	800-680-7289
Equifax	800-685-1111	www.equifax.com	PO Box 740241 Atlanta, GA 30374	800-525-6285

When it comes to your personal information, caution and prudence are the words of the day.

A business traveler checked into a hotel and used his personal credit card by mistake. He didn't realize the mistake until after the clerk had swiped his card and had a print out with the full account number. His business card was then processed to pay for the hotel stay. Over the next few days, more than $1500 of merchandise was fraudulently purchased on his personal credit card. The fraud was discovered by the credit card issuer that identified unusual activity on the card and cancelled the card. It's important to make sure any documents that have a full credit card or account number are placed in a secure shredding bin and not left out in the open.

NOTES

NOTES

GreenPath®
debt solutions

36500 Corporate Drive
Farmington Hills, MI 48331
248-553-5400 fax: 248-553-8970
www.greenpath.org

GreenPath UNIVERSITY

Accel®
Members Financial Counseling

Búsqueda greenpathdebt