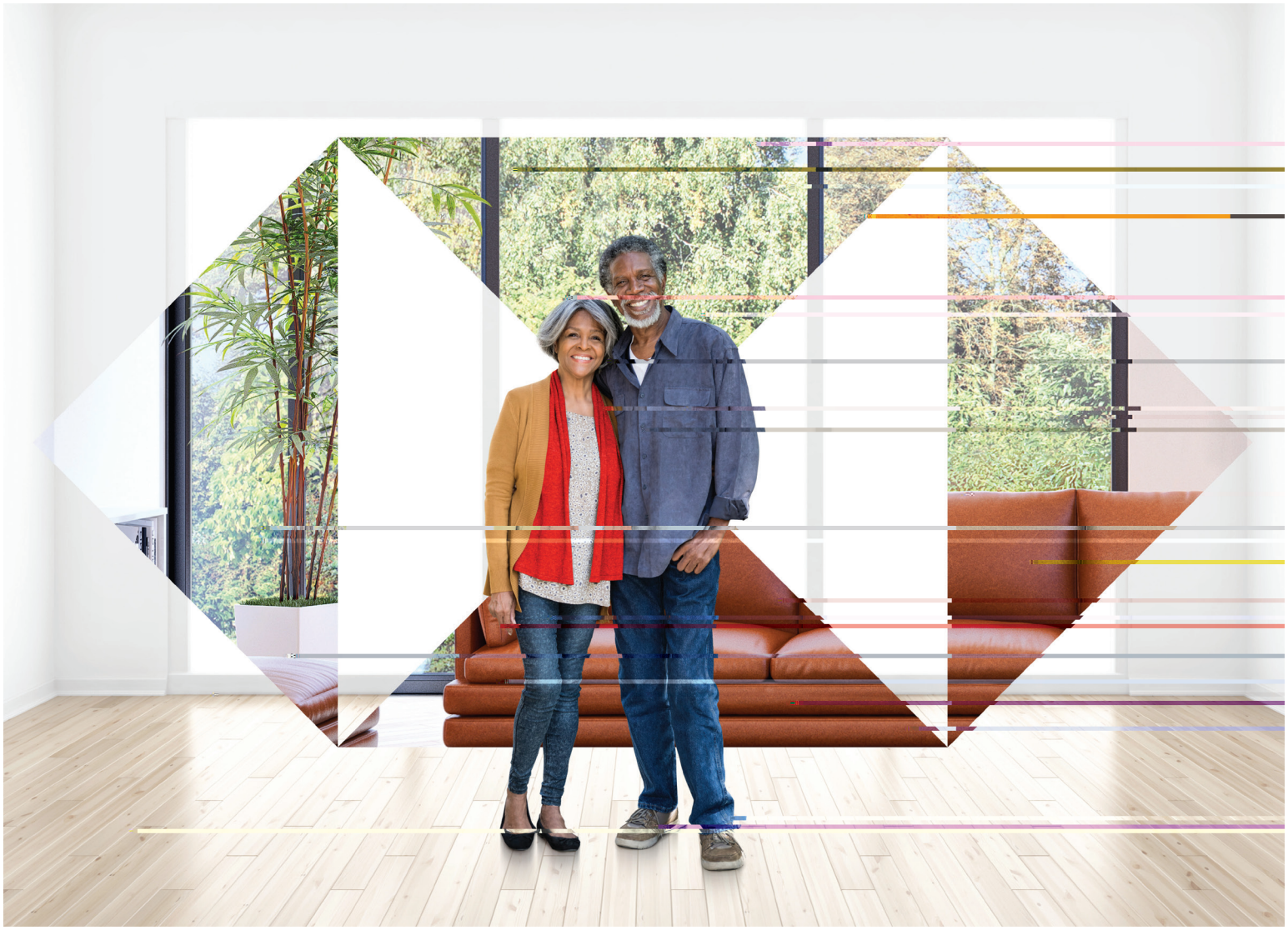


YOUR MONEY COUNTS
IDENTITY THEFT

HSBC Bank

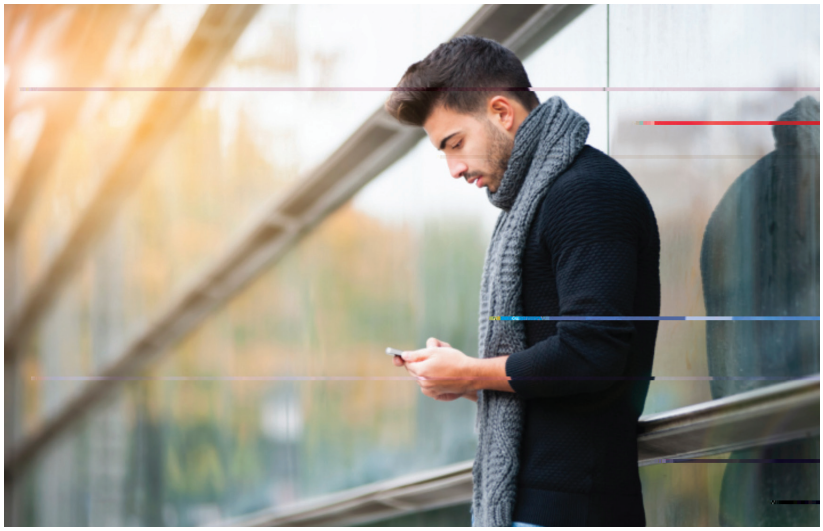
Together we thrive

TABLE OF CONTENTS

WHAT IS IDENTITY THEFT?

Identity theft is the crime of using another person's personal information, credit history or other identifying characteristics to make purchases, borrow money, gain employment or secure legal documents. Unfortunately, most people don't consider the impact of identity theft until after they have been a victim. Each year, millions of Americans are affected and it can occur in many different forms.

It is easy to assume that our personal information is safe, however 19 people become victims of ID theft each minute. That's a scary number but you shouldn't be alarmed as there are steps that you can take to safeguard your identity.



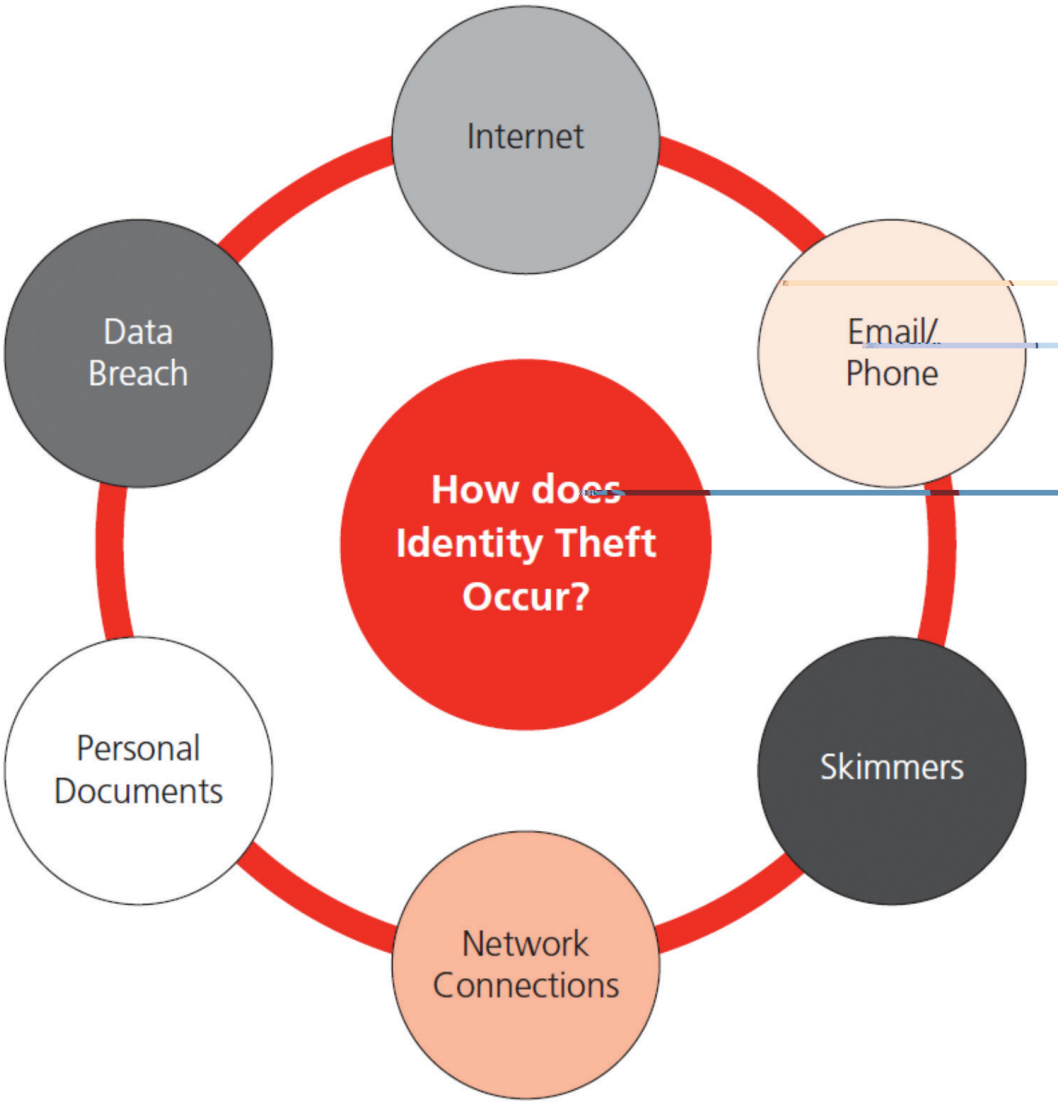
HOW IDENTITY THIEVES USE YOUR INFORMATION

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.
- Open new credit accounts. They will use the accounts and may not pay the bills, causing the delinquent accounts to appear on your credit report. Other times, they may make minimum payments on time to keep the credit line open and active.
- Establish phone or wireless service in your name.
- Open bank accounts and write bad checks.
- Take out loans in your name and buy consumer goods.
- Obtain a passport, employment, health insurance, legal documents, drivers' license, etc.

HOW IDENTITY THEFT OCCURS

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



INTERNET

Pharming

Pharming is a form of identity theft that occurs over the internet when a person (Pharmer) directs users to fraudulent commercial web sites and captures personal data entered by users. You may be directed to these fraudulent websites through an email.

Look at the example websites below. You may not notice any difference at first. However, if you look closer, what is wrong with the second website? This website is fishy. If you review the text you will see that it is not Facebook.com. It looks very similar, but, it does not end in .com and additionally, it is not a secure website (no lock symbol or https://). If you input your email and password into the second site, the information you enter may be stored and used by an identity thief, placing you at risk. So be careful! Be sure to check for a secure lock icon or https: in front of the website address, and read the web address to ensure you are on the site you intended to be on.

Reputable websites that require a login will be secure. Spoofed websites will capture your login information and potentially steal your data.

TIPS TO AVOID PHARMING:

- Be aware of where you are on the internet. Are you on the site you thought you were?
- Don't send personal or financial information via email or enter it into a website that you are not sure of.
- 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. It may also show a lock icon:

EMAIL

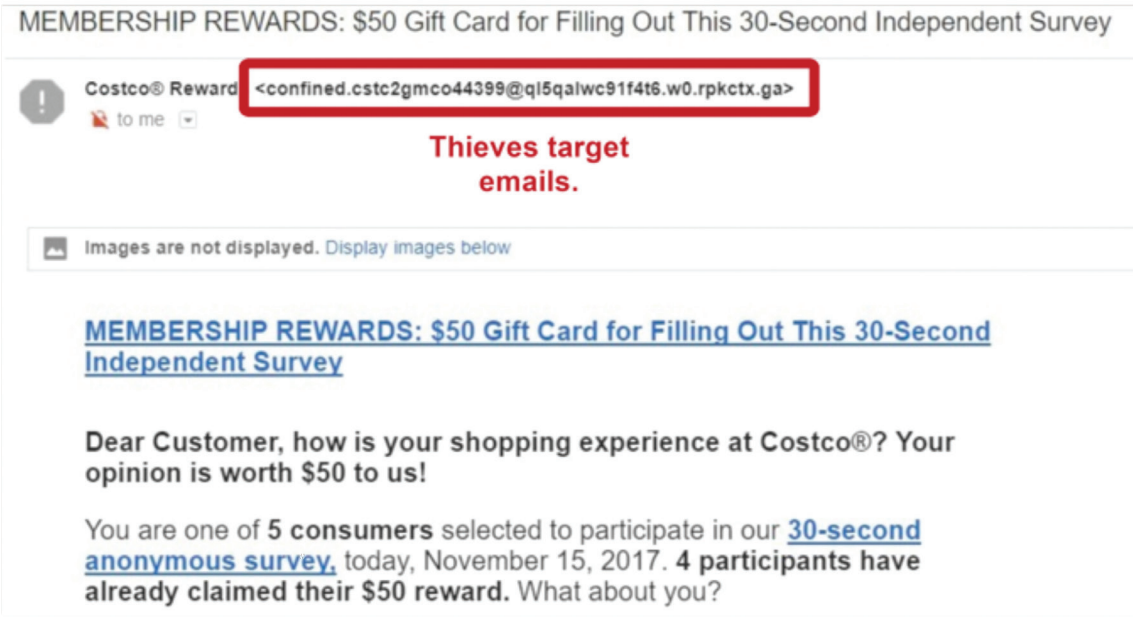
Phishing

Phishing is a practice where identity thieves attempt to "fish" for confidential passwords and financial data using email. Fraudsters build a fake site and send out thousands of phishing emails with a link to the fake site. Victims click on the link in the email, believing it is legitimate. The site then prompts them to enter personal information. Fraudsters compile the stolen personal information and sell it online or use it themselves.

Look at the example email below. What is wrong with this email? Would you click on the links in this email?

This is an example of a spam email, where an identity thief is "phishing" for your personal information. The email address that this is coming from has random letters and symbols instead of a traditional@costco.com or similar corporate email address. If you clicked on a link in this email, you may actually be directed to a fishy site where a thief is waiting to steal your username and password.

You might receive a similar email where an identity thief makes it look like the email is coming from your bank. HSBC will never send you an email asking for your personal information in the email and no other bank should either. You should use the same diligence and logic to determine the validity of this type of email. If you are unsure, do not click!



TIPS TO AVOID PHISHING:

- Delete unknown email messages and don't download attachments or click on links included in the email.
- Don't allow convenience to get in the way of security. Don't click on links in emails that you were not expecting or are unsure of who sent them.
- Reach out to the company or individual by phone to confirm the validity of the email. Do not reply to the email.

PHONE

Vishing

"Vishing" or voice phishing is a type of attack made by phone. Fraudsters call and attempt to manipulate people into taking actions or providing information. A visher may try to gain information about family members or the victim's personal life by asking questions, which ultimately result in the victim unknowingly providing information used to defraud themselves. A visher may also use scare tactics, such as telling you that a family member is in trouble and that they need you to send money to help them. Vishers may pretend that they are your financial institution, and try to get you to provide passwords, pin numbers, or credit card numbers so that they can then access your financial accounts.

Often seniors are targeted with this type of fraud. Be sure to talk to your parents, grandparents and elderly neighbors to ensure they are aware and protect themselves. If you do not know the caller, do not give out any personal or sensitive information!

SMShing

SMShing or SMiShing (a fairly new term in the cyber world) is the mobile equivalent to Phishing. SMShing happens when you receive an SMS message (text) on your phone that claims to be from a reputable source and asks for personal information.

TIPS TO AVOID VISHING AND SMSHING:

1. Do not give sensitive information over the phone or text. Financial institutions will never ask for passwords or PINs.
2. If you are unsure the caller or texter is who they claim to be, advise that you are ending the call and contact the institution directly.
3. Add your number to the national Do Not Call list, which will remove you from most telemarketers' lists. Register at *www.donotcall.gov*.
   - Keep in mind, that the Do Not Call list is observed by legitimate organizations. Fraudsters will not follow this law.

SKIMMERS

A skimmer is a small device used to steal credit or debit card information in an otherwise legitimate credit or debit card transaction. When a credit or debit card is run through a skimmer, the device captures and stores all the details stored in the card's magnetic strip. Simmers are most commonly found on ATMs and gas pumps.

TIPS TO AVOID SKIMMERS:

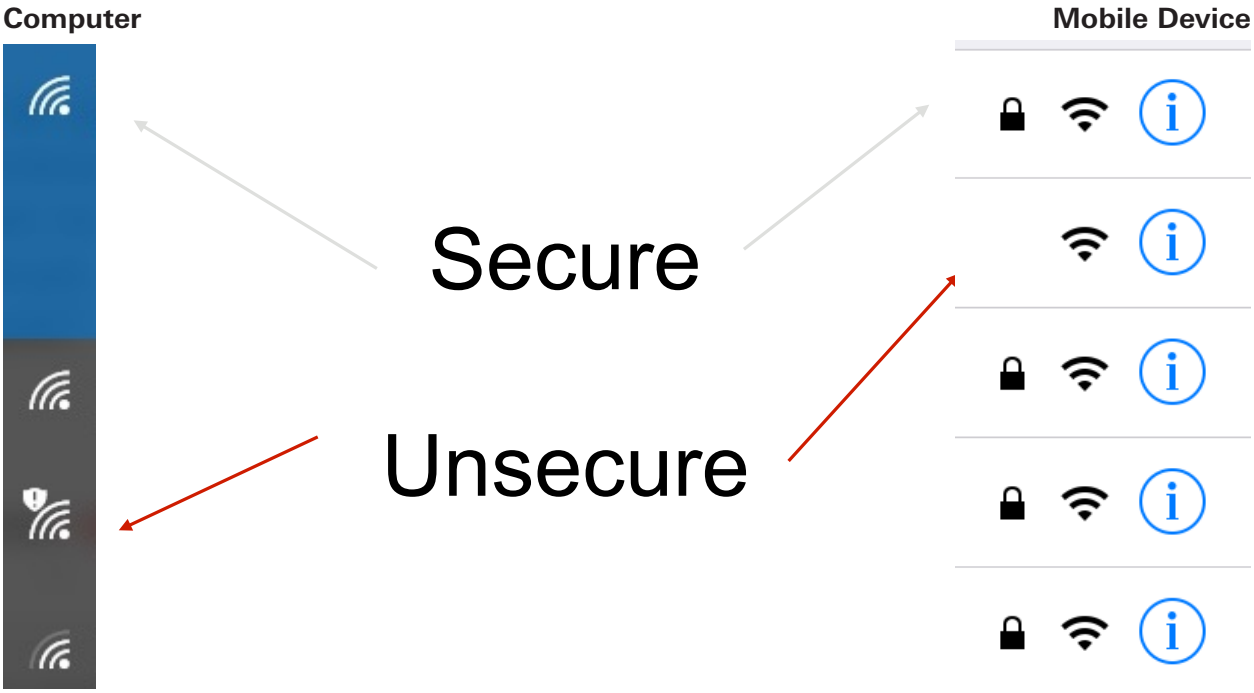
- Use a gas pump within the attendant's view at a gas station.
- Use ATMs at your financial institution whenever possible.

NETWORK CONNECTIONS

A common way that identity thieves access information is via unsecure network connections. So, it is important that you use secure Wi-Fi connections when using your mobile devices or computers.

Look at the connection images below. How do you know if you are connecting to a secure network from your computer or mobile device? When you go to connect to Wi-Fi from a computer, an unsecured network connection will have a symbol with a black exclamation point and will not require a password. A secure network will require that you enter a password.

When connecting via a mobile device, a lock symbol will indicate a secure network, and will require a password to connect. If you do not see a lock symbol and are not required to enter a password, it is an open or unsecure connection.



TIP TO AVOID CONNECTING TO AN UNSECURE NETWORK:
Turn off settings on your computer and mobile device that will automatically connect you to an open network.

PERSONAL DOCUMENTS

Another way that identity theft occurs is through the loss of personal information. This is when a friend, relative, employee or stranger steals your data or your personal information is compromised in some way. Identity thieves have been known to steal mail, sort through trash, or simply take your wallet, purse or cell phone to access personal information. They can also look over your shoulder while you are working or take information if you walk away without locking your computer.

TIP TO AVOID LOSS OF PERSONAL INFORMATION:
Do not write down your PIN and keep it with your cards or where it is easily visible to others.

You will find more ways for you to proactively protect your personal information and documents starting on page 11.

DATA BREACH

A data breach occurs when personal files are stolen from a place where you have conducted business. For example, you may have heard about a large retailer that had a breach where credit/debit card numbers were stolen.

TIP TO AVOID BEING IMPACTED BY A DATA BREACH:

Be proactive. If you learn about a data breach that could impact you, change your passwords associated with the compromised account.

Data Breach Examples: Headlines

- "Delta Data Breach 2018: Was Your Payment Info Exposed?"
- "The Target Data Breach Is Becoming A Nightmare"
- "Yahoo says 500 million accounts stolen"

2017 EQUIFAX Breach

In 2017, 144 million Americans were impacted by the Equifax data breach. Equifax is one of the three major credit bureaus. Because of this breach, Equifax offered 1 year of free credit monitoring to anyone that was impacted and requested it. It is very important to check your credit report for accuracy every four months, or in this case, immediately following a data breach that could have affected you. To obtain your free credit report, go to ***annualcreditreport.com***.

PROTECTING YOUR IDENTITY

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:

Social Security Number (SSN)

- Give your SSN only when it is absolutely necessary (i.e. your employer will need it for wage and tax reporting).
- DO NOT carry your Social Security card with you. Keep your Social Security card in a secure location, like a safe at home.
- 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 do you protect it from being stolen?
  - How will it be used?
  - What will happen if I don't give it to you?
- Check your Social Security earnings and benefit statement each year for fraud.

Passwords

- Create complex passwords using upper and lower case letters, numbers and special characters.
  - Do not use easily identifiable information such as: mother's maiden name, address, date of birth or your telephone number.
  - Make new passwords significantly different from previous passwords.
  - If you have trouble remembering your passwords, write down clues that will jog your memory, but wouldn't be easy to figure out by another person. Keep the clues hidden in a safe place.
- Use different passwords for different accounts.
- Do not save passwords on a shared laptop or your phone.
- If you think someone else knows your password or has accessed your account, change your password immediately.
- Do not share passwords with anyone and do not write them down and carry them with you.

PERSONAL DOCUMENTS/INFORMATION

At Home

- Shred all sensitive materials such as bills, pre-approved credit offers, and other documents with personal information.
- Do not write your PIN number down and carry it with you.
- Do not 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.
- If you receive a phone call, ask if you can call the person back. Do not give out information unless you know who you are speaking with.
- Report any questionable charges on your bills.
- Don't put your credit card or account number on checks, when you pay your bills by mail.
- Sign and activate new credit cards immediately. Cut up and throw away or shred expired credit cards.
- If you live in an area where your outgoing mail is picked up by a mail-carrier, make an effort to take outgoing mail to the post office and keep your trash cans in a secured area.
- Make a copy of all your financial, personal and insurance cards and identification that you carry in your wallet. Keep them in a safe place at home.
- Order a credit report once a year from each of the three major credit bureaus through *annualcreditreport.com*.

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

- Lock your laptop whenever you step away. If you use your laptop when you are in a hotel room, turn off the laptop and secure it when you step out of the room.
- Do not throw personal information in the trash.
- 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.

Technology

- Use a secure browser to guard the privacy of your online transactions.
- Enable the passcode option on your mobile device.
- Update your home computer virus protection software regularly.
- Pay your bills online. The odds of identity theft are lower when you pay your bills online, compared to paying them through the mail.
- Read privacy policies carefully.
- 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.
- Avoid using the automatic log-in feature offered for online services.

Reducing Risk Online

Since so much of what we do today is done online, it is important that we reduce our risk as much as possible. Here are some additional tips to protect yourself online.

- *Anti-virus program* – An anti-virus program is a software program that detects, prevents and removes viruses from a computer. Be sure to use reputable anti-virus programs on all technology devices and update them regularly. Some good options include Bitdefender, Norton, Kaspersky Lab, and McAfee.
- *Clear cookies* – Web cookies are special files used by websites to keep track of various user activities. You should clear your cookies from your web browser on a regular basis by going to settings and following instructions to delete. Most web browser cookie settings are in the "options" or "setting" menu. Search online to determine how to delete your preferred browser's cookies. You can also use incognito or InPrivate browsing. You do this by right-clicking on your internet icon and then choosing In-private or incognito browsing. This allows you to search without attaching to history or cookies.
- *Be cautious of what you share on social media* – Identity thieves look for your information in many places, and social media can be an easy place for them to piece your personal information together if you are not careful. Do not share picture IDs, bills, travel confirmations or event tickets.
- *Using Apps* – what access do you allow? Be careful when using apps that ask to access your data or your locations. Allowing access to your contacts or "Logging in through Facebook" on third party apps allows access to your data.

In summary, make sure you protect what you can control as best you can. 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.

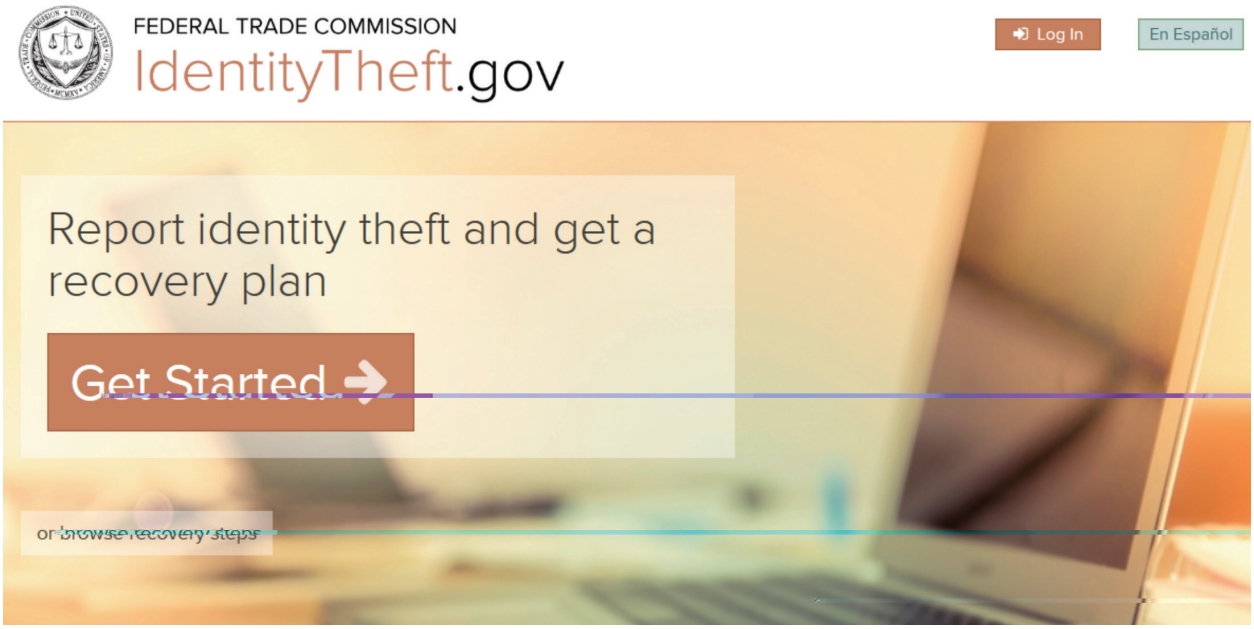
Some of the most common ways to know if you have been a victim include:

- Unexplained charges or withdrawals on your checking or savings account.
- Failing to receive monthly bills.
- Receiving credit cards that you did not order.
- Denied credit for no apparent reason.
- Collection calls from creditors and debt collectors for bills that are not yours.
- Inaccuracies on your credit reports that are not the result of human errors.

HOW DO YOU RECOVER?

If you have been a victim of identity theft, you must find out how many of your records have been compromised and you may need to file a police report. 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 Department 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 Social Security Number.

If you become a victim of identity theft, act quickly to restore your good name. A good resource that provides step by step instructions to help you through the recovery process can be found at *IdentityTheft.gov*.



There may be different steps to take based on the type of identity theft that has occurred, and the site will walk you through the appropriate steps. Generally, you will want to consider the following:

STEP 1: Call the companies where you know fraud occurred.	• Ask for the fraud department. • Close or freeze accounts. • Follow procedures to dispute inaccuracies. • Create new PINS, passwords, etc.
STEP 2: Contact the credit bureaus to place a fraud alert and obtain your credit reports.	• Place a fraud alert with all three agencies — Equifax, Experian and Transunion — on your credit report. • Review your credit reports carefully (you can order your free report at *Annualcreditreport.com*).
STEP 3: Report identity theft to FTC and other appropriate authorities.	• File a complaint with the FTC *www.ftc.gov*. • You may choose to file a police report with the local police department where the identity theft occurred. A police report is required in order to put a freeze on accounts. • If it appears someone is using your Social Security Number, contact the Social Security Administration (SSA) at *www.ssa.gov*. • Contact US Postal Service to report if your mail is being tampered with.
What to Do Next: Follow up to repair the damage and maintain good records. (Document your actions and get confirmations in writing.)	• Close accounts that have been opened. Ask for confirmation in writing. • Ask that any fraudulent charges be removed. • Follow up with the Credit Reporting Agencies to correct inaccuracies on your credit report. Obtain a copy of your report again in a few months to verify all corrections have been made. • Consider adding an extended fraud alert past the 90 days, or consider a credit freeze.

TIP:

Identity theft is not resolved overnight. On average it takes 6 months or 200 hours to repair ID theft. It may have a negative impact on your credit score and impact your ability to do things such as purchase a home, rent an apartment, obtain a loan, or obtain any other type of credit. It can even make it difficult to open new accounts such as utility accounts or checking accounts. So it is very important to act quickly to take the appropriate steps to correct it.

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

- 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

- Makes it a federal crime when someone transfers or uses another person's means of identification, without a lawful reason to do so and with the intent to commit a crime.

Identity Theft Penalty Enhancement Act

- Provides greater penalties for identity thieves.
- 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

- Gives consumers particular rights when dealing with billing errors.

The Electronic Fund Transfer Act

- Establishes procedures for resolving mistakes on electronic fund transfer account statements.

Fair Credit Reporting Act

- Designed to promote the accuracy, fairness and privacy of information in the files of every Consumer Reporting Agency, the most common of which is a credit bureau.

TIP:

If you are having issues with your credit after identity theft, and would like to talk with someone about your situation, there are non-profit credit counseling agencies that can help. You may wish to reach out to GreenPath Financial Wellness, a non-profit that has been helping people for nearly 60 years. Your individual situation can be reviewed at no-cost by calling *866.692.2659* or visiting *www.greenpath.org*.

MONITOR 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 1) to make sure your credit report is accurate and 2) 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 from *annualcreditreport.com*.

For example:

1. In January, order your Experian report.
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. If you find inaccuracies, you can file a dispute with each of the three agencies. Contact information is below.

CREDIT BUREAUS		
Contact:	Phone:	Website:
Experian	888-EXPERIAN	www.experian.com
TransUnion	800-916-8800	www.transunion.com
Equifax	800-685-1111	www.equifax.com

Children can also become victims of identity theft. If you have a child, and suspect that they have been a victim of identity theft, you can check to see if a credit report exists for your child. Each credit bureau website has instructions on how to do this.

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

CONCLUSION

Identity theft is a crime. It affects many Americans each year. Although there is no guaranteed way to avoid it, there are steps you can take to protect yourself. Protecting your Social Security Number, reviewing your credit report, being aware of your surroundings when shopping, especially if sensitive information is required, are all steps you can take to protect yourself. And remember, if you are a victim of identity theft don't panic. Contact the appropriate authorities and refer back to the steps outlined in this booklet.

RESOURCE: GreenPath Financial Wellness is a national nonprofit organization that provides financial counseling, education and products to empower people to lead financially healthy lives. In working directly with individuals, and through partnerships with other organizations, GreenPath aims to remix the American dream so it works for everyone. Headquartered in Farmington Hills, Mich., GreenPath has nearly 500 employees and operates about 60 branch offices in 19 states. GreenPath is a member of the National Foundation for Credit Counseling (NFCC), and is accredited by the Council on Accreditation (COA). For more information, visit greenpath.org or to speak one-on-one with a certified financial wellness expert, call 866.692.2659.

WHAT ARE YOUR NEXT STEPS?

It is important to take what you have learned and act on it. Being proactive is your best defense against identity theft. Complete the following action plan, and use the checklist to ensure you keep moving toward your goals. Check the box as you complete the action item.

ACTION PLAN:

- ☐ 1 **I will:** Be cautious on the internet and with emails that I don't recognize.
- ☐ 2 **I will:** Be aware of skimming devices in ATMs and other places where I use my card.
- ☐ 3 **I will:** Only use secure network connections and turn off auto connection options on my computer and mobile devices.
- ☐ 4 **I will:** Protect my personal documents and information, including social security number, passwords, PINs, and sensitive materials. I will create complex passwords, shred sensitive documents, and carefully use technology so as to protect my personal information.
- ☐ 5 **I will:** Be mindful of data breaches in the news, and be proactive if I learn about a data breach that impacts me.
- ☐ 6 **I will:** Work to reduce my risk online by using and updating anti-virus programs, clearing cookies when on the internet, not sharing personal information on social media and being safe when using apps to not allow access to my personal information.
- ☐ 7 **I will:** Follow the steps on identitytheft.gov, should I become a victim of identity theft. I will continuously monitor my credit report each year for accuracy, and I will contact GreenPath Financial Wellness at 866.692.2659 if I need additional guidance from an expert.

Additional Notes or goals: _____

_____

I will be prepared!

KEY TERMS

Anti-virus Program – A software program that detects, prevents and removes viruses from a computer.

App – An application or program designed to be downloaded on a mobile device.

Cookies – Special files used by websites to keep track of various user activities. You should clear your cookies from your web browser on a regular basis by going to settings and following instructions to delete.

Credit Freeze – A consumer can place a credit freeze on their credit report which locks down the report and makes it so that no new credit accounts can be opened. The credit freeze stays on your report until you remove it. (In a few states it expires after 7 years.) Depending on the state law, credit freezes may involve fees. In most states, they're free for victims of identity theft. For others, they cost about $5 to $10 each time the consumer freezes or unfreezes their account with each credit reporting agency.

Credit Report – A financial report card used to evaluate your credit worthiness and calculate your credit score. A credit report contains detailed information on a person's credit history including personal identifying information, information on credit accounts and loans (including payment history), public records, and inquiries.

Data Breach – Personal files are stolen from a place where you have conducted business.

Encryption – The process of converting information or data into a code, especially to prevent unauthorized access.

Fraud Alert – A consumer can place a fraud alert on their credit report which makes it harder for an identity thief to open more accounts in your name, by requiring a business/lender to try to verify a consumer's identity before extending new credit. A fraud alert is free and typically stays on a credit report for 90 days, unless it is renewed.

Identity Theft – The crime of using another person's personal information, credit history or other identifying characteristics to make purchases, borrow money, gain employment or secure legal documents.

Password – A secret word or phrase that must be used to gain admission to something. A strong password should be complex and contain both upper and lowercase letters, numbers, and special characters.

Personal Identification Number (PIN) – A numeric or alpha-numeric code used in many electronic financial transactions to authenticate a user to a system. For example, you must enter your PIN to access money from your account at an ATM.

Personal Information/Documents – Documents that contain personal identifying information such as social security numbers, date of birth, address, etc. that thieves steal and then use this data to commit fraud without you knowing.

Pharming – A form of identity theft that occurs over the internet when a person (Pharmer) directs users to fraudulent commercial websites and captures personal data entered by users.

Phishing – A practice where identity thieves attempt to "fish" for confidential passwords and financial data using email. Fraudsters build a fake site and send out thousands of phishing emails with a link to the fake site. Victims click on the link in the email, believing it is legitimate. The site then prompts them to enter personal information. Fraudsters compile the stolen personal information and sell it online or use it themselves.

Secure Network Connection – A connection that is encrypted by one or more security protocols to ensure the security of data flowing. A password is needed to establish the secure connection.

Skimmer – A small device used to steal credit or debit card information in an otherwise legitimate credit or debit card transaction. When a credit or debit card is run through a skimmer, the device captures and stores all the details stored in the card's magnetic strip.

SMShing – SMShing or SMiShing is the mobile equivalent to Phishing. It happens when you receive an SMS message (text) on your phone that claims to be from a reputable source and asks for personal information.

Unsecure Network Connection – A network connection that you can access without a password and is not encrypted. These networks are open to the public.

Vishing – "Vishing" or voice phishing is a type of attack made by phone. Fraudsters call and attempt to manipulate people into taking actions or providing information.

NOTES