Township of O'Hara

325 Fox Chapel Road | Pittsburgh, PA 15238 | Phone 412-782-1403 | Fax 412-782-3291
Superintendent of Police Jay Davis

POLICE DEPARTMENT

VICTIMS OF IDENTITY THEFT

IDENTITY THEFT is a common rapidly growing crime. The theft and use of an individual's personal identifying information for a variety of fraudulent criminal activities causes financial and other damage to many victims. This document will help you understand how identity theft occurs, what steps you can take to protect your personal information, and what to do if it happens to you.

The personal information thieves can use to steal your identity include your:

- Full name
- Address (home or other)
- Phone number
- Date and place of birth
- Historical information (mother's maiden name, school names, etc.) often times obtained from obituaries
- Social security number
- Driver's license number
- Passport number
- Email address
- Screen or usernames
- Passwords and PINS
- Health plan information
- Geolocation information
- Credit and debit card numbers
- Financial account numbers or information
- Photos, videos, or audio files
- Information that provides access to the above items listed

Identity theft is the act of stealing a victim's Personal Identifying Information (PII). Remember identity thieves are always looking for the next scam to obtain personal identifying information from unsuspecting people. Here are some of the common ways in which identity thieves steal personal identifying information:

1. **Phishing**
Scammers often use phishing emails to trick victims into providing personal or financial information. Phishing emails can be deceiving in that they may appear to come from a known or trusted company, such as a bank or an online retailer, and use various tactics to get the victim to click a link or open an attachment.

2. **Smishing**
Scammers may also target victims via text message—a crime called smishing. Similar to phishing attacks, criminals may impersonate trusted organizations or even friends to trick victims into divulging information. Smishing may be increasing as more people trust text messages over phone calls and emails.

3. **Vishing**
Fraudsters can also use phone calls, also known as voice phishing or vishing, to target potential victims. Phone scammers sometimes use promises, like the offer of a prize, or threats, such as the risk of not getting a tax refund, to prompt victims into giving up personal information. Scammers will also use spoofing to send falsified information to a caller ID. A spoofed call looks like it's coming from a local number or a trusted organization when it could be originating anywhere in the world.

4. **Fake Websites**
Fake websites often look like legitimate and trustworthy sites to make people more apt to provide their personal information. Some online shopping scams use a bogus website or mobile app that mimics a trusted retailer, including a familiar logo and similar URL. Purchases made on these fraudulent sites will likely never arrive, or worse, scammers may seed the website with malware that infects the victim's device and harvests personal or financial information.

5. **Impersonation Scams or Confidence Fraud**
Confidence fraud occurs when a criminal deceives a victim into believing they have a trusted relationship—as a family member, friend, or romantic interest—to convince the victim to send money, provide information, make purchases, or even launder money. One-way thieves steal taxpayer information is through IRS impersonation scams. Scammers call their victims claiming to work for the IRS or send fraudulent emails that look like official communications.

6. **Data Breaches**
A data breach is the intentional or unintentional release or theft of information, whether it is due to a cyberattack or simply the improper disposal of physical documents. If an individual is notified of a breach, their financial or personal information may have been exposed. The theft of usernames and passwords from data breaches may also fuel credential stuffing attacks in which criminals use stolen username and password combinations to hack into other accounts.

7.**Skimming**
Skimming occurs when a criminal steals information as the debit or credit card is swiped. Scammers may tamper with the electronic card reader so that it captures card data, place a recording device at an ATM, or recruit a crooked salesperson to steal customers' card data.

8. **Public Wi-Fi and USB Charging Stations**
Many public Wi-Fi networks are vulnerable to threats from hackers, making it possible for thieves to eavesdrop on users' private information. Scammers may also employ a USB charging scam, called juice jacking, in which malware infects the user's device when connected to an airport USB charging station or hotel USB port.

9. **Purchase of Information on the Dark Web**
The dark web, or dark net, is a part of the internet that serves as a highly profitable marketplace where criminals can purchase stolen personal information. Private photos, medical records, and financial information have all reportedly been stolen and shared on the dark web. Security researches have reported a concerning trend that cybercriminals have begun targeting children, even infants, and advertising their stolen information for sale on the dark web.

10. **Theft by a Family Member or Friend**
An identity could be stolen by a family member or friend, such as a parent who uses a child's information to get a credit card or loan, or someone who uses their spouse's information without permission to open an account. According to one report, 51 percent of new account fraud victims stated that they personally knew the individual who committed the fraud.

11. **Theft of a Wallet, Mail, or Even Trash**
Personal and financial information can also be stolen using low-tech methods, such as a criminal going through the victim's mail or even their trash.

Acting quickly is important once you recognize you are a victim of identity theft.

Immediate Steps:

1. Call any business where you know fraud took place. Ask to speak to the fraud department. Advise the fraud department that your identity was stolen. Ask for your account(s) to be closed or frozen so an identity thief cannot add new charges.

2. Place initial fraud alert on your files. Contact one of the three major U.S. credit reporting companies to report yourself as a victim of identity theft.

   They are:

   - Equifax 888-766-0008 Equifax.com
   - Experian 888-397-3742 Experian.com
   - Transunion 800-680-7289 TransUnion.com

   Whichever company you contact they must tell the other two agencies. Ask the credit reporting company you contact for confirmation that this will be done.

   A fraud alert on your credit report lets lenders and creditors know that they should take steps to verify your identity before they issue you credit. This may help prevent identity thieves from opening new accounts in your name. An initial fraud alert is good for 90 days and may be renewed. You may choose to place an extended fraud alert. You might also choose at this time to place a credit freeze.

3. Order a credit report. By law, you are entitled to a free copy of your credit report once a year from all three companies. You must contact each individually to order a report. (You may wish to order one now and the other two at later times to track new activity or corrections.) Immediately review your credit report and note any unfamiliar transactions or accounts.

4. File a complaint about the theft with the FTC. You can do so online or over the phone at ftccompliantassistant.gov or 877-438-4338

   Include as much information as possible and follow instructions carefully. Make sure to save and print out your completed complaint. Once it's printed out, it becomes an Identity Theft Affidavit. The affidavit helps you create an Identity Theft Report.

   Keep a record of the day you filed the complaint, your complaint reference number and copies of the affidavit. If you later need to update your complaint, call the phone number shown above and have your complaint reference number ready.

5. File a police report. Go to your local police station (or the police station where the theft occurred). Say you are a victim of identity theft and wish to file a police report. Bring along:

    1. A copy of your FTC Identity Theft Affidavit.
    2. Any proof or documents showing you are a victim of identity theft.
    3. Proof of your address
    4. A Government issued photo I.D.

Be Organized & Attentive

As you respond to identity theft, set up a system that helps you track information and deadlines.

- Log every phone call. Write down the date and time, phone number and any other contact information. Also record the name, department, and title of the person you spoke with, as well as a summary of the of the information discussed.
- Confirm discussions in writing with follow-up letters or emails.
- Set up a filing system especially for this issue.
- Never send original documents. Keep them securely filed. Send only copies to others,
- Send all letters, document copies or other materials by certified mail with a return receipt. Log who you sent what and when.
- Make and file copies of all the correspondence or completed forms you send. File all correspondence or documents you receive.
- Note important dates and deadlines in your calendar. Always learn how long you have to supply information or to have others supply it to you.

Additional Steps to Take

Once you have taken care of all immediate actions, there are a few more things you can do to continue to limit damage or recover from it. What you do next, including whom you contact, will depend on what personal information was stolen and how far-reaching are the effects.

Visit **identifytheft.gov** for specific information, sample letters to send, and contact links for various situations.

As you learn of any issues through your credit report or other avenues, respond quickly.

Close fraudulent accounts:

- Call the fraud department of each business and ask for the account to be closed.
- As required, send each business a copy of your Identity Theft Report and/or completed dispute form it requests along with a letter.
- Ask for a letter that confirms the account was fraudulent, that you are not liable for it, and that it was removed from your credit report.

Get Proof of Fraudulent Activity:

- Ask businesses for copies of documents the identity thief used to open a new account or make a purchase in your name.
- Don't take NO for an answer. Speak with a supervisor if necessary.

Get Rid of Fraudulent Charges

- Call the fraud departments of every bank or business to report all wrongful transactions.
- As required, send them a copy of your Identity Theft Report and/or any completed dispute form along with a letter.
- Request letters from them that confirm their removal of fraudulent charges.

Correct Credit Report Errors

- Send a letter to the three credit reporting companies requesting all fraudulent information be blocked (removed).
- Enclose a copy of your Identity Theft Report, proof of identity and copies of documents that show the errors your letter is reporting.

Consider an Extended Fraud Alert

- An extended fraud alert lasts for seven years. Unlike an initial fraud alert, which says creditors should contact you before extending credit in your name, an extended fraud alert requires they do so using the contact information you provide when you place the extended alert. You also become entitled to two free copies of your credit report each year.
- If you choose to place one, send a letter of request and a copy of your Identity Theft Report to each of the three credit reporting companies.

Think About a Credit Freeze

- Also known as a security freeze, this is designed to restrict access to your credit report unless you temporarily lift or permanently remove the freeze.
  A credit freeze makes it less likely that an identity thief can open new accounts in your name. Be aware that a credit freeze can cause delays or other issues when you submit requests or applications that involve your credit report. Ask about such issues and weigh any concerns against your need for identity security.
- To place a credit freeze on your file, contact each of the credit reporting agencies. There may be small fees to place, lift, or remove a freeze. It depends on your state law. Many states do not charge fees to identity theft victims. Ask your state Attorney General's office about state laws and fees for credit freezes.

Look into Identity Theft Protection Services

- Many companies, including credit reporting companies, offer identity theft protection services. These are provided on a subscription basis for a fee. Generally, they help you monitor your accounts. Some provide other types of benefits. Basic credit monitoring services track your credit history, report on your credit score, provide alerts to suspicious activity and may include forms of assistance.

- More comprehensive identity theft protection plans usually include credit monitoring activities as part of a package of services benefits. These can include family coverage options, internet scanning to look for misuse of personal information online, recovery assistance or insurance to cover reimbursement for certain identity theft related expenses.

- Depending on your situation, you may wish to consider purchasing identity theft protection services. If so, be sure to investigate various options and weigh the pros and cons of each. Thoroughly research any company you consider. Make sure you read all of the fine print, including all legal information, policies and notices. Know exactly which services are provided, their limits and the costs involved.

- Remember these services primarily help you in monitoring. None can ensure the safety of your identity or take the place of your own caution and oversight.

What's your Identity Theft Risk?

Take the following quiz to see how well you protect your personal information from identity thieves. Read each statement. Write T for true and F for false on the line. If a question does not apply to you leave it blank.

1. My mailbox has a locking device.
2. I put all outgoing mail into a postal mailbox.
3. I shred all unwanted documents.
4. I use a good-quality crosscut shredder.
5. I carry only the payment cards I need and will be using each day.
6. I know exactly what identity cards, documents, and other items are always in my purse or wallet.
7. I memorize all my PINS.
8. I shield keypads when entering passwords or card numbers.
9. I change my pins and passwords often.
10. My passwords are all at least 10-12 characters long and a mix of capital and lower-case letters, digits and special characters.
11. I use a password manager.
12. I carry my Social Security Card only when absolutely necessary.
13. I am very cautious about sharing my Social Security number and ask why it's needed and how it will be kept safe before I give it out.
14. I don't share personal information with unknown callers.
15. I donate to established charities only.
16. I use a credit monitoring service.
17. I use a VPN when on public wi-fi.
18. I never click on links in pop-up windows.
19. I don't click on links in emails or text messages from unknown senders, and only do so cautiously from known senders.
20. Before using ATM's and sales terminals, I check for signs of skimming devices.
21. I always take receipts, safely store them, and shred them when they are no longer needed.
22. I don't autosave login information.
23. I stay alert to risks when traveling.
24. My computer and devices have comprehensive security programs.
25. I stay on top of updating operating systems and software.
26. I independently verify Web addresses, then enter them directly into my browser's address bar instead of using email links.
27. I download software, apps, and email attachments only from reliable sources.
28. I read all disclosure information before downloading the software.
29. I limit what I share on social networking sites.
30. I don't trust anyone online and know people may not be who they say they are.
31. I secure my at home wireless network.
32. I use two-factor authentication on online accounts.
33. I keep all computer and internet related security and privacy settings at strong, identity protecting levels.
34. I know about and utilize security options for all my internet connecting devices.

35. I make sure my mobile devices don't automatically connect to nearby Wi-Fi.
36. I always log off an account and close my browser when finished with an online transaction.
37. I check for signs that a website and its business are secure and trustworthy before entering personal information.
38. I am careful about securely storing personal items I bring to my workplace.
39. I don't store personal information or access personal accounts on work computers or devices.

If all or most of these statements are true for you, congratulations! You're doing a good job in preventing identity theft. If any were not, consider how you may be putting yourself at higher risk for identity theft.

REMEMBER: Your personal information is only as secure in the least secure way it is stored or disclosed.

Helpful Websites:

- The Better Business Bureau – bbb.org
- The Federal Trade Commission – consumer ftc.gov
  Identitytheft.gov
- The Financial Fraud Enforcement Task Force - stopfraud.gov
- Internal Revenue Service – irs.gov/individuals/identity-protection
- The Internet Crime Complaint Center – ic3.gov
- National Cyber Security Alliance – StaySafeOnline.org
- U.S. Department of Homeland Security – dhs.gov
- US-CERT.gov
- dhs.gov/stopthinkconnect
- U.S Government's Online Safety Site – OnGuardOnline.gov