IDENTITY THEFT PREVENTION

Identity theft can happen if your Social Security number, health records, bank accounts, credit card information, passwords/PINs, or other personal data falls into the wrong hands. There are three basic ways that identity thieves can obtain your personal information: steal it, obtain it from a public source like social media, or trick you into giving it away.

How to prevent identity theft due to…

Stolen information

- Replace credit and debit cards as soon as possible after they are lost, stolen, or compromised.
- Don't write down passwords. If you can't remember them, write down clues. Don't use the same password for multiple sites.
- If a company that you do business with reports a "data breach", take it seriously. Take advantage of any offers for free credit reports. Change passwords for the company's website and any other passwords stored on the site. Cancel accounts related to that business.
- Keep sensitive documents in a safe secure place out of general view. Documents that are no longer needed should be cut up or destroyed. Also shred credit card offers that you are not interested in. Better yet, opt-out of pre-approved credit offers by calling 1-888-5-OPT-OUT (567-8688).
- Make copies of your credit cards, Social Security card, ID cards, and insurance cards in case of theft. Keep the copies in a safe place.

Social media

- Don't post personal information (e.g., birthday) on social media that could be used to steal your identity.
- When choosing security questions for your financial accounts, avoid using information that is likely to be available online. Better yet, make up false answers. (Just make sure you remember your answers!)

Deception

- Don't send personal information by e-mail and don't click on attachments from e-mail addresses you don't recognize.
- Be very suspicious of any e-mail that asks you to click on a link or asks you to enter your personal information online. Learn more about these scams (known as "phishing"): **https://www.transunion.com/blog/identity-protection/avoiding-phishing-scams**
- Stay up to date on the latest scams: **https://www.experian.com/blogs/ask-experian/the-latest-scams-you-need-to-aware-of/**

General Identity Theft Prevention Tips

- Request a credit report. The three national credit reporting agencies — Equifax, Experian, and TransUnion— have permanently extended a program that lets you check your credit report at each of the agencies once a week for free.
    - Phone: 877-322-8228
    - Online: **www.annualcreditreport.com**
    - Mail: [form can be found on page 21 of AOG ID Theft document]

IDENTITY THEFT PREVENTION

MARYLAND VOLUNTEER LAWYERS SERVICE

General Identity Theft Prevention Tips

- Consider a "credit freeze". This prevents businesses from accessing your credit history and will thus prevent identity thieves from getting credit in your name. Of course, it also prevents you from getting credit until you "thaw" the credit reports. You can freeze or thaw your credit reports for **free**, by contacting all **three** of the credit reporting agencies.
- Equifax:
  - Phone: 888-298-0045
  - Online: **www.equifax.com/personal/credit-report-services/credit-freeze**
  - Mail: Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348
- Experian
  - Phone: 888-397-3742
  - Online: **www.experian.com/freeze/center.html**
  - Mail: Experian Security Freeze, P.O. Box 9554, Allen, TX 75013
- TransUnion
  - Phone: 888-909-8872
  - Online: **www.transunion.com/credit-freeze**
  - Mail: TransUnion LLC, P.O. Box 2000, Chester, PA 19022
- If requesting a credit freeze by mail, provide the following information:
  - Full name, address, Social Security number, and date of birth
  - Prior addresses and prior names if either have changed in the last five years
  - Copy of government-issued ID (driver's license, passport, ID card)
  - Bank statement or utility bill confirming current address
- Consider protecting your federal taxes with an IRS Identity Protection PIN (IP PIN). This is a special PIN issued to you each year by the IRS to help ensure no-one falsely files taxes in your name to try and get your refund. It works much like a passcode some sites and apps send to your phone to prove your identity. Whenever you file, you, or your tax preparer, include that year's IP PIN on your return to prove it's you filing. You can learn more about the program here: **https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin**

Additional Resources:

- Maryland Attorney General: **https://www.marylandattorneygeneral.gov/pages/identitytheft**
- The Identity Theft Resource Center: **https://www.idtheftcenter.org/**
- Privacy Rights Clearinghouse: **https://privacyrights.org/**
- Equifax: **https://www.equifax.com/personal/education/identity-theft/**
- Experian: **https://www.experian.com/help/identity-theft-victim-assistance.html**
- TransUnion: **https://www.transunion.com/identity-protection**
- IRS help page on Tax-related Identity Theft: **https://www.irs.gov/identity-theft-central**