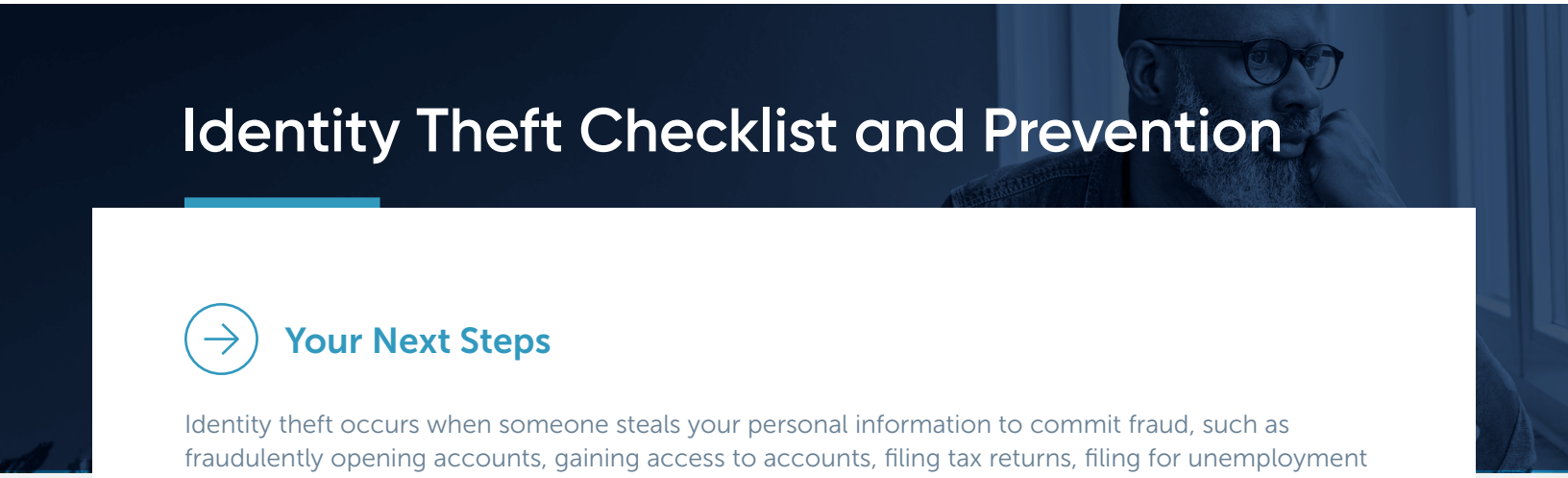
HOMAN
WEALTH ADVISORS



# Identity Theft Checklist and Prevention

## Your Next Steps

Identity theft occurs when someone steals your personal information to commit fraud, such as fraudulently opening accounts, gaining access to accounts, filing tax returns, filing for unemployment benefits, obtaining medical services, or sending fake bills to your health insurer, etc. If you have been a victim of identity theft, we recommend taking the following steps. While these are core steps to take, this is not designed to be an exhaustive list of all steps you may need to take. You should review additional resources based on your particular identity theft situation.

### ✓ Contact your Advisory Team at Buckingham.

Once you have contacted us, we will contact the custodians or instruct you to contact your custodians related to your accounts. You should also immediately contact any custodians and other financial service providers for accounts not under Buckingham's management. Request a freeze on your current accounts; if possible, open a new account.

- Review all accounts to ensure no suspicious activity has occurred.
- Change all account passwords. Set up two- factor authentication where available.
- Pull your credit report from the three major credit bureaus and contact them to place a "fraud alert" on your credit records or consider freezing your credit.

| TransUnion | Experian | Equifax |
|---|---|---|
| www.transunion.com | www.experian.com | www.equifax.com |
| 800.680.7289 | 888.397.3742 | 800.525.6285 |

- Report identity theft to the Federal Trade Commission and obtain a recovery plan at www.identitytheft.gov.

### ✓ Contact the police in your city.

Securing a police report is of utmost importance. It could be necessary if:

- You know the identity of the thief
- The thief used your name in an interaction with police, or
- A creditor or another company requires you to provide a police report.

Under federal law you are entitled to one free copy of your credit report from all three credit reporting agencies once every 12 months. You may request the free credit report at www.annualcreditreport.com or by phone at 877 FACTACT. You can request all three reports at once or you can spread each individual request over a period of several month.

- **File a report with the Internet Crime Complaint Center (IC3), a division of the FBI, at** www.ic3.gov/Home/ComplaintChoice.

- **Contact the Social Security fraud hotline.**

  Contact the Social Security fraud hotline through the Office of the Inspector General for the Social Security Administration at www.ssa.gov/antifraudfacts.

- **Get a new driver's license.**

- **Consider identity monitoring services**

  Consider identity monitoring services, credit monitoring services, and identity recovery services. If you already have an identity monitoring services that has identity theft insurance, file a claim.

- **Review your homeowners or renters insurance policy.**

  Review your homeowners or renters insurance policy for any identity theft support provided under your policy.

- **Report specific types of identity theft to other federal agencies.**

  You may also need to report specific types of identity theft to other federal agencies. There are additional steps to take at the state level.

**Additional Resources**

Federal Trade Commission
https://consumer.ftc.gov/identity-theft-and-online-security/identity-theft

Securities and Exchange Commission
https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins/updated-2

Nerd Wallet
https://www.nerdwallet.com/article/finance/how-to-prevent-identity-theft

# Identity Theft Prevention

Below are different ways to prevent identity theft and protect yourself from fraudulent activity.

- Review your accounts regularly to ensure no suspicious activity.
- Perform a security scan on all devices at least every 30 days (most security scanning software allows you to schedule scans).
- Always keep computers and any internet-connected devices, including smart phones, updated.
- If possible, enable two-factor authentication for any online accounts, including email.
- Use a password manager to generate and store unique passwords for your accounts.
- Do not reuse passwords and use random unique passwords for each account.
- Encrypt and password protect all computers and mobile devices.
- Disable "remember my computer" or "auto-login" features when logging in.
- Store your personal information in a safe place.
- Sign up for banking and credit card alerts via email or text message.
- Look out for social engineering or phishing attempts.
- Do not respond to unsolicited requests for personal information (name, birthdate, Social Security number, bank account number, etc.) by phone, email, mail or online.
- Shred receipts, credit offers, account statements and expired cards to prevent "dumpster divers" from getting your personal information.
- Be prudent when using a wireless connection. Unsecured wireless connections can be vulnerable to cyberattacks based on their lack of security. If you are going to access any account on a public wireless network, make certain you secure the network with wireless encryption prior to logging on.
- Be careful downloading files or programs from unknown sources, as you open yourself up to the risk of malicious software programs being downloaded on your computer.
- Do not carry personal information such as your Social Security card in your wallet, and only give this information out when absolutely necessary.
- Collect your mail promptly and place a hold on your mail when you are away for several days.
- Pay attention to billing cycles. If bills or financial statements are late, contact the sender.
- Review your credit reports.

  TransUnion: www.transunion.com
  Experian: www.experian.com
  Equifax: www.equifax.com

- Consider freezing your credit files for free. Credit freezes prevent someone from applying for and getting approval for a credit account or utility services in your name.