Protecting Your Identity

Hemenway & Barnes LLP

Scam artists are constantly trying new methods to steal personal and business account information. We urge all of our clients and friends to be vigilant when sharing personal data and provide you with this information to help you identify and avoid fraud. Here are some steps you can take to help protect your personal data:

Steps you can take to protect your personal information:

1. Change your passwords for your online financial accounts
   - Use random combinations of letters, numbers and special characters
   - Do not use the same password on all of your accounts
2. Review your bank and financial accounts and, if you identify any unauthorized transactions, immediately notify your bank about the transactions and advise the bank that your information was taken in a data breach.
3. Order and review your credit reports at www.annualcreditreport.com
   - You may order a free copy of your credit report once every 12 months from each of the three major reporting companies: Equifax, Experian and TransUnion.
4. Place a Credit Freeze on your credit file or add a Fraud Alert
   - A credit freeze will prevent third parties from accessing your credit report. You may place or lift a credit freeze at any time free of charge. However, it may take several days to lift a freeze. Freezes must be placed individually with each of the three credit reporting agencies: Equifax, Experian and TransUnion. A credit freeze does not hurt your credit score.
   - A fraud alert adds a notice to new lenders to take extra precautions when verifying credit applications. A fraud alert typically lasts for one year. If you place a fraud alert with TransUnion, they will automatically notify Equifax and Experian.
5. Monitor your Social Security account
   - Set up an account: https://www.ssa.gov/myaccount/

Educating yourself about potential scams is one of the best ways to protect yourself.

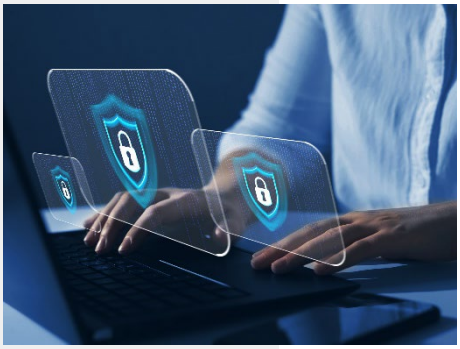
How to identify scams:

1. Never click on links or attachments in an unexpected email even if it looks like it is from a legitimate source.
2. Be wary of unsolicited calls and do not share personal information such as social security, Medicare, or account numbers with callers, via text messages or online.
3. Do not give your personal information to anyone who says they are from the government (IRS, Department of Unemployment, Small Business Association, Social Security Administration, etc.) and want to help you collect your benefits.
4. Do not be pressured by fundraising calls or emails to make immediate donations. Take your time to research the organizations or call us for assistance, if you like.
5. Keep your computers, tablets and mobile devices up to date with the latest operating systems and software. Apply updates and patches when they are issued. Consider installing antimalware software.

If you think you are the victim of identity theft:

1. Notify your bank and financial institutions.
2. Contact the Federal Trade Commission at www.ftc.gov/idtheft or 1-877-IDTHEFT (438-4338).
3. Contact your state Attorney General's office.
4. Contact your local police department.
5. Place a Credit Freeze on your credit file or add a Fraud Alert.
    - A credit freeze will prevent third parties from accessing your credit report. You may place or lift a credit freeze at any time free of charge. However, it may take several days to lift a freeze. Freezes must be placed individually with each of the three credit reporting agencies: Equifax, Experian and TransUnion. A credit freeze does not hurt your credit score.
    - A fraud alert adds a notice to new lenders to take extra precautions when verifying credit applications. A fraud alert typically lasts for one year. If you place a fraud alert with TransUnion, they will automatically notify Equifax and Experian.
6. Talk to your tax preparer about filing a Form 14039, Identity Theft Affidavit with the Internal Revenue Service – in most cases there is no need to file the form.

Educating yourself about potential scams is one of the best ways to protect yourself.



Additional Resources:

- Fair Credit Reporting Act outlines your rights under the FCRA
- IdentityTheft.gov is the official Federal Trade Commission website to report identity theft
- IRS Form 14039 Identity Theft Affidavit for fraudulently filed tax returns
- IRS Identity Protection: Prevention, Detection and Victim Assistance
- Social Security Administration set up an account and more information
- www.annualcreditreport.com to order a free credit report
- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800