

Tax-Related Identity Theft



Your Next Steps

Tax-related identity theft occurs when someone uses your stolen personal information, including your Social Security number, to file a tax return claiming a fraudulent refund. You may be unaware this has happened until you file your return and discover that a return has already been filed using your Social Security number. Alternatively, the IRS may send you a letter saying they have identified a suspicious return related to your Social Security number.

The IRS, state governments, and the tax industry have joined together to create safeguards to fight tax-related identity theft. For information regarding these safeguards and additional resources, please see www.irs.gov/privacy-disclosure/safeguards-program.

If you do become a victim of tax-related identity theft, there are some steps you should take:

- ✓ **Review the Taxpayer Guide.**
Review the Taxpayer Guide to Identity Theft provided by the IRS at www.irs.gov/newsroom/taxpayer-guide-to-identity-theft.
- ✓ **File a report with the Federal Trade Commission.**
File a report with the Federal Trade Commission at www.identitytheft.gov.
- ✓ **File a police report.**
File a police report with your local police department.
- ✓ **Pull your credit report.**
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: www.transunion.com
Experian: www.experian.com
Equifax: www.equifax.com
- ✓ **Close financial or credit accounts.**
Close any financial or credit accounts opened without your permission or tampered with by fraudsters.
- ✓ **Don't panic.**
Generally, the IRS and their authorized private collection agencies contact taxpayers by mail. The letter will provide a reason for the contact and instructions on what to do.
- ✓ **Do respond timely.**
Respond promptly to any IRS notice; call the number provided and inform your tax advisor.
- ✓ **Reply to letter in a timely manner.**
If the letter you receive requires a response by a specific date, taxpayers should reply in a timely manner to minimize additional interest and penalty charges and preserve their appeal rights if they don't agree.

✓ **Do avoid scams.**

The IRS initiates most contacts through regular mail and will never initiate contact with taxpayers by email, text or social media regarding a bill or tax refund. Never click on any unsolicited communication claiming to be the IRS, as it may surreptitiously load malware.

✓ **Contact the IRS if your e-file return was rejected.**

If your e-file return was rejected because of duplicate filing, your Social Security number may have been compromised and contact the IRS.

✓ **Obtain an IRS Identity Protection Pin (IP PIN).**

✓ **Check with your state tax agency to see if there are additional steps to take at the state level.**



Tax-Related Identity Theft Prevention

- Always use security software with firewall and anti-virus protections and use strong passwords. Do not reuse passwords.
- Learn to recognize and avoid phishing emails, which are fraudulent or threatening messages from thieves posing as legitimate organizations, such as banks, credit card companies and even the IRS. If you receive an email from someone claiming to be the IRS and they ask you for personal information, do not respond and forward the message to phishing@irs.gov.
- Obtain an IP PIN through the IRS Identity Protection PIN Opt-In Program for Taxpayers. All taxpayers, not just victims of identity theft, are eligible to receive one at www.irs.gov/ippin.
- Do not click on links or download attachments from unknown or suspicious emails.
- Protect your personal data. Do not carry around Social Security cards and make sure tax records are secure.
- Use a secure method to transfer sensitive data when working with professionals, such as a portal or encryption.
- If possible, always enable two-factor authentication for any online accounts, including email.
- Don't give out personal information on the phone if you receive a call you didn't expect. When in doubt, contact the organization through a trusted website or phone number.

From time-to-time we share third-party articles/information that may be of interest to our clients. These articles are being provided for informational purposes only, do not constitute investment advice and do not necessarily represent the opinions of Homan Wealth Advisors. Homan Wealth Advisors does not provide any guarantee, expressed or implied, that the information presented is accurate or timely, and does not contain inadvertent technical or factual inaccuracies. The past performance of securities is no guarantee of their future result. The value of any investment may fall, as well as rise, and investors may not receive the full amount of their principal at the time of redemption if asset values have fallen.

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 months.

*This document was produced with information from the IRS "Taxpayer Guide to Identity Theft": www.irs.gov/newsroom/taxpayer-guide-to-identity-theft.

© 2023 Buckingham Wealth Partners. Buckingham Strategic Wealth, LLC & Buckingham Strategic Partners, LLC (collectively, Buckingham Wealth Partners). For informational purposes only. Certain information may be based upon third party data which may become outdated or otherwise superseded without notice. Third-party information is deemed reliable, but its accuracy and completeness cannot be guaranteed. Updated August 2023.