



Identity Theft Information for Taxpayers



Identity theft places a burden on its victims and presents a challenge to many businesses, organizations and governments, including the IRS. The IRS combats this crime with an aggressive strategy of prevention, detection and victim assistance.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses your stolen Social Security number (SSN) to file a tax return claiming a fraudulent refund. If you become a victim, we are committed to resolving your case as quickly as possible.

You may be unaware that this has happened until you e-file your return and discover that a return already has been filed using your SSN. Or, the IRS may send you a letter saying it has identified a suspicious return using your SSN.

Know the warning signs

Be alert to possible tax-related identity theft if you are contacted by the IRS about:

- More than one tax return was filed for you,
- You owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages or other income from an employer for whom you did not work.

Steps for victims of identity theft

If you are a victim of identity theft, the Federal Trade Commission recommends these steps:

- File a complaint with the FTC at [identitytheft.gov](https://www.ftc.gov/identitytheft).
- Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
 - www.Equifax.com 1-800-525-6285
 - www.Experian.com 1-888-397-3742
 - www.TransUnion.com 1-800-680-7289
- Close any financial or credit accounts opened by identity thieves

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Respond immediately to any IRS notice; call the number provided.
- Complete IRS [Form 14039, Identity Theft Affidavit](https://www.irs.gov/identitytheft), if your e-file return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at [IRS.gov](https://www.irs.gov), print, then attach form to your paper return and mail according to instructions.

- Continue to pay your taxes and file your tax return, even if you must do so by paper.
- If you previously contacted the IRS and did not have a resolution, contact us for specialized assistance at 1-800-908-4490. We have teams available to assist.

More information is available at: [IRS.gov/identitytheft](https://www.irs.gov/identitytheft) or FTC's [identitytheft.gov](https://www.ftc.gov/identitytheft).

About data breaches and your taxes

Not all data breaches or computer hacks result in tax-related identity theft. It's important to know what type of personal information was stolen.

If you've been a [victim of a data breach](#), keep in touch with the company to learn what it is doing to protect you and follow the "Steps for victims of identity theft." Data breach victims should submit a Form 14039, *Identity Theft Affidavit*, only if your Social Security number has been compromised and IRS has informed you that you may be a victim of tax-related identity theft or your e-file return was rejected as a duplicate.

How you can reduce your risk

Join efforts by the IRS, states and tax industry to protect your data. [Taxes. Security. Together.](#) We all have a role to play. Here's how you can help:

- Always use security software with firewall and anti-virus protections. Use strong passwords.
- Learn to recognize and avoid phishing emails, threatening calls and texts from thieves posing as legitimate organizations such as your bank, credit card companies and even the IRS.
- Do not click on links or download attachments from unknown or suspicious emails.
- Protect your personal information and that of any dependents. Don't routinely carry Social Security cards, and make sure your tax records are secure.

See [Publication 4524, Security Awareness for Taxpayers](#) to learn more.

NOTE: The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.