



Identity Theft

Identity theft presents a challenge to businesses, organizations and governments, including the Internal Revenue Service. Tax-related identity theft occurs when someone uses a stolen Social Security number to file a tax return to claim a fraudulent refund. Although identity theft affects a small percentage of tax returns, it can delay a taxpayer's refund and have a major impact on the victim's peace of mind.

IRS-Impersonation Telephone Scam

Your SSN can be stolen through a data breach, a computer hack or a lost wallet. Recently, an aggressive and sophisticated phone scam targeting taxpayers, including recent immigrants, has been making the rounds throughout the country. Callers claim to be employees of the IRS, but are not. These con artists can sound convincing when they call. They use fake names and bogus IRS identification badge numbers. They may know a lot about you, and they usually alter the caller ID to make it look like the IRS is calling.

Victims are told they owe money to the IRS and it must be paid promptly through a pre-loaded debit card or wire transfer. If the victim refuses to cooperate, they are then threatened with arrest, deportation or suspension of a business or driver's license. In many cases, the caller becomes hostile and insulting.

Sometimes, victims are told they have a refund to try to trick them into sharing private information. If the phone isn't answered, the scammers often leave an "urgent" callback request.

Please remember that the IRS will *never*: 1) call to demand immediate payment, nor will the agency call about taxes owed without first having mailed you a bill; 2) demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe; 3) require you to use a specific payment method for your taxes, such as a prepaid debit card; 4) ask

for credit or debit card numbers over the phone; or 5) threaten to bring in local police or other law-enforcement groups to have you arrested for not paying.

Here are some additional tips to protect yourself from becoming a victim, and steps to take if you discover that someone may have stolen your identity.

Tips to protect you from becoming a victim of identity theft

- Don't carry your Social Security card or any documents that include your Social Security number (SSN) or Individual Taxpayer Identification Number (ITIN).
- Don't give a business your SSN or ITIN just because they ask. Give it only when required.
- Protect your financial information.
- Check your credit report regularly. The IRS suggests you do this every 12 months. We advise you to do it more often, even monthly.
- Review your Social Security Administration earnings statement annually.
- Secure personal information in your home.
- Protect your personal computers by using firewalls and anti-spam/virus software, updating security patches and changing passwords for Internet accounts.
- Don't give personal information over the phone, through the mail or on the Internet unless you have initiated the contact or you are sure you know who you are dealing with.

Know the Warning Signs

Be alert to possible tax-related identity theft. You may receive a notice from the IRS or, in filing your electronic return, we may discover and notify you that:

- 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;
- IRS records indicate you received more wages than you actually earned; or
- Your state or federal benefits (e.g. social security benefits) were reduced or cancelled because the agency received information reporting an income change.

Steps for Victims of Tax-Related Identity Theft

- All victims of identity theft should follow the recommendations of the Federal Trade Commission: **File a report with the local police.**
- File a complaint with the Federal Trade Commission at www.consumer.ftc.gov or the FTC Identity Theft hotline at 877-438-4338 or TTY 866-653-4261.
- Contact one of the three major credit bureaus to place a “fraud alert” on your account:
 - Equifax – www.equifax.com, 800-525-6285
 - Experian – www.experian.com, 888-397-3742
 - TransUnion – www.transunion.com, 800-680-7289
- •Close any accounts that have been tampered with or opened fraudulently.

In addition, if your SSN has been compromised and you know or suspect you may be a victim of tax-related identity theft, take these additional steps:

- Contact us if you receive an IRS notice. We can help you to understand what the notice means and be sure you respond immediately to the IRS request.
- We can also prepare IRS Form 14039, Identity Theft Affidavit, if applicable.
- We encourage you to continue to pay your taxes and file your tax return. Under some circumstances, we will instruct you to do so by paper.
- If necessary, we will work on your behalf with the IRS Identity Protection Specialized Unit to seek a resolution to your identity theft.

The IRS has greatly reduced the time it takes to resolve identity theft cases but please know these are extremely complex cases, frequently touching on multiple issues and multiple tax years. It can be time consuming. A typical case can take about 120 days to resolve with the IRS.

If you take steps to protect your information, you will reduce the risk of identity theft. However, if it becomes necessary, we are here to help you through the entire process and restore your peace of mind.