

Identity Theft and Your Taxes



JAMES F. KIMMEL & ASSOCIATES

Identity Theft and Your Taxes

Your identity and money can be stolen in a tax-related scam via email (“phishing”), fax, phone, or letters. Some recent examples of identity theft scams are:

- **Phone scam.** A bogus phone call where you are told you owe the IRS money and threatened that a warrant will be issued for your arrest. Variations include the threat of other law-enforcement agency intervention, deportation, or revocation of licenses. Some scam artists program their computers to display IRS phone numbers on your caller ID.
- **Email phishing scam.** A bogus email that appears to be from the IRS or a program closely related to the IRS, such as the Electronic Federal Tax Payment System (EFTPS), that attempts to trick you into revealing personal and financial information. The email includes links to bogus websites intended to mirror the official IRS website.
- **Tax transcript.** The bogus email carries an attachment labeled “Tax Account Transcript” or something similar, and the subject line uses some variation of the phrase “tax transcript.” The attachment may contain a computer virus or malware.
- **IRS refunds.** A bogus email, claiming to come from the IRS, tells you that you are eligible to receive a tax refund for a given amount if you just follow the instructions in the email.

Notify the IRS

If you receive a tax-related phishing email, do not click on the links or open any attachments. Forward the email to phishing@irs.gov or call the Treasury Inspector General for Tax Administration at 800-366-4484.

How the IRS Contacts Taxpayers

- The IRS will never initiate contact with you by email or any social media tools to request personal or financial information.
- It is unusual for the IRS to initiate contact by fax or phone call. You can call the IRS at 800-829-1040 to verify that an unexpected fax or phone call is legitimate.

Fraudulent Tax Returns

An identity thief might use your Social Security Number to fraudulently file a tax return and claim a refund. You could be completely unaware that your identity has been stolen until your return is rejected for e-filing or you get an IRS notice or letter.

Rejected e-File

Your electronically-filed return is rejected because the Social Security Number belonging to you, your spouse, or a dependent has already been used on a tax return.

- This situation can occur because of a mistyped number or dispute about claiming a dependency exemption. Such cases do not necessarily indicate identity theft.
- If your return has been rejected because of a previously used Social Security Number, it cannot be e-filed. You must file a paper return.

IRS Notice

You receive an IRS notice or letter stating that:

- More than one return was filed in your name for the year,
- You have a balance due, refund offset, or initiation of collection action for a year when you did not file a return, or
- IRS records indicate that you received wages from an employer you didn’t work for.

Identity Theft and Your Taxes

You should respond immediately to the name and phone number printed on the IRS notice or letter. You will be asked to complete Form 14039, *Identity Theft Affidavit*, and provide identifying information.

IRS Identity Theft Victim Assistance (IDTVA)

If you believe there is a risk of identity theft due to lost or stolen personal information, contact the IDTVA immediately so the agency can take action to secure your tax account.

- Call 800-908-4490.
- You will be asked to complete Form 14039, *Identity Theft Affidavit*.

Form 14039, Identity Theft Affidavit

Form 14039 has two purposes.

- 1) Informs the IRS you are an actual or potential victim of identity theft that has affected or could affect your tax account.
- 2) Requests that the IRS mark your account to identify any questionable activity.

You must provide details of the actual or potential identity theft situation, tax years impacted (if known), address and other contact information, and a photocopy of valid government-issued identification.

Identity Protection PIN (IP PIN) Program

An Identity Protection PIN (IP PIN) is a six-digit number assigned to eligible taxpayers to prevent the misuse of their Social Security Number (SSN) or individual taxpayer identification number (ITIN). Anyone who has an SSN or ITIN and is able to verify their identity is eligible for an IP PIN.

If you filed Form 14039, an IP PIN will be mailed to you each year. Go to www.irs.gov/IPPIN to:

- Retrieve your IP PIN if it was lost or misplaced.
- Sign up for an IP PIN if you are not a victim of identity theft but would like to opt-in to the program. You will need to return to this website each year to obtain your new IP PIN.

There is currently no opt-out option once you are enrolled in the program, but the IRS is working on one for 2022.

Using an IP PIN

If the IRS assigned you an IP PIN, you must use it to confirm your identity on any return filed during the calendar year. A new IP PIN is generated each year. Never share your IP PIN with anyone except your trusted tax provider.

If an IP PIN is missing or incorrect on an e-filed return, the return will be rejected and the correct IP PIN needs to be entered before e-filing again. If an IP PIN is missing or incorrect on a paper return, your return will take longer to process while the IRS verifies your identity.

Surprise IP PIN Letter

The IRS has been known to mail an IP PIN letter to a taxpayer who was previously unaware of a potential tax-related identity theft problem. If you receive an unexpected IP PIN letter, you can call the IDTVA phone number (800-908-4490) to verify that the IP PIN letter is legitimate.

Identity Theft Outside the Tax System

You may be at increased risk for tax-related identity theft for various reasons.

- You have lost or had stolen a wallet, purse, or documents that include sensitive identifying information.
- You have noted questionable credit card activity or credit report information.
- You have fallen victim to an identity theft scam.