



Preventing Tax Identity Theft

Originally published September 28, 2015. Updated to reflect current guidance.

Tax identity theft can turn an ordinary filing season into months of paperwork and uncertainty. A criminal who obtains your Social Security number may use it to file a fraudulent return and claim a refund in your name. You might discover the problem only when your legitimate return is rejected or an unexpected IRS notice arrives.

Protecting yourself starts with recognizing suspicious requests, limiting access to sensitive information, and knowing what to do if something goes wrong.

A Real Case With an Expensive Lesson

In 2014, Georgia resident Mauricio Warner was sentenced to 20 years in federal prison after using stolen identities to file more than 5,000 false tax returns. Victims had provided their names and Social Security numbers in response to promises of government payments.

Warner was ordered to pay more than \$5 million in restitution and forfeit seven bank accounts containing approximately \$4.2 million. His victims did not know returns were being filed in their names. [U.S. Department of Justice: Warner Sentencing](#)

The lesson remains relevant: an offer of easy money can be a way to collect the information needed to impersonate you.

Recognize the Warning Signs of a Scam

Scammers often create urgency. They may promise an unexpected refund, claim your account needs immediate verification, or threaten arrest unless you pay.

The IRS generally begins contact by mail. It does not initiate contact through unsolicited emails, texts, or social media messages to request personal or financial information. Legitimate follow-up calls can occur, so an unfamiliar call alone does not prove fraud.

However, demands for gift cards or prepaid cards, threats of immediate arrest, and pressure to disclose sensitive information are strong warning signs. Hang up and verify the matter through contact information you obtain independently from the IRS. [IRS: Recognizing Impersonation Scams](#)

Don't click a suspicious message's links or open its attachments. Report IRS-related phishing emails to phishing@irs.gov, following the agency's reporting instructions. [IRS: Report Fraudulent Messages](#)

Go Directly to the Source

An official-looking logo doesn't establish that a message or website is genuine. Neither does a familiar name on caller ID.

Rather than following a refund link in a message, type **IRS.gov** into your browser and navigate from there. Legitimate IRS services may use subdomains, so a web address does not have to begin with "www.irs.gov" to be authentic.

If a letter seems suspicious, verify it through IRS customer service or your IRS Online Account before providing information or making a payment. [IRS: Verifying Contact](#)

Freelancer Example: A Fake Client Requests Tax Information

Imagine Elena, a freelance graphic designer, receives an email from someone offering a \$2,400 project. Before discussing the work, the supposed client asks her to upload a completed W-9, a copy of her driver's license, and banking credentials through a link.

A real client may need a W-9 for tax reporting. That familiar request can make the rest of the message seem credible.

Elena pauses. She contacts the company through a phone number she finds independently and learns that the sender does not work there. She avoids the link and provides no documents.

For freelancers, the practical lesson is to verify who is requesting tax information and why. Use an agreed, secure method to transmit necessary documents. A client paying an invoice does not need your bank password.

Protect Your Information Throughout the Year

Keep your Social Security card and tax records in a secure location. Avoid carrying documents containing your Social Security number unless you need them, and ask why the number is required before sharing it.

Protect digital records as carefully as paper files:

- Use unique passwords and enable multifactor authentication where available.
- Keep devices and security software updated.
- Use a secure document portal when exchanging tax records.
- Avoid handling sensitive documents on shared computers.
- Limit access to stored returns, identification documents, and financial records.

File promptly once you have complete, accurate information. Early filing may reduce the opportunity for someone else to file first, but it is not a guarantee against identity theft. [IRS: Identity Theft Prevention](#)

Add Protection With an IRS Identity Protection PIN

An **Identity Protection PIN**, or **IP PIN**, is a six-digit number that helps prevent someone else from filing a federal tax return using your Social Security number or individual taxpayer identification number.

You do not have to be an identity theft victim to request one. Eligible taxpayers who can verify their identity can enroll proactively.

An IP PIN is valid for one calendar year. Use the appropriate current PIN when filing, and share it only with a trusted tax professional who needs it to prepare your return. Start with the IRS's official enrollment page. [IRS: Get an IP PIN](#)

Know the Signs of Tax Identity Theft

Potential warning signs include:

- An electronic return rejected because your Social Security number was already used.
- An IRS inquiry about a return you did not file.
- Unexpected tax account activity or notices about unfamiliar income.
- Wage documents from an employer you do not recognize.

These issues deserve prompt attention, but they do not always prove theft. A duplicate filing rejection, for example, may also involve an error. Confirm the details before deciding how to respond. [IRS: Identity Theft Guide](#)

What to Do if Someone Uses Your Identity

Respond to verified IRS correspondence. Follow the instructions in a legitimate notice, including any request to verify whether you filed a return.

Determine whether Form 14039 is needed. The Identity Theft Affidavit is used in certain tax identity theft situations. Some IRS verification letters direct you to a different process and do not require a separate affidavit. Follow the instructions for your circumstances rather than automatically submitting the form. [IRS: When to File an Identity Theft Affidavit](#)

Continue meeting your tax obligations. Identity theft does not remove the responsibility to file and pay. If you cannot file electronically, follow IRS instructions for submitting your legitimate return on paper. Keep copies of your correspondence and proof of submission. [IRS: Victim Assistance](#)

Address the wider damage. Visit [IdentityTheft.gov](https://www.identitytheft.gov) for a recovery plan. Contact affected financial institutions and secure compromised accounts. Consider placing a free credit freeze with each of the three nationwide credit bureaus—Equifax, Experian, and TransUnion—to help prevent new credit accounts from being opened in your name. A credit freeze does not replace the IRS recovery process. [FTC: Identity Theft Recovery](#), [FTC: Credit Freezes](#)

Stay Organized While the IRS Investigates

Resolving tax identity theft can take considerable time. Keep a folder containing notices, submitted forms, payment records, and a dated log of conversations.

Avoid sending duplicate affidavits in an effort to speed things up; the IRS warns that duplicate submissions can delay resolution. Follow the agency's instructions for your case. [IRS: How Victim Assistance Works](#)

Protecting your tax identity is an ongoing habit. Verify unexpected requests, safeguard your records, and respond promptly to confirmed problems. If identity theft occurs, use the IRS and FTC recovery resources to work through the next steps.