Your Monthly Money

brought to you by KOFE® Knowledge of Financial Education

A product of Consolidated Credit® When debt is the problem, we are the solution.

4 Tips to Prevent Tax ID Theft

Take these four steps to help protect your tax refund this year.

What is tax ID theft?

Tax identity theft occurs when someone steals your Social Security number in order to file a false tax return in your name. The goal is to get your refund before you even have a chance to file a return. You may not even know you're at risk until you try to file and the IRS tells you a return was already filed in your name.
Unfortunately for everyone, tax identity theft doesn't discriminate. Anyone with a Social Security number is vulnerable. Criminals even prey on children's identities during tax season so they can claim them as dependents and get a deduction.

The good news is that in recent years, cases of tax ID theft have been vastly reduced. According to the IRS, ID theft cases dropped 40% from 2016 to 2017. Hopefully, that trend continues. In the meantime, it's best to prepare yourself for tax identity theft before it happens. That's why federal agencies have Tax Identity Theft Awareness Week. It's a week at the beginning of tax season that encourages taxpayers to protect their identities and their refunds. This year, it runs from January 30 through February 3rd. So, let's look at four things you could do next week to protect yourself from tax ID theft.
4 ways to help keep your refund out of someone else's hands

1. File as early as possible

Tax identity theft relies on fraudsters getting a return submitted in your name before you do. If someone has your Social Security number (SSN), they can accomplish this relatively easily. Filing your return early keeps them from being able to file fraudulently. This way, you are the only one who gets to cash in on your tax return.
Once you have all of your W2s, don't wait! File immediately so you can get your refund and avoid a giant hassle. Also, remember your 1095s – they are still required this year.

2. Take steps to protect your Social Security number

Your Social Security number is necessary for a fraudster to use your identity for tax ID theft. Taking steps to protect your SSN helps you minimize the risk of tax identity theft (and a host of other problems).
There are standard best practices that you can follow:
Don't carry your Social Security card in your wallet or purse
Keep your cards locked up at home
Get a locked mailbox and retrieve your mail promptly every day

Shred documents that include your SSN and other personal data before you toss them
Avoid putting your SSN on forms at doctors' offices, hospitals, and other service providers – even if they ask for it, see if it's required
Additionally, you can register your Social Security number at www.ssa.gov/myaccount to open a "my Social Security account" online. This account allows you to check your Social Security statements anytime you want. It also shows your earnings, which can reveal that someone has gotten a job using your number. It's another sure sign of SSN identity theft.

3. Sign up for an Identity Protection PIN (IP PIN)

This year, the IRS announced they have a new tool that can help taxpayers protect their refunds. It's called an Identity Protection PIN. It's a 6-digit number that a taxpayer sets up that must be submitted when they submit their returns. This number is known only to the taxpayer and the IRS.
You can set up your IP PIN through the IRS website at Get an IP PIN. You will go through what the IRS describes as a "rigorous identity verification process" to confirm you are really whom you say you are. Then you can select your PIN.

IP PINs are only valid for one year, so if you sign up for a PIN now it will be good for one year. When you submit your returns this year, you would provide the IP PIN to verify your identity. If you e-file, your unique identity protection PIN must be provided to submit your return electronically. If you file a paper return by mail, you will provide your PIN next to your signature.
If the IP PIN is not provided when a return is submitted in your name, the return will be rejected. This ensures that tax scammers cannot file a return in your name, even if they have your Social Security number. It's an added layer of protection that may be worth the time it takes to set up, especially if your identity has been compromised.

4. Only trust-mailed IRS communications

Whether you've already filed or not, you should never trust any communication from the IRS unless it's an official, mailed letter. The IRS will never email you, text you, call you on a phone (even your home landline) or send you a message over social media to initiate contact. If someone contacts you any other way claiming to be the IRS, it's a scam!
The most common type of this scam is IRS collections. Someone calls or texts claiming to be an employee of the IRS, stating you owe money and must pay immediately. They may even offer all or part of your SSN as proof that they are whom they say they are. They aren't.
If someone contacts you about an IRS collection action, verify it first before you give them anything. You can call an IRS collection hotline at 1-800-829-1040 to confirm that you owe federal taxes.