# Taxpayer ID Theft and Refund Fraud


You receive a telephone call from an IRS agent who informs you that the agency is holding a refund for you, but needs you to verify your personal information: your name, date of birth and Social Security number. You check your caller ID and it tells you it *is* the IRS calling, so you give the agent your personal information. Or, you receive an email from the IRS that directs you to "update your IRS e-file immediately." You Google IRS and, lo and behold, the website looks exactly like the site that sent you the email. You think everything is legit, so you comply and give up your personal information. But, you have been scammed, and you will likely not discover the deception until you file your taxes and the IRS flags your return as a duplicate. This is when you realize that you have become the victim of a crime.

**What is taxpayer ID theft and refund fraud**? According to the IRS Taxpayer Guide to Identity Theft, taxpayer ID theft and refund fraud occurs when someone uses your Social Security number to file a tax return claiming a fraudulent refund. It is not just credit and debit cards that cyber hackers are after these days, says the Federal Trade Commission. Cyber thieves resort to different tactics, like IRS-impersonation telephone calls, spoof websites and email phishing scams, to obtain your Social Security number and other key pieces of your personal information in order to file a fraudulent tax return and claim your refund. These scammers generally file the fraudulent return early in the season, beating you to the punch. Tax-related ID theft is growing rapidly, and one of the main reasons for the growth is that it takes so little to file a false claim. A criminal needs only your name, Social Security number and date of birth to file a tax return, and falsified W-2 information to attempt to claim a refund.

**So, fraudsters filed a tax return in your name. Now what?** If your Social Security number has been compromised, or you know or suspect you are a victim of taxpayer ID theft or refund fraud, the IRS Taxpayer Guide to Identity Theft recommends that you immediately take the following steps:

**Step one:** Report the incident to the IRS and respond immediately to any IRS notice by calling the number provided.

**Step two:** Complete IRS Form 14039 (www.irs.gov/pub/irs-pdf/f14039.pdf). The agency will require that you submit IRS Form 14039, Identity Theft Affidavit, to prove that you're the real taxpayer. Check Box 1 under Section A of that form to indicate that someone has stolen your identity and it has affected your tax account since a return was filed using your identifying information. You will also need to provide information about the tax year affected and the last return you filed prior to the ID theft.

If the identity of a deceased spouse or relative was stolen and his/her Social Security number used to file a fraudulent return, you will also use Form 14039 to alert the IRS of the fraud. (See Consumer Action's fact sheet on Theft of a Deceased Person's Identity: www.consumer-action.org/downloads/outreach/2015_deceased_ID_theft.pdf.)

If your identity has been compromised and fraudulently used to obtain credit, or if you were the victim of a home robbery or a purse snatching and your Social Security card was stolen, Form 14039 can also be used to notify the IRS of the incident.

After you complete Form 14039, mail it with a copy of your Social Security card, driver's license, U.S. passport, military ID or other form of government-issued identification. If you received an IRS notice concerning the fraudulent return, include a copy of the notice as well.

**Step three:** File your tax return. Even if an ID crook has already filed a fraudulent tax return using your identity, you must file a return. If you're unable to file your return electronically because the thief filed first, you must attach Form 14039 and documentation to a paper return and submit all to the IRS.

**Step four**: Complete the FTC's online complaint form at www.ftc.gov. Based on the information you enter, the FTC complaint system will create your Identity Theft Affidavit. Use the affidavit to file a report with your local police department. (You can also call the FTC Identity Theft Hotline at 877-438-4338/TTY 866-653-4261 to complete or update your affidavit.) Then, summon a bit of patience. You must come to grips with the notion that it could take months to not only sort through this process, but to receive your tax refund.

**Step five:** Act quickly to alert your financial institutions—bank, credit union and credit card companies—about the fraud. Contact the fraud departments of the three major credit bureaus (Equifax, Experian and TransUnion) to request that an initial fraud alert be placed on your credit file. After you assess the damage, you may want to consider obtaining a credit freeze. When someone has enough of your personal information to file a fraudulent tax return, he or she could use it for other purposes. Thieves don't just use your information once and discard it—they typically use it again and again. The faster you act, the less time they have to do damage. (For additional information on a fraud alert or credit freeze, see Consumer Action's MoneyWi$e ID Theft training module: www.consumer-action.org/modules/module_id_theft_and_account_fraud.)

**Step six:** Get an Identity Protection PIN from the IRS. This is a six-digit number created for eligible taxpayers to help prevent future fraudulent use of their Social Security number. If you have been a victim of identity theft, the IRS will send you a notice inviting you to apply for a PIN. However, according to an article that appeared in *U.S. News & World Report*, if you live in Florida, Georgia or Washington, D.C., where there is a high incidence of taxpayer ID theft and refund fraud, it may be a good idea to get the Identity Protection PIN, or IP PIN, anyway, for an added layer of protection against taxpayer ID theft and refund fraud.

**How can you protect yourself against fraud?** You can't protect yourself one hundred percent from all forms of ID theft, but you can certainly reduce your risk of becoming a victim of taxpayer ID theft and refund fraud by taking a few of the following precautions.

- File your tax return early in the tax season, if you can, and use a secure Internet connection if you file electronically, or mail your tax return directly from the post office.
- Research a tax preparer thoroughly before you hand over your personal information.
- If your Social Security number has been compromised in a data breach or otherwise, contact the IRS ID Theft Protection Unit at 800-908-4490 and request an Identity Protection PIN.
- 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 whom you are dealing with.
- Protect your financial information while online, and check your credit report at least once a year at www.annualcreditreport.com to make sure no fraudulent accounts have been opened in your name.
- Check your Social Security Administration earnings statement annually.
- Protect your personal computer and mobile devices by using firewalls and anti-spam/virus software, by updating security software and by password-protecting your devices and accounts. (For additional information on how to protect your devices and accounts from fraud, see Consumer Action's Put a Lock On training module: www.consumer-action.org/modules/module_internet_security_and_privacy.)

**Resources:**

- Taxpayer Guide to Identity Theft (IRS): www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft
- Beating Tax Refund Fraud Happens Early (AllClear ID): www.allclearid.com/blog/beating-tax-refund-fraud-happens-early
- Tax Scams/Consumer Alerts (IRS): www.irs.gov/uac/Tax-Scams-Consumer-Alerts