TAXPAYER GUIDE TO IDENTITY THEFT

# Identity Theft Help At a Glance

If your SSN has been compromised, take these steps:

File a Federal Trade Commission (FTC) complaint and/or a police report.

Contact all of the three (3) credit bureaus to place a lock and fraud alert on your account:

* [www.Equifax.com](http://www.Equifax.com),
* 1-800-525-6285
* [www.Experian.com](http://www.Experian.com)
* 1-888-397-3742
* [www.TransUnion.com](http://www.TransUnion.com)1-800-680-7289

Close any financial accounts opened without your permission.

Respond immediately to any IRS notice, according to instructions.

We will complete IRS Form 14039, Identity Theft Affidavit for you.

Continue to file your tax return, even if by paper.

Other Resources:

[www.irs.gov](http://www.irs.gov)

[www.ftc.gov](http://www.ftc.gov)

IRS publication 5027, Identity Theft Information for Taxpayers.

Identity theft is a frustrating process for victims. We are committed to working with you to resolve your case as quickly as possible, if necessary.

REDUCE YOUR RISK, BE PROACTIVE AND CONSIDER THE FOLLOWING:

* Placing a lock on your credit reports (see list of credit bureaus in box on right).
* Monitoring your credit reports AT LEAST once per year.
* Putting a cap or ceiling on credit card and debit card transactions – for example, a $500 limit per transaction:
  + Have a lower spending limit per transaction placed on ATM and debit cards – for example, a $100 limit per transaction.
  + Require credit card companies to text and/or call for your authorization approval and password when the spending limit is exceeded.
* Monitoring credit card statement activity closely:
  + Follow up on ANY suspicious activities no matter how small or insignificant the amount.
* Going online and monitoring your checking account activity and/or credit card activity periodically each month.
* Keeping your Social Security Card or any other document with your SSN on it in a secure location.
* Checking your Social Security Administration earnings statement annually.
* Giving a business or doctor’s office your SSN only when absolutely necessary – not just because they ask for it.
* Protecting your personal financial information at home and on your computer:
  + Protect your personal computers by using firewalls, anti-spam/virus software, update security patches and change passwords for Internet accounts frequently.
* Giving personal information over the phone, through the mail or the Internet should be avoided at all cost unless you have either initiated the contact or are sure you know who is asking.

WHAT IS TAX-RELATED IDENTITY THEFT?

Tax-related identity theft occurs when someone uses your stolen Social Security Number (SSN) to file a tax return claiming a fraudulent refund.

Generally, an identity thief will use your SSN to file a false return early in the year. You may be unaware you are a victim until you file your tax return and learn one already has been filed using your SSN.

KNOW THE WARNING SIGNS:

Be alert to possible identity theft if you receive an IRS notice or letter that states that:

* More than one tax return was filed using your SSN.
* You owe additional tax, 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 wages from an employer unknown to you.

STEPS TO TAKE IF YOU BECOME A VICTIM:

* Report identity theft at [www.ftc.gov](http://www.ftc.gov) or at [www.irs.gov/identitytheft](http://www.irs.gov/identitytheft) and learn how to respond to it at [www.identitytheft.gov](http://www.identitytheft.gov).
* Contact all of the three (3) major credit bureaus to place a ‘fraud alert’ on your credit records:
* Equifax, [www.Equifax.com](http://www.Equifax.com), 1-800-525-6285
* Experian, [www.Experian.com](http://www.Experian.com), 1-888-397-3742
* TransUnion, [www.TransUnion.com](http://www.TransUnion.com), 1-800-680-7289
* Contact your financial institution, and close any accounts opened without your permission or tampered with.
* Consider filing a police report.

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, take these additional steps:

* Respond immediately to any IRS notice; call the number provided by the IRS on the notice.
* We will complete IRS Form 14039, Identity Theft Affidavit for you. You will need to include a copy of your driver’s license or passport, cell phone number or home number so that the IRS knows you are the victim of identity theft and not the person committing the fraud.
* Continue to pay your taxes and file your tax return, even if you must do so by paper. If you are expecting a refund, please be aware that it could be delayed six (6) months to one (1) year before you receive it.

If you previously contacted the IRS and did not have a resolution, contact the Identity Protection Specialized Unit at 1-800-908-4490. Teams will be available to assist you.

The IRS does not initiate contact with taxpayers by phone or email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels. ALL documents related to this matter MUST be mailed through the Post Office by Certified Return Receipt Requested.

Report suspicious online or emailed phishing scams to: [phishing@irs.gov](mailto:phishing@irs.gov). For phishing scams by phone, fax or mail, call: 1-800-366-4484. Report IRS impersonation scams to the Treasury Inspector General for Tax Administration’s IRS Impersonation Scams Reporting.

See the main Identity Protection page on [www.irs.gov](http://www.irs.gov) for more information.

Identity Protection Personal Identification Number (IP PIN)

What’s an IP PIN?

An IP PIN is a six-digit number assigned to eligible taxpayers that helps prevent the misuse of your Social Security number on fraudulent federal income tax returns. You cannot use an IP PIN as your e-file signature PIN.

## **Getting Your IP PIN:**

## To get your IP PIN, you must verify your identity online at [www.irs.gov](http://www.irs.gov) or call 1-866-704-7388. If online, type IP PIN in the search bar and select the appropriate link. You will need to have immediate access to your email account to receive a confirmation code. If you are eligible, you will receive your IP PIN online once the IRS verifies your identity. The IRS will send you a new IP PIN each December by postal mail.

## **Retrieving Your IP PIN:**

## If you lost your IP PIN or you did not receive a new one, you can retrieve it by following the three (3) steps on www.irs.gov for “Getting Your IP PIN.” You will receive your most current IP PIN after the IRS verifies your identity.

If you are unable to retrieve your IP PIN or use the “Get an IP PIN online tool” on www.irs.gov, you may call the Identity Theft Specialized Unit at 1-800-908-4490 to obtain a replacement IP PIN. You must verify your identity and a replacement IP PIN will be issued to you. However, please know that the use of a replacement IP PIN will subject your tax return to greater review and may mean a delay in processing your refund. Visit “[Retrieve Your Lost or Misplaced IP PIN](https://www.irs.gov/Individuals/Lost-or-Misplaced-IP-PINs)” on [www.irs.gov](http://www.irs.gov) for details.