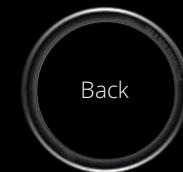


Identity theft

Look again at how you safeguard your personal financial information. While the IRS has made solid strides toward reducing the number of individual and entity identity theft instances, you still need to remain vigilant about your personally identifiable information. In 2018, you should also be prepared for the IRS to be inquiring about new information to assist it in verifying your true identity. Your tax adviser can help you take another look at how to guard yourself from identity theft or how to respond if it occurs.



Identity theft

How to protect yourself

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.

Personal tax-related identity theft

All too often in recent years, a taxpayer goes to file an individual income tax return and finds that, unbeknownst to him or her, a return has already been filed on the taxpayer's behalf. Tax-related identity theft occurs when someone uses your personal information, such as your name, Social Security number (SSN), or other information, without your permission to file a tax return claiming a fraudulent refund. All income levels of the US population have experienced tax-related identity theft. It is typically discovered when you attempt to e-file and learn that a tax return has already been filed with your SSN. This erroneous filing can affect your income tax filing obligations or available credits. It also leaves you open for further fraudulent use of your SSN.

If you believe you are a victim of tax-related identity theft, you should contact the IRS immediately. If you are unsure and would like someone to assist with determining if you have been a victim, then you could also contact your tax adviser. Your adviser can use Form 2848, Power of Attorney and Declaration of Representative, to secure IRS transcripts of your

account to determine if the fraudulent return has been processed. If you are a victim, then you should file and submit Form 14039, Identity Theft Affidavit, to the IRS. After receipt of Form 14039 by the IRS, it will be subject to an accuracy review. If accepted and processed by the IRS, the IRS will send you a CP01A Notice with an Identity Protection Personal Identification Number (IP PIN).

Your IP PIN can be used when filing electronic or paper returns. If you do not use your IP PIN, then your electronic return will be rejected and your paper return will be subject to additional screenings to validate your identity, which will delay your refund (if applicable). Each IP PIN can be used only once. Thereafter, a distinct IP PIN will be issued systematically on an annual basis in December. Even if you are a victim, you still must continue to pay your taxes and file your tax returns, even if you must do so by paper. The IP PIN will eliminate any delay in processing the valid tax returns.

Additionally, if you have been subject to identity theft, there are other steps that you can take to protect yourself. You should contact any respective state tax agencies, file a report with local law enforcement, and file a complaint with the Federal Trade Commission (www.ftc.gov/complaint). In general, you should contact one of the three major credit bureaus to place a "fraud alert" on your credit records and monitor your credit reports. If any of your financial accounts have been affected, then you should contact the financial institutions and close them. It is also a good idea to check your Social Security Administration earnings statement annually to reconcile your earnings with what was reported.

How to
protect yourself

IRS initiatives to
prevent identity theft

Identity theft at the
entity level

Back

Forward

Identity theft

How to protect yourself



Warning signs for individuals

- ! You owe additional tax, refund offset, or have collection actions against you for a year you did not file a tax return
- ! You receive an unexpected tax transcript or IRS notice that does not correspond to anything submitted by you
- ! IRS records indicate that you received wages from an employer unknown to you
- ! You are impacted by a data breach (for example, improper disposal of personally identifiable information in the trash or a sophisticated cyberattack on corporate computers by criminals)
- ! High risk: data breach of SSN and financial data (such as wage information)
- ! Low risk: credit card numbers, health records without SSNs, driver's license numbers
- ! You lost a cell phone
- ! Your mail was stolen
- ! You receive confirmation of a change of address when your address did not change

How to mitigate your individual risk

- * Do not give a business your SSN just because it asks; only provide this information when absolutely necessary
- * Check your credit report annually
- * Check your Social Security Administration earnings statement annually
- * Protect your personal computers by using firewalls and anti-spam/virus software, updating security patches, and changing passwords for Internet accounts
- * Do not give personal information over the phone, through the mail, or via the Internet unless you have either initiated the contact or are sure you know who is asking
- * Change all financial account and email passwords on a regular basis

How to
protect yourself

IRS initiatives to
prevent identity theft

Identity theft at the
entity level

Identity theft

IRS initiatives to prevent identity theft

IRS's new initiatives to stop individual tax-related identity theft

The IRS does not initiate contact with taxpayers by phone or email to request personal or financial information. To reinforce that fact, the IRS started an education series called “Don't Take the Bait,” which focuses on vigilance toward computer security and warns about email scams dubbed “spear phishing” in which senders identify themselves as a friend, customer, or company. You should not respond to the IRS via any type of electronic communication, such as text messages and social media channels. Also, remember that the IRS does not call taxpayers with threats of lawsuits or arrests.

If you change your address, then you should expect the IRS to send a change of address letter to both the new address and the old address.

You may also have noticed in 2017 that the IRS and/or state tax agencies asked for your driver's license number or a state-issued identification number. This information is optional for most state tax returns, but a few states do require it to complete the electronic filing process. It is also optional for a federal tax return. However, providing these identification numbers helps the IRS verify your identity, which can prevent unnecessary delays in tax return processing.

In 2018, there will be a new verification code box on all official Forms W-2. Piloted in 2017, the verification code is a 16-digit alphanumeric code that taxpayers and tax preparers enter when prompted by their software product. The objective is to verify the information at the point of filing and prevent

fraudsters from using fake Forms W-2 to create fraudulent refunds. Both the IRS and the states will receive several new data elements from individual returns that will help improve authentication of the taxpayer and identify possible identity theft scams.



How to
protect yourself

IRS initiatives to
prevent identity theft

Identity theft at the
entity level

Back

Forward

Identity theft

IRS initiatives to prevent identity theft

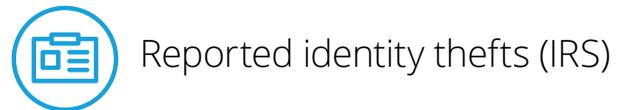
How to
protect yourself

IRS initiatives to
prevent identity theft

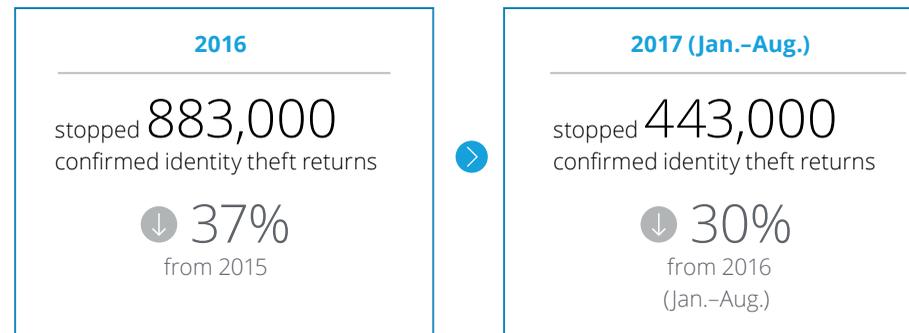
Identity theft at the
entity level

Making progress against individual identity theft returns

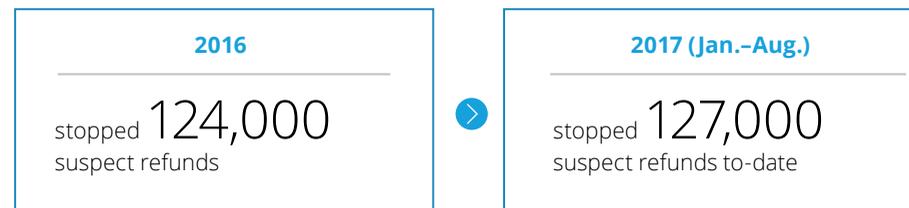
Decreased incidences of reported and confirmed individual identity theft returns



IRS



Financial institutions



Back

Forward

Identity theft

Identity theft at the entity level

Identity theft at the entity level

The IRS has expanded its efforts to better protect pass-through and corporate entity filers and identify suspected identity theft returns. This includes C and S corporations, partnerships, estates, and trusts. For example, if a corporation or pass-through entity files Form 4466, Corporation Application for Quick Refund of Overpayment of Estimated Tax, the IRS will ask for confirmation of the filing before issuing the refund. It is also common for entity taxpayers to receive a notice confirming the responsible party for the corporation. If an estate or trust receives such a notice, it is to confirm the trustee as a responsible party.

Common business scams

Identity theft perpetrators often attempt to steal employee Forms W-2 or business employer identification numbers (EINs) to create fake Forms W-2 or 1099s. This data is then used to file fraudulent individual return filings seeking refunds. Information on reporting such scams is available in the IRS publication Form W-2/SSN Data Theft: Information for Businesses and Payroll Service Providers. The perpetrators may also use Schedule K-1 data to file fraudulent individual returns on behalf of shareholders, partners, or beneficiaries. Additionally, there has been an increase in fraudulent trust and estate return filings, including both on behalf of existing entities and those established using stolen individual taxpayer information. All entities should be certain to protect their computers and data to guard against identity theft and refund fraud.

IRS initiatives to prevent entity identity theft

Person signing the return	<ul style="list-style-type: none">• The name and SSN of the company executive authorized to sign the corporate tax return.• Is this person authorized to sign the return?
Payment history	Were estimated tax payments made? If so: <ul style="list-style-type: none">• When?• How?• How much?
Parent company information	Is there a parent company? <ul style="list-style-type: none">• Name, EIN, address of parent company.
Filing history	Has the business filed: <ul style="list-style-type: none">• Form 940?• Form 941?• Other business-related tax forms?

 Additional information may be requested based on deductions claimed.

Warning signs for entities

As with fraudulent individual returns, there are certain warning signs that may indicate entity identity theft. Business, partnerships, and estate and trust filers should be alert to potential identity theft and contact the IRS if they experience any of these issues:

- An extension to file request is rejected because a return with the EIN or SSN is already on file
- An e-filed return is rejected because a duplicate EIN/SSN is already on file with the IRS
- Failure to receive expected and routine correspondence from the IRS, which may indicate a criminal has changed the address

Look again at how you safeguard your personal financial information

While the IRS has made solid strides toward reducing the number of individual and entity identity theft instances, you still need to remain vigilant about your personally identifiable information. In 2018, you should also be prepared for the IRS to be inquiring about new information to assist it in verifying your true identity. Your tax adviser can help you take another look at how to guard yourself from identity theft or respond if it occurs.

How to
protect yourself

IRS initiatives to
prevent identity theft

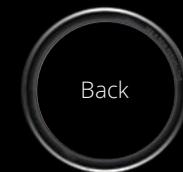
Identity theft at the
entity level

Back

Forward

Resources

Private wealth	Deloitte Private Wealth Private Wealth brochure
Tax reform	Tax Reform insights Tax News & Views: Capitol Hill briefing
Individual income tax planning	Private wealth tax controversies: Deep experience navigating interactions with taxing authorities
Wealth transfer planning	Wealth planning: Securing your legacy US estate and gift taxation of resident aliens and nonresident aliens
Philanthropy	Private foundations: Establishing a vehicle for your charitable vision
Identity theft	IRS Identity Protection Specialized Unit: +1 800 908 4490 IRS.gov, Identity Protection: Prevention, Detection and Victim Assistance IRS.gov, Taxpayer Guide to Identity Theft IRS.gov, Identity Theft Guide for Business, Partnerships and Estate and Trusts Helpful resources: Publications, articles, YouTube videos and other identity theft related outreach IRS.gov, Tax Scams / Consumer Alerts IRS.gov, IRS Publication 5027, Identity Theft Information for Taxpayers Federal Trade Commission: Consumer Information, Identity Theft



Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2017 Deloitte Tax LLC. All rights reserved.