Tax-Related Identity Theft

Quick Guide for Tax Professionals and Taxpayers to help Protect, Prevent and Resolve

NATP™
National Association of Tax Professionals

Last updated September 2017.

Warning Signs

Tax-related identity theft occurs when someone uses a stolen social security number (SSN) to file a tax return claiming a fraudulent refund. Thieves also may use stolen Employer Identification Numbers to create false Forms W-2 to support refund fraud schemes.

Warning signs for individual clients

Your client's SSN has been compromised, putting them at risk when:

- A return is rejected; IRS reject codes indicate the taxpayer's SSN already has been used to file a tax return.
- Your client observes activity or receives IRS notices regarding a tax return after all tax issues have been resolved, refund has been received or account balances have been paid.
- An IRS notice indicates your client received wages from an employer unknown to them.

Remember: You must have a power of attorney on file and authenticate your identity before an IRS customer service representative can provide you with any taxpayer information.

Warning signs for business clients

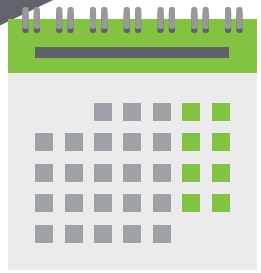
Business identity theft happens when someone creates, uses or attempts to use the identifying information of a business, without authority, to obtain tax benefits. Business identity thieves file fraudulent business returns to receive refundable business credits or to perpetuate individual identity theft. Signs include:

- Your client's return is accepted as an amended return, but the taxpayer has not filed a return for that year.
- Your client receives IRS notices about fictitious employees.
- Your client notices activity related to or receives IRS notices regarding a defunct, closed or dormant business after all account balances have been paid.

Quick Protection Tips

Here are some tips to protect you and your clients from becoming a victim.

Don't carry your social security card or any documents that include your social security number (SSN) or Individual Taxpayer Identification Number (ITIN).



Check your credit report and your Social Security Administration earnings statement every 12 months.

Don't give a business your SSN or ITIN just because they ask. Give it only when required.

Protect your personal and financial information.

Protect your personal computers by using fire-walls and anti-spam/virus software, updating security patches and changing passwords for Internet accounts.

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 who you are dealing with.

Detailed Security Awareness

Keep Your Computer Secure

- Use security software and make sure it updates automatically; essential tools include:
  - Firewall
  - Virus/malware protection
  - File encryption for sensitive data
- Treat your personal information like cash, don't leave it lying around.
- Check out companies to find out who you're dealing with.
- Give personal information only over encrypted websites – look for "https" addresses or a lock icon in the right corner of the address bar.
- Use strong passwords and protect them.
- Back up your files.

Avoid IRS Impersonators

- The IRS will not call you with threats of jail or lawsuits.
- The IRS will not send you an unsolicited email suggesting you have a refund or that you need to update your account.
- The IRS will not request any sensitive information online.

These are all scams, and they are persistent. Don't fall for them.

Avoid Phishing and Malware

- Avoid phishing emails, texts or calls that appear to be from the IRS and companies you know and trust, go directly to their websites instead.
- Don't open attachments in emails unless you know who sent it and what it is.
- Download and install software only from websites you know and trust.
- Use a pop-up blocker.
- Talk to your family about safe computing and not providing personal information over the phone to unknown people.

Protect Personal Information

- Don't routinely carry your social security card or documents with your SSN.
- Do not overshare personal information on social media. Information about past addresses, a new car, a new home and your children help identity thieves pose as you.
- Keep old tax returns and tax records under lock and key or encrypted if electronic.
- Shred tax documents before trashing.

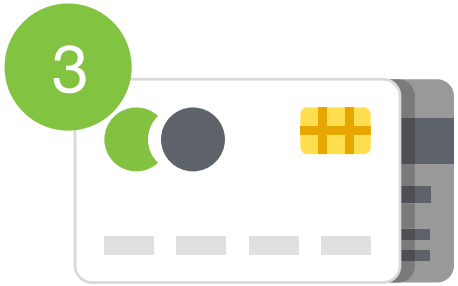
Victim of Identity Theft – Now What?

For all victims of identity theft, the Federal Trade Commission recommends these steps:

File a complaint with the FTC at identitytheft.gov.

Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:

- Equifax, Equifax.com, 800.766.0008
- Experian, Experian.com, 888.397.3742
- TransUnion, TransUnion.com, 800.680.7289



Contact your financial institutions, and close any financial or credit accounts opened without your permission or tampered with by identity thieves.

Tax Return Compromised

If your e-filed tax return is rejected because of a duplicate filing under your SSN and you haven't filed already, you may be a victim of identity theft.

Report this to the IRS by following these steps:

1. Download IRS Form 14039, *Identity Theft Affidavit*.
2. Complete the form for each taxpayer that has been rejected. *Note: In Section B, you'll be checking box 1.*
3. Print the form and attach your correct tax return and form of identification.
4. Mail or fax according to instructions.

It may take several weeks for the IRS to process Form 14039, but once it's been processed, you'll receive an acknowledgement letter.

Your case will be then sent to the Identity Theft Victim Assistance (IDTVA) organization if another return is already present on the account (the fraudulent return), where it will be handled by employees with specialized training.

The Identity Theft Victim Assistance organization will:

- Assess the scope of the issues and try to determine if your case affects one or more tax years.
- Address all the issues related to the fraudulent return. This includes determining if there are additional victims, who may be unknown to you, listed on the fraudulent return.
- Research the case to double check whether all the names, addresses and SSNs are accurate or fraudulent.
- Conduct a case analysis to determine if all outstanding issues were addressed.
- Ensure your tax return is properly processed and if you are due a refund, release your refund.
- Remove the fraudulent return from your tax records.
- Mark your tax account with an identity theft indicator, which completes the work on your case and helps protect you in the future.

You will receive notification that your case has been resolved. This is generally within 120 days but complex cases may take 180 days or longer.

It is also recommended that you reach out to your State Department of Revenue.

Receive IRS Notice of Fraud

Stopping identity theft and refund fraud is a top priority for the IRS. IRS programmers work with major software providers to stop fraud. Plus, IRS systems have several built-in identifiers to flag suspicious returns.

When a return is identified as suspicious by the IRS Taxpayer Protection Program bearing your name and SSN, they will send you a notice or letter.

If you receive a Letter 4883C from the IRS, you should respond in 30 days. Remember to:

- Follow the letter's instructions carefully to verify your identity.
- Call the number on the letter. You'll be connected to the Taxpayer Protection Program.
- Have a copy of your prior-year tax return, if you filed one, to help verify your identity.

If you are unable to verify your identity with the customer service representative, you may be asked to visit an IRS Taxpayer Assistance Center in person. You should plan on providing picture identification, plus the letter and a copy of the tax return if you did file it.

If you receive this or similar notices about suspicious returns, you do not need to complete the Form 14039 unless instructed to do so.

Once you verify your identity with the IRS, you can tell the representative if you did or did not file the return.

- If you did not file the return, it will be removed from your IRS records. You may be told you will need to file a paper return for the current filing season.
- If you did file the return, it will be released for processing and, barring other issues, your refund will be sent.

How quickly the IRS can work identity theft cases depends upon the volume of work and the complexity of the cases. Usually this process takes approximately 9 weeks.

Once the IRS has completely resolved your tax account issues, it will mark your account with an identity theft indicator to help protect you in the future.

Certain tax-related identity theft victims will be placed into the Identity Protection PIN program and receive by mail a new, six-digit IP PIN annually that must be entered on the tax return. The IP PIN adds an extra layer of identity protection.

Social Security Number Compromised

There might be situations that don't result in tax-related identity theft, but your social security number is compromised.

These situations include:

- Data breach (ex: IRS website, credit card database, department store)
- Computer hack, phishing email, compromised website
- Lost wallet

Victims should submit a Form 14039, *Identity Theft Affidavit*, only if your social security number has been compromised.

To do this:

1. Download IRS Form 14039, *Identity Theft Affidavit*.
2. Complete the form for each taxpayer that has been rejected. *Note: In Section B, you'll be checking box 2.*
3. Print the form and attach your form of identification.
4. Mail or fax according to instructions.

Report Suspected Tax Fraud Activity

The IRS has resources available to work towards closing down those involved in illegal activities. If you have information, please report it!

If You…	Then…	And…
Suspect or know of an individual or a business that is not complying with the tax laws on issues such as: • False Exemptions or Deductions • Kickbacks • False/Altered Document • Failure to Pay Tax • Unreported Income • Organized Crime • Failure to Withhold	Use Form 3949-A, *Information Referral*	Print the form and mail to: Internal Revenue Service Stop 31313 Fresno, CA 93888
Suspect fraudulent activity or an abusive tax scheme by a tax return preparer or tax preparation company	Use Form 14157, *Complaint: Tax Return Preparer* *Form 14157-A (see below) may also be required	You may complete the form online, print it and mail it to the IRS address on the form.
Suspect a tax return preparer filed a return or altered your return without your consent and you are seeking a change to your account	Use Form 14157, *Complaint: Tax Return Preparer* AND Form 14157-A, *Tax Return Preparer Fraud or Misconduct Affidavit*	Send BOTH forms (Form 14157 and Form 14157-A) to the address shown in the Instructions for Form 14157-A.
Suspect an abusive tax promotion or promoter	Use Form 14242, *Report Suspected Abusive Tax Promotions or Preparers*	Mail or fax to the address provided on the form.
Suspect misconduct or wrongdoing by an exempt organization or employee plan	Use Form 13909, *Tax-Exempt Organization Complaint (Referral)*	Mail it to the address provided on the form.
Suspect you received or are aware of fraudulent IRS e-mails and websites	Forward the email to: phishing@irs.gov	Delete the email! If you entered your username and password in one of these sites, it is strongly recommended to change your password for that email address as soon as possible and contact your IT resource.

Tax Pro Resources

Monitor Your PTIN for Suspicious Activity

Criminals are increasingly targeting tax professionals, not only to steal client data but also to steal the professionals' data, such as PTINs, EFINs or e-Service passwords. Tax preparers should be checking their PTIN accounts to ensure the number of returns filed using their identification number matches IRS records.

The IRS offers many preparers the ability to monitor Returns Filed Per PTIN. This information is available in the online PTIN system for tax return preparers who meet both of the following criteria. You must have:

- A professional credential (Enrolled Agent, Certified Public Accountant, Attorney, Enrolled Retirement Plan Agent or Enrolled Actuary) or are an Annual Filing Season Program participant, and
- At least 50 tax returns from the Form 1040 series processed in the current year.

It is important to monitor this information even if you do not prepare returns or only prepare a small number of returns. If there is no data shown, less than 50 returns have been processed with your PTIN.

To access "Returns Filed Per PTIN" information, follow these steps:

1. Visit irs.gov/ptin and log into your PTIN account.
2. From the Main Menu, find Additional Activities.
3. Under Additional Activities, select View Returns Filed Per PTIN.
4. Review the chart labeled Returns Per PTIN.

The chart will include a count of individual income tax returns filed and processed in the current year.

The information in the Returns Per PTIN chart is updated weekly and it is important that you regularly check this information. If the number of returns processed is significantly more than the number of tax returns you've prepared and you suspect possible misuse of your PTIN, complete and submit Form 14157, *Complaint: Tax Return Preparer.*

Tax Pro Resources

Monitor Your EFIN for Suspicious Activity

Identity thieves increasingly target tax professionals. A thief who breaches the data of one tax return preparer can gain hundreds or thousands of taxpayers' data.

One way you can monitor for suspicious activity is to check how many federal tax returns have been filed with your Electronic Filing Identification Number (EFIN).

As part of the ongoing concerns about security and identity theft, the IRS recommends that you verify the number of returns submitted under your EFIN. Do this routinely and especially during filing season. Verify your EFIN through IRS e-Services. If you do not have an e-Services account, then your first step would be to go to e-Services and register for an account.

Once you have logged into your e-Services account, follow these steps to verify the number of returns electronically filed with the IRS:

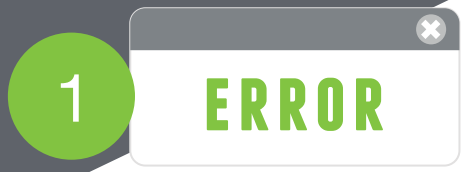
1. Select your name,
2. In the left banner, select Application,
3. In the left banner, select e-File Application,
4. Select your name again,
5. In the listing, select EFIN Status and on this screen you can see the number of returns filed based on return type.**

** These statistics are updated weekly. Please contact the IRS e-help Desk at 866.255.0654 if you see a significantly higher volume than you transmitted.

Tax Pro Resources

Perform a Deep Security Scan of Your Computer Drives

Ensuring that your computer is free of malware/viruses will help prevent the spread of infections during the filing season when you are in contact with clients and others.



Ensure that you and your employees have robust security software that helps block malware and viruses and that it remains turned on and active at all times.

Use the “deep scan” function to fully scour all computer drives and files for any malware or viruses. These bugs can hide in places that a “quick scan” does not search. Perform a deep scan periodically.

Ensure that your security software updates automatically so that it is always up-to-date and on-guard against new and emerging malware and viruses.

Review the security plan for your office and operations.

Educate your employees about the dangers of phishing, malware, emails and other scams that could lead to malware/virus infections. One phishing email can result in all office computers being hacked for sensitive data.

Tax Pro Resources

Create Strong Passwords

Stopping identity theft and refund fraud is a top priority for the IRS. IRS programmers work with major software providers to stop fraud. Plus, IRS systems have several built-in identifiers to flag suspicious returns.

Here are some things you should consider in creating and protecting passwords:

- Longer passwords are safe and more difficult to guess. A strong password should be a minimum of eight characters. It should include a combination of letters, numbers and symbols or special characters. Your password should include at least one uppercase letter, one lowercase letter, one number and one symbol or character.
- Personal information should not be included in your passwords. Names of siblings, children, pets, etc., are generally available on social media, which makes it easier for cybercriminals to figure out your password.
- Avoid using the same password for all of your information systems, accounts or devices. If someone does guess one password, they will not have access to all your systems, devices or data.
- Substitute numbers and symbols for letters in words or phrases to make it more difficult to guess a password.
- Do not share your password and be careful of attempts to trick you into revealing your password.

More information on two-factor authentication, as well as additional information can be found in the Phishing, Vishing and Smishing article from our Spring 2017 *TAXPRO Journal.* (Members Only)

Tax Pro Resources

Secure Your Office

Tax professionals can help protect taxpayer data by looking around their own offices. It's more important than ever that tax professionals take aggressive steps to protect taxpayer information. Securing office space is as important as securing computers.

In assessing how secure your office is, consider these questions:

- Are all the places where taxpayer information is located protected from unauthorized access and potential danger such as theft, flood or severe storms?
- Do you have written procedures that prevent unauthorized access and unauthorized processes?
- Do you leave taxpayer information, including data on hardware and media, unsecured? Check on desks, photocopiers, mailboxes, vehicles and trash cans. What about in rooms in the office or at home where unauthorized access could occur?
- Who authorizes and/or controls delivery and removal of taxpayer information, including data on hardware and media?
- Are the doors to file rooms and/or computer rooms locked?
- Do you provide secure disposal of taxpayer information? Do you use items such as shredders, burn boxes or secure temporary file areas for information until it can be properly disposed?

A data backup strategy is also important when securing your office. For example, if there is a ransomware attack, instead of paying the ransom, everything could be wiped out and restored from a backup, with only a minimal amountw of work lost.

For more information, see the Protecting Against Data Loss article from our Summer 2016 *TAXPRO Journal.* (Members Only)

Additional Resources

- The IRS guide, Safeguarding Taxpayer Data, includes checklists
- The FTC guide, Data Breach Response
- The IRS website, Data Theft Information for Tax Professionals
- The National Institute of Standards and Technology special publication, Security and Privacy Controls for Federal Information Systems and Organizations
- The National Institute of Standards and Technology special publication, Guide for Cybersecurity Event Recovery

Visit natptax.com to learn more about the National Association of Tax Professionals.

NATP™
National Association of Tax Professionals