Gleason
TAX ADVISORY

TAX-RELATED IDENTITY THEFT

Quick Guide to Help Protect, Prevent & Resolve

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

How we know a 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.
- The 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.

WARNING SIGNS FOR INDIVIDUAL CLIENTS

How we know a client's SSN has been compromised, putting them at risk when:

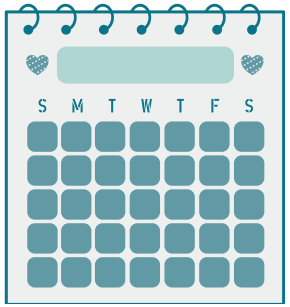
- A return is rejected; IRS reject codes indicate the taxpayer's SSN already has been used to file a tax return.
- The client observes activity or receives IRS notices regarding a tax return after all tax issues have been resolved, refund has been received or account balances have been paid.
- An IRS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

Remember:
We 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.

Quick Protection Tips

Here are some tips to protect you from being 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 firewalls 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 and 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 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

AVOID IRS IMPERSONATORS

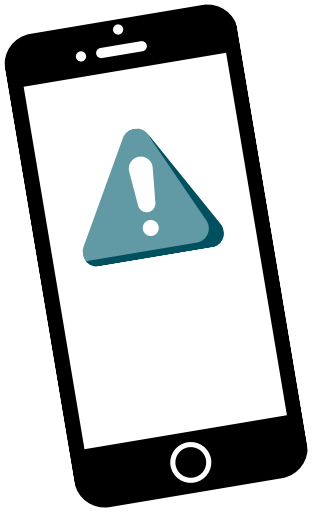
- The IRS will not call you with threats of jail or lawsuits.
- The IRS will not send you an unsolicited email suggesting you have a refund or that you need to update your account.
- The IRS will not request any sensitive information online.

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

Victim of Identity Theft – Now What?

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

1 **File a complaint with the FTC at identitytheft.gov.**

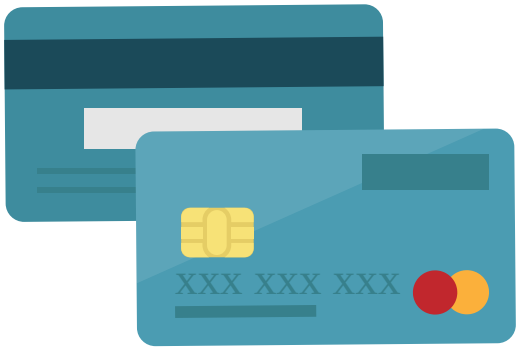


2 **Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:**

Equifax, Equifax.com, 1-888-378-4329

Experian, Experian.com

TransUnion, TransUnion.com
1-833-395-6938



3 **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

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

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.

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 nine 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.

RECEIVE IRS
NOTICE OF FRAUD

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.