Tax-Related Identity Theft: IRS Efforts to Assist Victims and Combat IDT Fraud

Brian Wozniak
IRS Stakeholder Liaison

November 4, 2015

Prevention and Detection

In recent years, the IRS has made numerous improvements to catch fraud before refunds are issued:

- Deployed more than 100 filters
- Limited direct deposit
- Locked deceased taxpayers' accounts
- Improved cooperation with local law enforcement

Recommended steps for IDT victims

Steps recommended by FTC for all identity theft victims:

- File a police report
- File a complaint with the FTC
- Contact one of the three credit bureaus to place a "fraud alert"
- Close any account opened without your permission

Identity Theft Information for Taxpayers

Identity theft places a burden on its victims and presents a challenge to many businesses, organizations and governments, including the IRS. The IRS combats this crime with an aggressive strategy of prevention, detection and victim assistance.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses your stolen Social Security number to file a tax return claiming a fraudulent refund. If you become a victim, we are committed to resolving your case as quickly as possible.

Know the warning signs

In tax-related identity theft, the criminal generally will use a stolen SSN to file a forged tax return and attempt to get a fraudulent refund early in the filing season.

You may be unaware that this has happened until you file your return later in the filing season and discover that two returns have been filed using the same SSN.

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

- More than one tax return was filed for you,
- You owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages from an employer unknown to you.

Steps for victims of identity theft

1. File a report with the local police.

2. File a complaint with the Federal Trade Commission at www.identitytheft.gov or the FTC Identity Theft Hotline at 1-877-438-4338 or TTY 1-866-653-4261.

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

- www.Equifax.com 1-800-525-6285
- www.Experian.com 1-888-397-3742
- www.TransUnion.com 1-800-680-7289

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

4. Respond immediately to any IRS notice; call the number provided

5. Complete IRS Form 14039, *Identity Theft Affidavit.* Use a fillable form at IRS.gov, print, then mail or fax according to instructions.

6. Continue to pay your taxes and file your tax return, even if you must do so by paper.

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

More information: www.irs.gov/identitytheft or FTC's www.identitytheft.gov.

About data breaches and your taxes

Not all data breaches or computer hacks result in tax-related identity theft. It's important to know what type of personal information was stolen.

If you've been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you and follow the "Steps for victims of identity theft."

How you can reduce your risk

- Don't routinely carry your Social Security card or any document with your SSN on it.
- Don't give a business your SSN just because they ask – only when absolutely necessary.
- Protect your personal financial information at home and on your computer .
- Check your credit report annually.
- Check your Social Security Administration earnings statement annually.
- Protect your personal computers by using firewalls, anti-spam/virus software, update security patches and change passwords for Internet accounts.
- Don't give personal information over the phone, through the mail or the Internet unless you have either initiated the contact or are sure you know who is asking.

NOTE: The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

Suspicious IRS Emails / Phone Calls

www.irs.gov/uac/Report-Phishing

You discover a **website** on the Internet that **claims to be the IRS** but you suspect it is bogus ...	**... send the URL of the suspicious site** to phishing@irs.gov. Please add in the subject line of the email, 'Suspicious website'.
You receive a **phone call** or **paper letter via mail** from an individual **claiming to be the IRS** but you suspect they are not an IRS employee ...	**Phone call:** 1. Ask for a call back number and employee badge number. 2. Contact the IRS to determine if the caller is an IRS employee with a legitimate need to contact you. 3. If you determine the person calling you is an IRS employee with a legitimate need to contact you, call them back. **Letter or notice via paper mail:** 1. Contact the IRS to determine if the mail is a legitimate IRS letter. 2. If it is a legitimate IRS letter, reply if needed. Report the incident to the Treasury Inspector General for Tax Administration if the caller or party that sent the paper letter is **not legitimate.**

Name: Wozniak, Brian C.
Spouse: Tabatha E. Wozniak

Tax Year: 2013
Reject Date: 4/11/2014

Reject(s) applied to this return are as follows:

FORM: Code: IND-508
Taxing Authority: Federal

Explanation:
Primary SSN in the Return Header must not be equal to the Spouse SSN on another tax return for which filing status is Married Filing Jointly or [filing status is Married Filing Separately and the Spouse exemption is claimed].
Solution:
Interview Forms View

1) Please verify the taxpayer's SSN is correct and has not been filed for this year. If the information is correct, please contact the Internal Revenue Service at 1-866-255-0654 for additional information.

Worksheet View

1) Please verify the taxpayer's SSN is correct and has not been filed for this year. If the information is correct, please contact the Internal Revenue Service at 1-866-255-0654 for additional information.

Recommended steps for IDT victims

Victims of **tax-related** identity theft should take these additional steps:

- Submit IRS Form 14039, Identity Theft Affidavit
- Respond immediately to IRS notices and letters
- Continue to file and pay taxes even if by paper
- Visit IRS.gov/identitytheft

Types of IRS Notices

- 5071C (www.idverify.irs.gov)
- 4883C
- 12C
- CP01
- CP01A
- CP01F

Taxpayers Receiving Identity Verification Letter Should Use IDVerify.irs.gov

IR-2015-54, March 18, 2015

WASHINGTON — The Internal Revenue Service today reminded taxpayers who receive requests from the IRS to verify their identities that the Identity Verification Service website, idverify.irs.gov, offers the fastest, easiest way to complete the task.

Taxpayers may receive a letter when the IRS stops suspicious tax returns that have indications of being identity theft but contains a real taxpayer's name and/or Social Security number. Only those taxpayers receiving **Letter 5071C** should access **idverify.irs.gov**.

The website will ask a series of questions that only the real taxpayer can answer.

Once the identity is verified, the taxpayers can confirm whether or not they filed the return in question. If they did not file the return, the IRS can take steps at that time to assist them. If they did file the return, it will take approximately six weeks to process it and issue a refund.

Letter 5071C is mailed through the U.S. Postal Service to the address on the return. It asks taxpayers to verify their identities in order for the IRS to complete processing of the returns if the taxpayers did file it or reject the returns if the taxpayers did not file it. The IRS does not request such information via email, nor will the IRS call a taxpayer directly to ask this information without you receiving a letter first. The letter number can be found in the upper corner of the page.

The letter gives taxpayers two options to contact the IRS and confirm whether or not they filed the return. Taxpayers may use the idverify.irs.gov site or call a toll-free number on the letter. Because of the high-volume on the toll-free numbers, the IRS-sponsored website, idverify.irs.gov, is the safest, fastest option for taxpayers with web access.

Taxpayers should have available their prior year tax return and their current year tax return, if they filed one, including supporting documents, such as Forms W-2 and 1099 and Schedules A and C.

Taxpayers also may access idverify.irs.gov through www.IRS.gov by going to Understanding Your 5071C Letter or the Understanding Your IRS Notice or Letter page. The tool is also available in Spanish. Taxpayers should always be aware of tax scams, efforts to solicit personally identifiable information and IRS impersonations. However, idverify.irs.gov is a secure, IRS-supported site that allows taxpayers to verify their identities quickly and safely.

IRS.gov is the official IRS website. Always look for a URL ending with ".gov" — not ".com," ".org," ".net," or other nongovernmental URLs.

Department of the Treasury	Transmittal Number	Date of Issue
	15-05	05/04/2015
	Originating Office	**Form Number**
IDRS CORRESPONDEX	SE:W:RICS:E:PRP	4883C

Internal Revenue Service

Title: Potential Identity Theft during Original Processing

Number of Copies	Distribution to:	Former Letter
Original and 1	2 to TP	4883C (Rev. 12-14)

OMB Clearance Number	Expires	
-		IMF

Letters Considered in Revision:

Social security number: [01 12T]
Tax year: [02 4Y]
Telephone number: [03 14V]
A Control number: [04 14V]

Dear [-30V]

We received a federal income tax return, Form [05 9V], for the tax year listed above with your name and social security number. To protect you from identity theft, we need to verify your identity before we process the return.

Please call the telephone number listed above between [06 10V] and [07 15V] within 30 days from the date of this letter. When you call, be sure you have a copy of your prior year tax return, your current year tax return (if you filed one), and any supporting documents (such as W-2's, 1099's, Schedule C, Schedule F, etc.).

If you didn't file this tax return, you should still contact us to confirm that you may be a victim of identity theft. We will take steps to assist you as soon as you complete the verification process.

If you choose to have an authorized power of attorney or a third party designee represent you, we encourage you to be available with your

representative when calling.

We won't be able to process your [08 13P] tax return until we hear from you.

To understand more about this letter, go to www.irs.gov, keyword search: 4883C.

Thank you for your cooperation.

Sincerely yours,

[09 35S]
[10 35S]

Enclosures:
Copy of this letter
.
B

NOTE: Include the appropriate time zone in fill-in 07.

NOTE: If Sel. A is not used, you must use Sel. B.

Types of IRS notices

- CP01 – Notifies the taxpayer that the IRS has resolved IDT issues and that an identity theft indicator has been placed on their account.
- CP01A – An annual notice that contains the latest IP PIN.
- CP01F – A one-time notice for 2015 giving certain taxpayers option of obtaining an IP PIN through www.irs.gov/getanippin.

Retrieving lost or misplaced IP PINs

- Use online application to retrieve original at www.irs.gov/getanippin, or
- Contact IPSU at 1-800-908-4490 for a “replacement” IP PIN.
- A replacement IP PIN will result in processing and refund delays because of validation requirements

Get Transcript: IRS Statement

The IRS announced today that criminals used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information on approximately 100,000 tax accounts through IRS' "Get Transcript" application. This data included Social Security information, date of birth and street address.

These third parties gained sufficient information from an outside source before trying to access the IRS site, which allowed them to clear a multi-step authentication process, including several personal verification questions that typically are only known by the taxpayer. The matter is under review by the Treasury Inspector General for Tax Administration as well as the IRS' Criminal Investigation unit, and the "Get Transcript" application has been shut down temporarily. The IRS will provide free credit monitoring services for the approximately 100,000 taxpayers whose accounts were accessed. In total, the IRS has identified 200,000 total attempts to access data and will be notifying all of these taxpayers about the incident.

As always, the IRS takes the security of taxpayer data extremely seriously, and we are working aggressively to protect affected taxpayers and continue to strengthen our protocols.

Additional information

The IRS announced today it will be notifying taxpayers after third parties gained unauthorized access to information on about 100,000 accounts through the "Get Transcript" online application.

The IRS determined late last week that unusual activity had taken place on the application, which indicates that unauthorized third parties had access to some accounts on the transcript application. Following an initial review, it appears that access was gained to more than 100,000 accounts through the Get Transcript application.

In this sophisticated effort, third parties succeeded in clearing a multi-step authentication process that required prior personal knowledge about the taxpayer, including Social Security information, date of birth, tax filing status and street address before accessing IRS systems. The multi-layer process also requires an additional step, where applicants must correctly answer several personal identity verification questions that typically are only known by the taxpayer.

The IRS temporarily shut down the Get Transcript application last week after an initial assessment identified questionable attempts were detected on the system in mid-May.

The online application will remain disabled until the IRS makes modifications and further strengthens security for it.

The matter is under continuing review by the Treasury Inspector General for Tax Administration and IRS offices, including Criminal Investigation.

The IRS notes this issue does not involve its main computer system that handles tax filing submission; that system remains secure.

On the Get Transcript application, a further review by the IRS identified that these attempts were quite complex in nature and appear to have started in February and ran through mid-May. In all, about 200,000 attempts were made from questionable email domains, with more than 100,000 of those attempts successfully clearing authentication hurdles. During this filing season, taxpayers successfully and safely downloaded a total of approximately 23 million transcripts.

In addition, to disabling the Get Transcript application, the IRS has taken a number of immediate steps to protect taxpayers, including:

* Sending a letter to all of the approximately 200,000 taxpayers whose accounts had attempted unauthorized accesses, notifying them that third parties appear to have had access to taxpayer Social Security numbers and additional personal financial information from a non-IRS source before attempting to access the IRS transcript application. Although half of this group did not actually have their transcript account accessed because the third parties failed the authentication tests, the IRS is still taking an additional protective step to alert taxpayers. That's because malicious actors acquired sensitive financial information from a source outside the IRS about these households that led to the attempts to access the transcript application.

* Offering free credit monitoring for the approximately 100,000 taxpayers whose Get Transcript accounts were accessed to ensure this information isn't being used through other financial avenues. Taxpayers will receive specific instructions so they can sign up for the credit monitoring. The IRS emphasizes these outreach letters will not request any personal identification information from taxpayers. In addition, the IRS is marking the underlying taxpayer accounts on our core processing system to flag for potential identity theft to protect taxpayers going forward – both right now and in 2016.

These letters will be mailed out starting later this week and will include additional details for taxpayers about the credit monitoring and other steps. At this time, no action is needed by taxpayers outside these affected groups.

The IRS is continuing to conduct further reviews on those instances where the transcript application was accessed, including how many of these households filed taxes in 2015. It's possible that some of these transcript accesses were made with an eye toward using them for identity theft for next year's tax season.

The IRS emphasizes this incident involves one application involving transcripts – it does not involve other IRS systems, such as our core taxpayer accounts or other applications, such as Where's My Refund.

The IRS will be working aggressively to protect affected taxpayers and strengthen our protocols even further going forward.

“Get Transcript” IRS Notices

- 4281G
- 4281B
- 4281F

The IP PIN Pilot

- There is an ongoing pilot program for taxpayers who filed 2013 returns from Florida, Georgia or District of Columbia.
- Taxpayers from these states *did not* have to be victims of identity theft to qualify for this program.
- Taxpayers could opt-in to get an IP PIN by using online application at www.IRS.gov/getanippin.

Understanding Your CP148A Notice

When we change a business address in our records, we send a CP 148A to the new address.

We issue a notice of confirmation of an address change to both the employer's former and new address.

We update an address when we receive either a:

- Form 8822-B
- Employment tax return with an address different from what's on our records.

Identity Theft (continued)

- POAs requesting client IP PIN
- Cancelling third party refund checks
- Practitioner phishing emails
- Verifying IRS employees
- PTIN Fraud
- Truncating / Redacting TINs
- IRS realignment

Business-related identity theft

- An identity thief files a business tax return (Form 1120, 720 etc.) using the Employer Identification Number of an active or inactive business to obtain a fraudulent refund.
- An identity thief, using the EIN of an active or inactive business, files fraudulent Forms 941 and W-2 to support a bogus Form 1040 claiming a fraudulent refund.

18

Protecting your business and clients

More system safeguards -

- Don’t store sensitive data on a machine with an internet connection
- Back up system(s) periodically on secure media
- Maintain updated firewalls, anti-virus, software updates, security patches, anti-spyware and anti-adware
- Provide central management security tools and passwords/security protections

19

Protecting your business and clients

If you have a security breach:

- Notify law enforcement
- Notify the Federal Trade Commission (www.FTC.gov)
- Notify customers and business partners
- Take corrective actions
- Prevent other breaches

20

Summary

Contact Information:

Brian Wozniak
brian.wozniak@irs.gov

21