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

Anita Douglas, Senior Stakeholder Liaison
May 27, 2015

What is tax-related identity theft?

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

IRS Strategy

The IRS combats identity theft with a multi-pronged strategy:

- Prevention
- Detection
- Victim Assistance

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

Prevention and Detection

Improvements, continued:

- Worked with state Departments of Corrections to curtail refund fraud by prisoners
- Partnered with financial institutions and software developers
- Worked with the pre-paid access card industry

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

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

Victim Assistance Process

- Confirmed IDT victim files IRS Form 14039, Identity Theft Affidavit (with or without a return).
- IRS codes taxpayer's account to show we received identity theft documentation.
- If necessary, IRS reconciles taxpayer's account to reflect valid return information.
- IRS places identity theft indicator on the taxpayer's account.

Victim Assistance Process

- IRS issues a CP01 notice
- Before the next filing season, the IRS generally assigns the taxpayer a unique Identity Protection PIN to use when filing.
- If the IRS identifies the taxpayer as deceased, the account is locked to prevent future filings from being processed.

Victim Assistance Process

- The IP PIN is a six-digit number assigned annually to:
  - A validated identity theft victim or
  - A taxpayer who voluntarily opt in to an ongoing pilot project
- The IP PIN is used as a supplement to the taxpayer's SSN to identify the taxpayer as the valid owner of the SSN and related tax account.

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.

News Essentials

- What's Hot
- News Releases
- IRS - The Basics
- IRS Guidance
- Media Contacts
- Facts & Figures
- Around the Nation
- e-News Subscriptions

The Newsroom Topics

- Multimedia Center
- Noticias en Español
- Radio PSAs
- Tax Scams
- The Tax Gap
- Fact Sheets
- IRS Tax Tips
- Armed Forces
- **Latest News Home**

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

Español

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

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

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.

Prevention and Detection

- IRS filters stop the vast majority of invalid refunds
- FY 11-14: stopped 19 million suspicious returns; protected more than $63 billion in fraudulent refunds
- Greatly reduced the time it takes to resolve a taxpayer's identity theft case.

Enforcement

FY 2014 Criminal Investigation efforts:

- Initiated 1,063 identity theft related investigations.
- Resulted in 748 sentencings as compared to 438 in FY 2013 and incarceration rate rose 7.1 percent to 87.7 percent.
- Jail time average at 43 months as compared to 38 months in FY 2013 — the longest sentencing being 27 years.

Preventing online identity theft

- Don’t respond to suspicious IRS emails, texts, or faxes
- Secure your computers (i.e., firewalls, anti-virus/anti-phishing/anti-spam, etc.)
- Use strong passwords
- Back up critical personal information
- Limit the personal information you provide on social media
- Never answer ‘yes’ to pop-up screens
- Visit onguardonline.gov

Suspicious IRS-related communication

If you or a client receive a suspicious communication claiming to be the IRS:

- Go to IRS.gov, scroll to the bottom of the homepage and click on ‘Report Phishing’
- Report all unsolicited email claiming to be from the IRS to phishing@irs.gov
- BEWARE – Phone scam is ongoing

Business-related identity theft

- Business Master File, or BMF, identity theft is defined as creating, using or attempting to use a business' identifying information, without authority, to obtain tax benefits.

- The following examples represent situations that *may* be due to identity theft related to the fraudulent use of business information.

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.

More Business-related identity theft

- An identity thief obtains an EIN using the name and Social Security Number of another individual as the responsible party, then files fraudulent tax returns (Form 941, 1120, 1041 etc.) to obtain a refund, avoid paying taxes, or further perpetuate individual identity theft or fraud.

Business-related identity theft

In January, 2014, IRS released BMF identity theft program guidance, policy and procedures. The new BMF procedures included:

- Form 14039-B, an electronic form designed for employees to use when they require taxpayers to provide supporting BMF identity theft documentation.
- BMF identity theft tracking indicators used to mark EINs affected by identity theft.
- Mandatory research requirements needed in support of a BMF identity theft determination.

Protecting Businesses from identity theft

Businesses can take practical measures to reduce the risk of tax-related identity theft:

- Protect the organization's federal employer identification number as you would a personal identification number.
- Only provide your organization's federal employer identification number and other sensitive information when necessary.

Protecting Businesses from identity theft cont.

- Verify the security of any website through which your organization transmits sensitive data.
- Properly dispose of sensitive company documents (for example using a micro-cut shredder).
- Increase identity theft awareness within your organization to ensure everyone is protecting sensitive data.

Dealing with tax-related identity theft

If you suspect your organization has been compromised by business identity theft, take the following steps:

- File a report with local law enforcement.
- Contact the major business credit agencies, including Equifax, Experian, TransUnion and Dunn and Bradstreet, to report the fraudulent activity and obtain a credit report to check for additional fraudulent activity.

Dealing with tax-related identity theft cont.

- Contact all credit card companies, financial institutions and creditors to alert them to the possibility of fraudulent activity.
- Respond to any IRS notices you receive and provide a detailed explanation of how you believe your organization has been affected by identity theft.

Protecting your business and clients

Physical safeguards

- Lock rooms and cabinets.
- Store records in secured area.
- Protect against destruction and damage.
- Inventory hardware.
- Dispose of information and hardware securely.

Protecting your business and clients

System safeguards:

- Use strong passwords: Minimum of eight alphanumeric characters
- Change passwords periodically
- Use timed, password-activated screen savers
- Don’t post or share passwords
- Encrypt sensitive data when:
  - Transmitting over networks
  - Storing on servers or media
- Encrypt entire computers, media

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

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

Additional information

- Identity theft information
- www.irs.gov/identitytheft
  - Individual identity theft
  - Business identity theft
  - Additional Resources
  - Taxpayer Guide to Identity Theft
  - Publication 5027 for taxpayers
  - Publication 5199 for tax preparers

Additional information

IP PIN Program

- General information:
  - www.irs.gov/uac/Newsroom/2014-Identity-Protection-PIN-(IP-PIN)-Pilot
- FAQs:
  - www.irs.gov/uac/Newsroom/2014-Identity-Protection-PIN-(IP-PIN)-Pilot:-Questions-and-Answers

THANK YOU!!!

Anita Douglas

405-297-4719

Anita.E.Douglas@irs.gov