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

Susan M Lamastro
SBSE Territory Manager

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses a Social Security Number (SSN) not belonging to them 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

How identity theft occurs

Identity theft most often occurs from the following sources:

- ✓ Dumpster diving
- ✓ Skimming
- ✓ Phishing
- ✓ Address changes
- ✓ Theft of records
- ✓ Pre-texting
- ✓ Trojan Horses
- ✓ Spyware
- ✓ Data breaches

Victim Assistance

Warning signs:

- E-filed return rejected as a duplicate
- IRS notice that more than one tax return was filed for taxpayer(s)
- Individuals may owe additional tax, have a refund offset or have collection actions taken against them
- IRS records indicate taxpayer(s) received wages from an employer unknown to them

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

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.

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.

Maintaining a well-trained workforce

- IRS has trained 37,000 employees who work with taxpayers over the phone, in person or through case work.

- The training emphasizes:
  - How to recognize signs of identity theft
  - How to help victims of identity theft
  - The importance of empathy when dealing with taxpayers who face this frustrating situation.

Suspicious IRS-related Communication

If a constituent receive a suspicious communication claiming to be the IRS, recommend the following steps:

- 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.

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.

Get Transcript Incident

The IRS is not immune to security breaches

- Discovered in May 2015 Get Transcripts on line option had unauthorized accesses.
  - IRS reviewed 23 Million uses
  - 334,000 unauthorized accesses
  - Additional 281,000 attempts were unsuccessful
- The program was shut down in response to the breach

ID Theft Summit

- ID Theft presents a huge burden to individuals and a challenge to businesses, organizations, and governmental agencies.
- ID Theft Summit began in March 2015
  - IRS
  - State Taxing Authorities
  - Tax Industry

ID Theft Summit

"The agreement represents a new era of cooperation and collaboration among the IRS, states and electronic tax industry that will help combat identity theft and protect taxpayers against tax refund fraud."

Commissioner Koskinen

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

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

Questions