Anderson Kill & Olick, P.C.
ESTATE PLANNING & TAX ADVISOR
Volume 12 Number 2 www.andersonkill.com Summer 2013

# Guarding Your "Tax" Identity From Being Stolen

By Carole B. Sheffield

Summer is upon us and the 2013 tax season is a distant memory — for most of us, including our estate planning and tax clients here at Anderson Kill. Yet, in 2012 I learned firsthand why the 2012 tax season might continue indefinitely, thanks to the successful efforts of a tax identity thief who fraudulently claimed our son's 2011 tax refund.

The stolen refund was truly an eye-opener because there were no conventional clues. On the contrary, it was a rejected, electronically "e-filed" IRS Form 1040 personal income tax return that triggered an eight-month journey into the unknown with the IRS to resolve our son's refund fraud case.

Our son was and is not alone. Tax identity theft is on the rise. Little has been written on the topic from the victim's perspective. Thus, the purpose of this article is to share the details of the IRS tax fraud resolution process — and to warn clients how to protect themselves from identity theft.

## Tax Identity Theft Defined and Discovered

Tax identity theft occurs when someone illegally uses a taxpayer's name and Social Security number to fraudulently claim a refund. The actual filed tax return appears authentic, except that the attached Form W-2 is entirely falsified and the reported wage and withheld tax data are completely fabricated.

The typical scammer e-files early in the tax season, before the unsuspecting victim may have even received the required W-2 and 1099 forms. Then, when the victim files, the legitimate tax return is rejected by the IRS because the system shows that a return has already been filed. In the meantime, the fraudulent refund has been deposited to the thief's prepaid credit or debit card.

## Scope of Tax Refund Fraud and Cost

Tax authorities consistently report the same trend — tax identity theft has been rising significantly since 2008. From 2008 to partial year 2012, tax identity theft cases increased by more than 650 percent.

Tax year 2011 offers the most comprehensive statistical picture. The IRS processed about 145 million returns in 2011 and of those returns filed, approximately 1.5 million returns were confirmed tax identity theft victims, representing a cost in stolen refunds of more than $5.2 billion.

## Reporting Tax Identity Theft

If you find yourself a possible tax identity theft victim, act quickly and report your case to the IRS. On the IRS website (www.irs.gov), under "Taxpayer Guide to Identity Theft," the IRS provides critical reporting steps. You should file Form 14039, *Identity Theft Affidavit*, and contemporaneously:

- If you receive a notice or letter from the IRS, respond immediately to the name and number found in the notice or letter.
- If you suspect you are a victim of tax identity theft, as with our son's rejected e-filed return, or if you have conclusive evidence of tax refund fraud, immediately call the IRS Identity Protection Specialized Unit (IPSU) at 1-800-908-4490.

## Case Opened — Expectations

Once your case is opened with the IPSU, expect regular IRS correspondence about every 45 days to provide a status update of its "research" necessary to complete your matter. The number of letters you receive depends on the success of the IRS in nabbing the perpetrator. It is the IRS's refund policy for tax identity victims that the IRS does not issue refunds until the alleged fraudster has been identified. In our son's case he received two such letters before his refund was electronically deposited into his bank account, without notice from the IRS.

## Case Closed — Expectations

Hooray! The tax refund was received, with interest (as required under the Internal Revenue

## who's who

**Carole B. Sheffield** is a shareholder in Anderson Kill's Philadelphia, PA, office. Ms. Sheffield's practice concentrates in estate and tax planning and trust and estate administration, including real estate matters. She handles complex matters of federal and state tax preparation of estate, gift, fiduciary income and personal income tax returns for trusts and estates. Her clients include high net worth individuals, financial institutions, closely held businesses and not-for-profit organizations.

**(267) 216-2732**

**csheffield@andersonkill.com**



Code). What next? The IRS then wrote in mid-December 2012 to say it had placed an identity theft indicator on our son's account for his protection. Also, in late December the IRS assigned a unique six-digit IP PIN, or identity protection personal identification number, to ensure the IRS that his 2012 filed return would be "really from you."

Caution: The IP PIN was not easily found in the notice. In fact, early in this process an IRS agent warned me that the IP PIN would arrive "buried" in a notice. This was true. The IP PIN was found in an unassuming separate sentence nestled in the midst of the entire notice — it was difficult to find.

A final notice from the IRS, dated December 31, 2012, officially confirmed the tax fraud for much needed closure and advised that the notice be kept with our son's tax records.

### Guard Your Tax Identity — Indefinitely

The IRS never told us how our son's tax identity was stolen. However, the IRS agent indicated that computer "hacking" into our son's place of employment was a strong possibility. The following tips are recommended to protect your tax identity from theft:

- Never carry your Social Security card or any documents containing your Social Security number or individual taxpayer identification number on them.
- Check your financial information online, frequently.
- Review your credit reports annually (Equifax, Experian and TransUnion).
- Keep personal information stored in your home securely.
- Maintain personal computer protection by using firewalls and anti-spam/virus software, updating security patches, changing your Internet account passwords often, and recording and keeping them in a secure location.
- Protect financial information by shredding documents before discarding them.
- Respond to genuine IRS correspondence promptly; however, do not click on links or open attachments from emails claiming to be from the IRS.
- Never give personal information over the phone, through the mail or on the Internet unless you have initiated the contact or you know the party.

Should you learn that you are a tax identity victim, please stay calm — the government stands behind you as a taxpayer and Anderson Kill is available to guide you through the resolution process.